



---

# proNX Service Manager User Guide

Release

7.8



---

Modified: 2019-01-29

Juniper Networks, Inc.  
1133 Innovation Way  
Sunnyvale, California 94089  
USA  
408-745-2000  
[www.juniper.net](http://www.juniper.net)

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

*proNX Service Manager User Guide*

7.8

Copyright © 2019 Juniper Networks, Inc. All rights reserved.

The information in this document is current as of the date on the title page.

#### YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

#### END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <https://support.juniper.net/support/eula/>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

# Table of Contents

	About the Documentation . . . . .	xxi
	Documentation and Release Notes . . . . .	xxi
	Documentation Conventions . . . . .	xxi
	Documentation Feedback . . . . .	xxiii
	Requesting Technical Support . . . . .	xxiv
	Self-Help Online Tools and Resources . . . . .	xxiv
	Creating a Service Request with JTAC . . . . .	xxv
<b>Chapter 1</b>	<b>proNX Service Manager . . . . .</b>	<b>27</b>
	About PSM . . . . .	27
	PSM Client . . . . .	27
	PSM Dashboard . . . . .	27
	PSM Server . . . . .	27
	Red Hat (CentOS) Linux . . . . .	28
	Support for RADIUS Server . . . . .	28
	PSM Overview . . . . .	28
	Running with Multiple Servers . . . . .	29
	Overview . . . . .	29
	Running Multiple Servers Without Server Replication . . . . .	30
	Running Multiple Servers with Server Replication . . . . .	30
	Supported Network Elements . . . . .	32
<b>Chapter 2</b>	<b>Getting Started . . . . .</b>	<b>33</b>
	Starting the PSM Client . . . . .	33
	PSM Client Navigation . . . . .	36
	Working with the PSM Client Window System . . . . .	36
	Customizing the Quick Access Toolbar . . . . .	38
	Displaying the Online Help . . . . .	40
	Viewing the List Of Supported Devices . . . . .	40
<b>Chapter 3</b>	<b>Managing PSM Users . . . . .</b>	<b>43</b>
	Introduction . . . . .	43
	Adding a User . . . . .	44
	Modifying a User . . . . .	46
	Deleting a User . . . . .	49
	Editing User Attributes on the Local RADIUS Server . . . . .	49
<b>Chapter 4</b>	<b>Managing Network Discovery and Ethernet Domains . . . . .</b>	<b>51</b>
	Introduction . . . . .	51
	Discovering Network Elements . . . . .	51
	Undiscovering a Network Element . . . . .	55

	Rediscovering a Network Element . . . . .	55
	Polling Discovered Network Elements . . . . .	55
	Ethernet Network Domains . . . . .	56
	Creating an Ethernet Domain . . . . .	56
	Checking Domain Membership for a Network Element . . . . .	57
	Scheduling Network Element Discoveries . . . . .	57
	Scheduling a Network Element Discovery Task . . . . .	58
	Viewing Scheduled Tasks . . . . .	61
	Deleting Scheduled Tasks . . . . .	62
<b>Chapter 5</b>	<b>Managing Network Topology . . . . .</b>	<b>63</b>
	Introduction . . . . .	63
	Icons and Definitions . . . . .	63
	Understanding the Network Topology View . . . . .	65
	Layer Views . . . . .	67
	Network Element and Link Details . . . . .	68
	Learning the Network Topology . . . . .	72
	Deriving Optical Topology Using DOL or ROADM Data . . . . .	73
	Deriving Layer 1 Topology Using Snooped LLDP Data . . . . .	73
	Deriving Ethernet Topology Using LLDP Data . . . . .	74
	Deriving Topology Using Remote IDs . . . . .	74
	Remote ID Format . . . . .	75
	Remote ID Configuration . . . . .	78
	Setting the Remote ID . . . . .	79
	Setting the Remote ID on a Multiplexer/Demultiplexer . . . . .	80
	Setting the Remote ID on a ROADM C2 Port . . . . .	82
	Deleting the Remote ID . . . . .	83
	Interactions with LLDP . . . . .	83
	Viewing External Devices . . . . .	85
	Detecting Remote ID Errors . . . . .	85
	Network Element Groups and Sites . . . . .	86
	Creating a New Group . . . . .	87
	Moving Network Elements, Groups, And/or Sites to a Different Group . . . . .	88
	Adding Network Elements to a New Group or Site . . . . .	88
	Adding Groups And/or Sites to a New Group . . . . .	89
	Navigating Between Parent and Child Groups . . . . .	89
	Changing the Background View . . . . .	91
<b>Chapter 6</b>	<b>Working with Network Elements . . . . .</b>	<b>95</b>
	Editing Notes for a Network Element . . . . .	95
	Identifying Services Associated with a Network Element . . . . .	96
	Viewing Network Element Inventory Information . . . . .	97
	Searching for a Network Element . . . . .	99
	Managing Information for a Network Element . . . . .	100
	Enabling or Disabling Network Element Maintenance Modes . . . . .	111
	Marking or Unmarking a Network Element . . . . .	112
	Enabling or Disabling Provisioning Mode on a Network Element . . . . .	113



	Connecting to the CLI on a Network Element . . . . .	114
	Provisioning OSPF on a BTI7000 Series Management Network . . . . .	114
	Adding OSPF Management . . . . .	114
	Editing OSPF Management Settings . . . . .	115
	Deleting OSPF Management . . . . .	116
	Adding an OSPF Management Interface . . . . .	117
	Editing an OSPF Management Interface . . . . .	119
	Deleting an OSPF Management Interface . . . . .	121
	Configuring In-Band Management on a BTI7800 Network Element . . . . .	122
<b>Chapter 7</b>	<b>Working with the Shelf View . . . . .</b>	<b>125</b>
	Introduction . . . . .	125
	Displaying Network Elements in the Shelf View . . . . .	125
	Displaying Alarms from the Shelf View . . . . .	129
	Setting the Remote ID from the Shelf View . . . . .	129
	Deleting the Remote ID from the Shelf View . . . . .	130
<b>Chapter 8</b>	<b>Nodal Management . . . . .</b>	<b>133</b>
	Introduction . . . . .	133
	Nodal Management for BTI7000 Series Network Elements . . . . .	134
	Launching the proNX 900 Node Controller . . . . .	134
	Provisioning a BTI7000 Series Shelf . . . . .	135
	Adding a Shelf . . . . .	135
	Deleting a Shelf . . . . .	137
	Provisioning a Slot on a BTI7000 Series Shelf . . . . .	137
	Adding a Module . . . . .	137
	Deleting a Module . . . . .	139
	Provisioning a Transponder on a BTI7000 Series Shelf . . . . .	139
	Provisioning Ports on a BTI7000 Series Transponder . . . . .	139
	Provisioning Cross-connects on a BTI7000 Series Transponder . . . . .	143
	Provisioning Line Protection Groups on a BTI7000 Series Transponder . . . . .	145
	Provisioning Client Protection Groups on a BTI7000 Series Transponder . . . . .	148
	Provisioning a Muxponder on a BTI7000 Series Shelf . . . . .	150
	Provisioning Ports on a BTI7000 Series Muxponder . . . . .	151
	Provisioning Virtual Concatenation Groups on a BTI7000 Series Muxponder . . . . .	155
	Provisioning Cross-connects on a BTI7000 Series Muxponder . . . . .	158
	Provisioning Protection Groups on a BTI7000 Series Muxponder . . . . .	160
	Provisioning Synchronization on a BTI7000 Series Muxponder . . . . .	162
	Provisioning a multiplexer/demultiplexer on a BTI7000 Series Shelf . . . . .	163
	Adding or Viewing a multiplexer/demultiplexer . . . . .	163
	Deleting a multiplexer/demultiplexer . . . . .	165
	Provisioning GCC on a BTI7000 Series Network Element . . . . .	165
	Provisioning GCC . . . . .	165
	Deleting GCC . . . . .	166
	Viewing Port PMs on a BTI7000 Series Network Element . . . . .	166

Provisioning the BTI7000 Series Dynamic Optical Layer (DOL) . . . . .	168
Provisioning Optical Groups . . . . .	168
Editing WDM Parameters in an Optical Group . . . . .	171
Adding and Deleting the C2 Port . . . . .	173
Editing Optical Port Parameters . . . . .	174
Configuring a Split ROADM Node . . . . .	176
Editing OSC Parameters in an Optical Group . . . . .	177
Enabling or Disabling a Port . . . . .	180
Nodal Management for BTI7800 Series Network Elements . . . . .	181
Provisioning a BTI7800 Chassis . . . . .	181
Adding a Shelf . . . . .	181
Editing a Shelf . . . . .	183
Deleting a Shelf . . . . .	184
Provisioning a Universal Forwarding Module on a BTI7800 . . . . .	184
Adding a UFM . . . . .	185
Editing a UFM . . . . .	187
Deleting a UFM . . . . .	188
Adding a BIC . . . . .	188
Editing a BIC . . . . .	190
Cloning a BIC . . . . .	191
Deleting a BIC . . . . .	192
Adding a Transceiver . . . . .	193
Editing a Transceiver . . . . .	195
Cloning a Transceiver . . . . .	196
Deleting a Transceiver . . . . .	197
Adding an Interface . . . . .	198
Editing an Interface . . . . .	205
Configuring a Multiplexed Interface . . . . .	211
Cloning an Interface . . . . .	213
Deleting an Interface . . . . .	214
Viewing Interface PMs on a UFM . . . . .	215
Provisioning a ROADM Node on a BTI7800 . . . . .	216
General Provisioning Procedure . . . . .	217
Adding a ROADM or an ILA Module . . . . .	218
Editing a ROADM or an ILA Module . . . . .	219
Deleting a ROADM or an ILA Module . . . . .	220
Adding a PRE Module . . . . .	220
Editing a PRE Module . . . . .	221
Deleting a PRE Module . . . . .	222
Adding or Viewing a multiplexer/demultiplexer . . . . .	222
Deleting a multiplexer/demultiplexer . . . . .	225
Editing a Port . . . . .	225
Editing the OMS . . . . .	226
Editing the OSC . . . . .	227
Adding a Fiber Connection on a ROADM or an ILA Client Port . . . . .	227
Editing a Fiber Connection on a ROADM or an ILA Client Port . . . . .	228
Deleting a Fiber Connection on a ROADM or an ILA Client Port . . . . .	229
Adding a Fiber Connection on a ROADM or an ILA Line Port . . . . .	230
Editing a Fiber Connection on a ROADM or an ILA Line Port . . . . .	231

Deleting a Fiber Connection on a ROADM or an ILA Line Port . . . . .	231
Adding a Fiber Connection on a UFM Interface . . . . .	232
Editing a Fiber Connection on a UFM Interface . . . . .	233
Deleting a Fiber Connection on a UFM Interface . . . . .	233
Viewing Fiber Connections . . . . .	234
Adding an Optical Channel . . . . .	234
Bulk Adding Optical Channels . . . . .	235
Editing an Optical Channel . . . . .	237
Deleting an Optical Channel . . . . .	238
Viewing Port PMs on a ROADM Element . . . . .	238
Viewing OMS PMs on a ROADM Element . . . . .	239
Viewing OSC PMs on a ROADM Element . . . . .	240
Viewing Optical Channel PMs on a ROADM Element . . . . .	240
Provisioning a 96-Channel Amplifier on a BT17800 . . . . .	241
Adding an Amplifier . . . . .	241
Creating an Optical Group for a BT17800 Series Amplifier . . . . .	242
Assigning or Unassigning an Amplifier . . . . .	244
Editing an Amplifier Port . . . . .	245
Editing WDM Parameters for an Amplifier . . . . .	246
Editing OSC Parameters for an Amplifier . . . . .	248
Changing an Amplifier's Group . . . . .	250
Viewing Port PMs on a 96-Channel Amplifier . . . . .	251
Provisioning a Wavelength Protection Switch Module on a BT17800 . . . . .	251
Adding a WPS Module . . . . .	251
Adding a Protection Group . . . . .	252
Editing a Protection Group . . . . .	254
Deleting a Protection Group . . . . .	255
Editing a Port . . . . .	255
Enabling or Disabling a Port . . . . .	257
Nodal Management for Juniper Networks Routers and Switches . . . . .	257
Editing an Interface . . . . .	258
Enabling or Disabling a Port . . . . .	262
Viewing Interface PMs on an MX Series or PTX Series Router or QFX Series Switch . . . . .	263
Nodal Management for BT1800 Series Network Elements . . . . .	265
Enabling or Disabling a Port . . . . .	265
<b>Chapter 9 Configuring PSM Client Options . . . . .</b>	<b>267</b>
Introduction . . . . .	267
Configuring General Options . . . . .	267
Setting Auto-logout . . . . .	267
Configuring Alerts Options . . . . .	268
Setting Alarm Alerts Options . . . . .	268
Configuring Display Options . . . . .	269
Setting Alarm Display Options . . . . .	269
Setting Auto-categorization Options . . . . .	270
Setting Device Display Options . . . . .	274
Setting Overlay Display Options . . . . .	274
Setting Service Display Options . . . . .	275

	Setting Topology Display Options . . . . .	276
	Configuring Performance Monitoring Options . . . . .	277
	Setting Historical PM Graphing Options . . . . .	277
	Setting Optical Graphing Options . . . . .	278
	Setting Real-time Collections Options . . . . .	278
	Configuring Utilities . . . . .	279
	Setting Utility Executables . . . . .	280
	Configuring the proNX 900 Node Controller . . . . .	282
<b>Chapter 10</b>	<b>Bulk Configuration Of Network Elements . . . . .</b>	<b>287</b>
	Introduction . . . . .	287
	Creating New Users on Multiple Network Elements . . . . .	287
	Configuring RADIUS Server Parameters on Multiple Network Elements . . . . .	291
	Configuring NTP Server Parameters on Multiple Network Elements . . . . .	297
<b>Chapter 11</b>	<b>Managing Optical and Transport Services . . . . .</b>	<b>301</b>
	Optical Services . . . . .	301
	Visualizing an Optical Service . . . . .	301
	Activating an Optical Service in a BTI7000 Network . . . . .	306
	Activating an Optical Service Between BTI7000 Optical Port Endpoints . . . . .	306
	Activating an Optical Service Between Transponder Interface Endpoints . . . . .	308
	Examples Of Path Selection in a BTI7000 Optical Network . . . . .	316
	Activating an Optical Service in a BTI7800 Network . . . . .	319
	Viewing the Cross-Connects in an Optical Service . . . . .	321
	Updating an Optical Service . . . . .	321
	Deleting an Optical Service . . . . .	321
	Viewing the Optical Services Table . . . . .	322
	Viewing the Optical Services Per Span Table . . . . .	322
	Viewing the Optical Topology Table . . . . .	323
	Transport Services . . . . .	323
	Visualizing a Transport Service . . . . .	324
	Activating a Transport Service . . . . .	328
	Updating a Transport Service . . . . .	332
	Deleting a Transport Service . . . . .	332
	Viewing the Transport Services Table . . . . .	332
	Viewing the Transport Services Per Span Table . . . . .	333
	Viewing the Transport Topology Table . . . . .	333
	Viewing the Transponder Tuning Grid . . . . .	334
	Working with Optical/Transport Services and Topology Tables . . . . .	334
	Sorting the Tables . . . . .	334
	Filtering the Tables . . . . .	335
	Saving a Service Image . . . . .	336
<b>Chapter 12</b>	<b>Managing Ethernet Services . . . . .</b>	<b>337</b>
	Introduction . . . . .	337
	Service Visualization . . . . .	337
	Visualizing an Ethernet Service . . . . .	337
	Service Visualization Scheme . . . . .	341

Understanding Ethernet Service States . . . . .	342
Service Activation . . . . .	344
Service Types . . . . .	346
Auto-provisioning NNIs . . . . .	347
Activating an Ethernet Service . . . . .	348
Example: Activating an EVPLINE Service . . . . .	364
Part 1: Setting Up the EVPLINE Service with CVLAN Translation . . . . .	364
Part 2: Setting Up the EVPLINE Service with the Virtual Untagged Option . . . . .	370
Example: Activating an Ethernet Service on a Multi-chassis LAG . . . . .	377
Example: Activating EVPLAN and EVPLINE Services Using Service Maps for Flow Redirection . . . . .	381
Part 1: Setting Up the Service Maps . . . . .	383
Part 2: Setting Up the EVPLINE Services . . . . .	390
Setting Up the EVPLAN Service . . . . .	395
Modifying a Service . . . . .	399
Modifying a Port in a Service . . . . .	399
Adding a Port to a Service . . . . .	400
Removing a Port from a Service . . . . .	401
Deleting a Service . . . . .	402
Adding SLA/CFM to a Service . . . . .	402
Running a Y.1731 Link Trace . . . . .	408
Running a Y.1731 Loopback . . . . .	409
Running an RFC 2544 Benchmarking Test . . . . .	410
Ethernet Ring Protection Switching (ERPS) . . . . .	414
Visualizing an ERPS Service . . . . .	414
Effect Of Link Failure on ERPS States . . . . .	417
Viewing the ERPS Services Table . . . . .	418
Adding VLANs to an ERPS Ring . . . . .	419
Routing Considerations in Mixed Networks . . . . .	421
GVRP - GARP VLAN Registration Protocol . . . . .	421
Mixed Networks - BTI7000 Series with BTI700 Series or BTI800 Series Elements . . . . .	422
Creating Services in BTI7000 Series packetVX Only Networks . . . . .	422
Creating Services Over BTI700 Series And/or BTI800 Series Only Networks . . . . .	423
Activating Services Over Combinations Of BTI7000 Series packetVX and BTI700 Series or BTI800 Series Networks . . . . .	424
Managing Profiles . . . . .	426
About Profile Manager . . . . .	426
Selecting a Profile During Service Activation . . . . .	427
Managing Profile Templates . . . . .	428
Creating a Profile Template . . . . .	428
Editing an Existing Profile Template . . . . .	430
Creating a Profile Template Through Cloning . . . . .	431
Deleting a Profile Template . . . . .	431
Bandwidth Profile Templates . . . . .	431
TCM Bandwidth Profiles . . . . .	432
Two-rate TCM . . . . .	433

	Single-rate TCM . . . . .	433
	CAR Bandwidth Profile Template . . . . .	433
	Color Mode and Actions . . . . .	433
	Setting DEI on Exceed Traffic . . . . .	434
	Internal Priority for Bandwidth Profile Templates . . . . .	434
	Class Map Profile Templates . . . . .	434
	Service Policy Profile Templates . . . . .	436
	Service Map Profile Templates . . . . .	438
	SLA Measurement Profile Templates . . . . .	439
<b>Chapter 13</b>	<b>Managing Pseudowire Services . . . . .</b>	<b>441</b>
	Introduction . . . . .	441
	Visualizing a Pseudowire Service . . . . .	441
	Service Activation . . . . .	444
	Activating a Pseudowire Service . . . . .	445
	Modifying a Pseudowire Service . . . . .	450
	Deleting a Pseudowire Service . . . . .	451
<b>Chapter 14</b>	<b>Managing Customers . . . . .</b>	<b>453</b>
	Introduction . . . . .	453
	Adding a Customer . . . . .	454
	Modifying a Customer . . . . .	455
	Deleting a Customer . . . . .	456
<b>Chapter 15</b>	<b>Managing Network Element Alarms . . . . .</b>	<b>457</b>
	Supported Network Elements and Devices . . . . .	457
	MX Series, PTX Series, and QFX Series Alarms . . . . .	457
	Alarm Visualization . . . . .	458
	Viewing Current Alarms . . . . .	460
	Understanding Alarm Timestamps . . . . .	461
	How the PSM Server Timestamps the Alarms . . . . .	462
	How the PSM Server Timestamps the Clears . . . . .	462
	How the PSM Client Displays Timestamps . . . . .	462
	Working with the Alarms Table . . . . .	462
	Sorting the Alarms Table . . . . .	462
	Filtering the Alarms Table . . . . .	463
	Using Service/alarm Correlation . . . . .	466
	Suspending Alarm Notification . . . . .	466
	Understanding the Alarms Summary Bar . . . . .	466
	Resetting the Deltas . . . . .	467
	Interpreting the Deltas . . . . .	468
	Filtering Based on Alarm Severity . . . . .	468
	Acknowledging, Emailing, and Clearing Alarms . . . . .	469
	Assigning an Alarm to a User . . . . .	470
	Viewing Historical Alarms . . . . .	470
	Viewing Alarms Through an RSS Feed . . . . .	472
	Sending Traps on the Northbound Interface . . . . .	473
	Adding a Trap Receiver for Alarms . . . . .	473
	Modifying a Trap Receiver for Alarms . . . . .	475
	Deleting a Trap Receiver for Alarms . . . . .	475

<b>Chapter 16</b>	<b>Managing Network Element System Software and FTP Servers . . . . .</b>	<b>477</b>
	Adding an FTP or SFTP Server . . . . .	477
	Modifying the Configuration for an FTP or SFTP Server . . . . .	479
	Deleting an FTP or SFTP Server . . . . .	480
	Manually Backing Up a Network Element Configuration Database . . . . .	481
	Restoring a Configuration Database to a Network Element . . . . .	482
	Upgrading System Software for a Network Element . . . . .	484
	Restoring a Database to Factory Defaults on a BT17800 Network Element . . . .	487
<b>Chapter 17</b>	<b>Managing Reports . . . . .</b>	<b>489</b>
	Generating Alarms Reports . . . . .	489
	Generating an Active Alarms Report . . . . .	489
	Generating a Historical Alarms Report . . . . .	490
	Generating Ethernet Reports . . . . .	493
	Generating Pseudowire Reports . . . . .	494
	Generating Transport Reports . . . . .	495
	Generating NE Logs Reports . . . . .	496
	Generating Optical Reports . . . . .	498
	Generating Inventory Reports . . . . .	499
	Generating Task History Reports . . . . .	501
	Changing the Report Generation Timeout . . . . .	504
<b>Chapter 18</b>	<b>Performance Monitoring . . . . .</b>	<b>507</b>
	Viewing Current Port, Interface, and Channel PMs . . . . .	507
	Viewing Real-time Optical Service PMs . . . . .	507
	Viewing Real-time Transport Service PMs . . . . .	515
	Viewing Real-time Ethernet PMs and SLAs . . . . .	520
	Viewing Real-time Pseudowire PMs . . . . .	528
	Collecting and Viewing Historical PMs . . . . .	531
<b>Chapter 19</b>	<b>Troubleshooting . . . . .</b>	<b>537</b>
	Managing Task Status . . . . .	537
	Discovering Task Status . . . . .	539
	Clearing Completed Tasks . . . . .	539
	Exporting Client and Server Logs . . . . .	539
	Performing Diagnostics . . . . .	540
	Viewing the PSM Client Log . . . . .	540
	Testing Network Element Connectivity . . . . .	541
	Verifying PSM Client-server Connectivity . . . . .	542
	Collecting and Viewing NE Logs . . . . .	542
	Saving Network Element Configuration Information . . . . .	545
	Troubleshooting Server Replication . . . . .	545
	Loss Of Connectivity to the Cluster . . . . .	545
	Loss Of Synchronization with a Cluster Member . . . . .	546
	Re-establishment Of Connectivity to the Cluster . . . . .	546
	Synchronizing Replicated Data Manually . . . . .	546
	Restarting the Cluster . . . . .	547

<b>Chapter 20</b>	<b>Appendix</b> .....	<b>549</b>
	Service Activation Error Messages .....	549
	PSM Alarms .....	550
	BTI7800 Alarm Details .....	554
	Installing Net-SNMP .....	555
	Configuring Historical PM Collection on BTI800 Series Network Elements . . .	558
	PM Counters .....	560
	PM Counters for BTI7000 Series Transponders and Muxponders .....	560
	PM Counters for BTI7000 Series DOL Modules .....	565
	PM Counters for BTI7000 Series packetVX Modules .....	567
	PM Counters for BTI718E Modules .....	573
	PM Counters for BTI800 Series Modules .....	574
	PM Counters for Optical Interfaces on MX Series and PTX Series Routers and QFX Series Switches .....	576
	Regular Expressions .....	578



# List of Figures

<b>Chapter 1</b>	<b>proNX Service Manager</b> . . . . .	<b>27</b>
	Figure 1: PSM Managed Network . . . . .	29
<b>Chapter 2</b>	<b>Getting Started</b> . . . . .	<b>33</b>
	Figure 2: Top Level Screen Layout for proNX Service Manager . . . . .	36
<b>Chapter 5</b>	<b>Managing Network Topology</b> . . . . .	<b>63</b>
	Figure 3: Hovering Over a Network Element . . . . .	68
	Figure 4: Hovering Over a PSM Server . . . . .	69
	Figure 5: Hovering Over a Network Element Group . . . . .	69
	Figure 6: Show Link Details . . . . .	69
	Figure 7: Link Details Data Widget Title Bar . . . . .	69
	Figure 8: Link Details Data Widget Window . . . . .	70
	Figure 9: BTI7000 Series DOL-DOL Link Details Data Widget . . . . .	71
	Figure 10: BTI7000 Series PVX-PVX Link Details Data Widget . . . . .	71
	Figure 11: BTI7000 Series Transponder-Transponder Link Details Data Widget . . . . .	71
	Figure 12: BTI7000 Series Muxponder-Muxponder Link Details Data Widget . . . . .	72
	Figure 13: MX Series Router Transponder to BTI7000 Series DOL Link Details Data Widget . . . . .	72
	Figure 14: External Device to BTI7000 Series PVX Link Details Data Widget . . . . .	72
	Figure 15: Hide Link Details . . . . .	72
	Figure 16: Provision Remote Port ID . . . . .	78
	Figure 17: Selecting the C2 Port . . . . .	82
	Figure 18: Map View Of Group Contents . . . . .	90
	Figure 19: Map View Of Parent . . . . .	91
<b>Chapter 6</b>	<b>Working with Network Elements</b> . . . . .	<b>95</b>
	Figure 20: Network Inventory . . . . .	98
	Figure 21: Network Inventory for PSM Server . . . . .	98
	Figure 22: Searching for an IP Address . . . . .	100
	Figure 23: Selecting the Search Category . . . . .	100
	Figure 24: Searching for a Service Type . . . . .	100
<b>Chapter 7</b>	<b>Working with the Shelf View</b> . . . . .	<b>125</b>
	Figure 25: Shelf View for a BTI7814 Network Element . . . . .	126
	Figure 26: Shelf View for an MX240 Router . . . . .	127
	Figure 27: Shelf View for a BTI7200 Network Element . . . . .	127
	Figure 28: Shelf View for a BTI718E Network Element . . . . .	127
	Figure 29: Shelf View for a BTI805 Network Element . . . . .	128
	Figure 30: Shelf View for a BTI810 Network Element . . . . .	128
	Figure 31: Shelf View for a BTI821 Network Element . . . . .	128

	Figure 32: Shelf View for a BTI822 Network Element . . . . .	128
<b>Chapter 8</b>	<b>Nodal Management . . . . .</b>	<b>133</b>
	Figure 33: BTI7000 Series Provision Shelf . . . . .	136
	Figure 34: BTI7000 Series Provision Slot . . . . .	138
	Figure 35: BTI7000 Series Provision/Edit Transceiver . . . . .	140
	Figure 36: BTI7000 Series Provision Port . . . . .	151
	Figure 37: Provision Optical Group . . . . .	169
	Figure 38: Edit WDM Dialog for a BTI7000 Series ROADM Module . . . . .	172
	Figure 39: Edit Optical Layer Port Dialog for a BTI7000 Series ROADM Line Port . . . . .	175
	Figure 40: Edit OSC Dialog for a BTI7000 Series ROADM Module . . . . .	178
	Figure 41: BTI7800 Series Provision Shelf . . . . .	182
	Figure 42: BTI7800 Series Provision Shelf . . . . .	183
	Figure 43: BTI7800 Series Provision Slot . . . . .	186
	Figure 44: BTI7800 Series Edit Slot (UFM) . . . . .	187
	Figure 45: BTI7800 Series Provision BIC . . . . .	189
	Figure 46: BTI7800 Series Edit BIC . . . . .	190
	Figure 47: BTI7800 Series Clone Equipment (BIC) . . . . .	192
	Figure 48: BTI7800 Series Provision Transceiver . . . . .	194
	Figure 49: BTI7800 Series Edit Transceiver . . . . .	195
	Figure 50: BTI7800 Series Clone Equipment (transceiver) . . . . .	197
	Figure 51: BTI7800 Series Provision Interface (OTU4) . . . . .	199
	Figure 52: BTI7800 Series Provision Interface (Optical Channel) . . . . .	200
	Figure 53: BTI7800 Series Edit Interface (OTU4) . . . . .	206
	Figure 54: BTI7800 Series Edit Interface (Optical Channel) . . . . .	207
	Figure 55: BTI7800 Series Edit Interface (ODU4) . . . . .	212
	Figure 56: ODU4 Interface with 10 ODU2 Sub-interfaces . . . . .	213
	Figure 57: BTI7800 Series Clone Equipment (interface) . . . . .	214
	Figure 58: Provision Optical Group . . . . .	243
	Figure 59: Edit WDM Dialog for a BTI7800 96-Channel Amplifier Module . . . . .	247
	Figure 60: Edit OSC Dialog for a BTI7800 96-Channel Amplifier Module . . . . .	249
	Figure 61: Edit Interface (OTU4) . . . . .	261
<b>Chapter 9</b>	<b>Configuring PSM Client Options . . . . .</b>	<b>267</b>
	Figure 62: Customers Branch Without Auto-categorization . . . . .	272
	Figure 63: Customers Branch with Auto-categorization Using Default Categories . . . . .	272
<b>Chapter 10</b>	<b>Bulk Configuration Of Network Elements . . . . .</b>	<b>287</b>
	Figure 64: Configure Radius Server . . . . .	293
	Figure 65: Configure Radius Server (BTI718E) . . . . .	293
<b>Chapter 11</b>	<b>Managing Optical and Transport Services . . . . .</b>	<b>301</b>
	Figure 66: Optical Service Between Transponder Endpoints . . . . .	312
	Figure 67: Selecting the First Path and Channel . . . . .	317
	Figure 68: Selecting the Second Path and Channel . . . . .	317
	Figure 69: Selecting a Path with No Decision Points . . . . .	318
	Figure 70: Selecting a Path with One Decision Point . . . . .	318
	Figure 71: Selecting a Path with Two Decision Points . . . . .	319

	Figure 72: Hovering Over a Transport Service . . . . .	325
	Figure 73: Hovering Over the Transport Service Component of a BTI7000 Optical Service . . . . .	325
	Figure 74: Optical Topology Column Selection . . . . .	335
<b>Chapter 12</b>	<b>Managing Ethernet Services . . . . .</b>	<b>337</b>
	Figure 75: Hovering Over a Switch . . . . .	342
	Figure 76: Hovering Over a UNI . . . . .	342
	Figure 77: Hovering Over a Link . . . . .	342
	Figure 78: Example: EVPLINE Services . . . . .	364
	Figure 79: Example: EVPLINE and EVPLAN Services . . . . .	382
	Figure 80: Creating Services in BTI7000 Series packetVX Only Networks . . . . .	422
	Figure 81: Creating Services in BTI7000 Series packetVX-only Networks . . . . .	423
	Figure 82: Creating Services Over BTI700 Series And/or BTI800 Series Only Networks . . . . .	423
	Figure 83: Creating Services Over BTI700 Series And/or BTI800 Series Only Networks . . . . .	424
	Figure 84: Activating Services Over a Combination Of BTI7000 Series packetVX, BTI700 Series, and BTI800 Series Networks . . . . .	425
	Figure 85: Bandwidth Profile Template Parameters . . . . .	432
	Figure 86: Class Map Profile Template . . . . .	435
	Figure 87: Service Policy Profile Template . . . . .	437
	Figure 88: Service Map Profile Template . . . . .	438
	Figure 89: SLA Measurement Profile Template . . . . .	439
<b>Chapter 13</b>	<b>Managing Pseudowire Services . . . . .</b>	<b>441</b>
	Figure 90: BTI800 Series Component Model . . . . .	444
	Figure 91: Activate Pseudowire Service (CESOP) . . . . .	446
<b>Chapter 15</b>	<b>Managing Network Element Alarms . . . . .</b>	<b>457</b>
	Figure 92: Alarm Table View . . . . .	458
<b>Chapter 17</b>	<b>Managing Reports . . . . .</b>	<b>489</b>
	Figure 93: PSM Client Communication Timeout . . . . .	504
<b>Chapter 18</b>	<b>Performance Monitoring . . . . .</b>	<b>507</b>
	Figure 94: Real-time PMs Port View . . . . .	511
	Figure 95: Real-time PMs OSC View . . . . .	511
	Figure 96: Real-time PMs Service Channel View . . . . .	512
	Figure 97: Real-time PMs All Channels View . . . . .	512
	Figure 98: Real-time PMs Port View Graph . . . . .	513
	Figure 99: Real-time PMs OSC View Graph . . . . .	513
	Figure 100: Real-time PMs Service Channel View Graph . . . . .	513
	Figure 101: Real-time PMs All Channels View Graph . . . . .	514
	Figure 102: Real-time PMs Simple View . . . . .	518
	Figure 103: Real-time PMs Simple View Graph . . . . .	519
	Figure 104: Real-time PMs Detailed View . . . . .	523
	Figure 105: Real-time PMs Simple View . . . . .	524
	Figure 106: Real-time PMs SLA View . . . . .	524
	Figure 107: Real-time PMs Port Utilization View . . . . .	524
	Figure 108: Real-time PMs Bandwidth Utilization View . . . . .	525

	Figure 109: Real-time PMs Detailed View Graph . . . . .	525
	Figure 110: Real-time PMs Simple View Graph . . . . .	525
	Figure 111: Real-time SLAs View Graph . . . . .	526
	Figure 112: Real-time PMs Port Utilization View Graph . . . . .	526
	Figure 113: Real-time PMs Bandwidth Utilization Graph . . . . .	527
	Figure 114: Real-time PMs . . . . .	530
<b>Chapter 20</b>	<b>Appendix . . . . .</b>	<b>549</b>
	Figure 115: BTI7800 Detailed Alarm Information Window (example) . . . . .	555

# List of Tables

	<b>About the Documentation</b> . . . . .	<b>xxi</b>
	Table 1: Notice Icons . . . . .	xxii
	Table 2: Text and Syntax Conventions . . . . .	xxii
<b>Chapter 1</b>	<b>proNX Service Manager</b> . . . . .	<b>27</b>
	Table 3: Replicated Data . . . . .	31
<b>Chapter 2</b>	<b>Getting Started</b> . . . . .	<b>33</b>
	Table 4: Quick Access Toolbar Buttons . . . . .	38
<b>Chapter 3</b>	<b>Managing PSM Users</b> . . . . .	<b>43</b>
	Table 5: PSM Privilege Equivalencies . . . . .	44
	Table 6: PSM Privilege Equivalencies . . . . .	47
<b>Chapter 4</b>	<b>Managing Network Discovery and Ethernet Domains</b> . . . . .	<b>51</b>
	Table 7: Discovery Criteria . . . . .	52
	Table 8: Scheduler Tab . . . . .	62
<b>Chapter 5</b>	<b>Managing Network Topology</b> . . . . .	<b>63</b>
	Table 9: Topology Map Icons . . . . .	63
	Table 10: Service Icons . . . . .	64
	Table 11: Link Details . . . . .	70
	Table 12: When LLDP is Enabled and Remote ID is Configured . . . . .	84
<b>Chapter 6</b>	<b>Working with Network Elements</b> . . . . .	<b>95</b>
	Table 13: System Info Tab for BTI7000 Series NE . . . . .	102
	Table 14: System Info Tab for BTI7800 Series NE . . . . .	105
	Table 15: System Info Tab for BTI800 Series NE . . . . .	106
	Table 16: System Info Tab for MX Series and PTX Series Routers and QFX Series Switches . . . . .	108
	Table 17: System Info Tab for BTI700 Series NE . . . . .	108
	Table 18: System Info Tab for OPS, EDFA, and RAMAN Devices . . . . .	110
	Table 19: System Info Tab for PSM Server . . . . .	110
<b>Chapter 8</b>	<b>Nodal Management</b> . . . . .	<b>133</b>
	Table 20: OTU Protocol Attributes . . . . .	202
	Table 21: ODU Protocol Attributes . . . . .	202
	Table 22: SONET/SDH Protocol Attributes . . . . .	202
	Table 23: Ethernet Protocol Attributes . . . . .	203
	Table 24: Fibre Channel Protocol Attributes . . . . .	203
	Table 25: Physical Attributes . . . . .	203
	Table 26: UFM6 Optical Channel (OCH) Attributes . . . . .	204
	Table 27: OTU Protocol Attributes . . . . .	208

	Table 28: ODU Protocol Attributes . . . . .	208
	Table 29: SONET/SDH Protocol Attributes . . . . .	208
	Table 30: Ethernet Protocol Attributes . . . . .	209
	Table 31: Fibre Channel Protocol Attributes . . . . .	209
	Table 32: Physical Attributes . . . . .	209
	Table 33: UFM6 Optical Channel (OCH) Attributes . . . . .	210
<b>Chapter 11</b>	<b>Managing Optical and Transport Services . . . . .</b>	<b>301</b>
	Table 34: Fields in the Activate Optical Service Dialog . . . . .	307
	Table 35: Supported Interface Endpoints for the BTI7000 Optical Service . . . . .	308
	Table 36: Fields in the Activate Optical Service Panel . . . . .	315
	Table 37: Fields in the Activate Optical Service Panel . . . . .	320
	Table 38: Supported Service Activation Endpoint . . . . .	328
	Table 39: Fields in the Activate Transport Service Dialog . . . . .	331
<b>Chapter 12</b>	<b>Managing Ethernet Services . . . . .</b>	<b>337</b>
	Table 40: Service Types . . . . .	346
	Table 41: Fields in the Service Attributes Pane . . . . .	351
	Table 42: Port-based Attributes . . . . .	357
	Table 43: Advanced Switch Attributes . . . . .	359
	Table 44: Advanced Port Attributes . . . . .	359
	Table 45: Advanced LAG Port Attributes . . . . .	362
	Table 46: Advanced LAG Member Attributes . . . . .	363
	Table 47: SLA Provisioning Constraints . . . . .	403
<b>Chapter 13</b>	<b>Managing Pseudowire Services . . . . .</b>	<b>441</b>
	Table 48: Fields in the Service Attributes Pane . . . . .	447
	Table 49: TDM Attributes . . . . .	448
	Table 50: Physical Interface Attributes (TI/EI Card Only) . . . . .	448
	Table 51: CESOP Payload Sizes . . . . .	448
<b>Chapter 15</b>	<b>Managing Network Element Alarms . . . . .</b>	<b>457</b>
	Table 52: Alarm Severity Mapping for Chassis Alarms . . . . .	458
	Table 53: Alarms Summary Bar . . . . .	467
	Table 54: Interpreting the Alarms Summary . . . . .	468
<b>Chapter 18</b>	<b>Performance Monitoring . . . . .</b>	<b>507</b>
	Table 55: BTI7000 Series Optical Service PMs . . . . .	508
	Table 56: BTI7800 Series Optical Service PMs . . . . .	509
	Table 57: BTI7800 Series Transport Service PMs . . . . .	515
	Table 58: BTI7000 Series PMs . . . . .	520
	Table 59: BTI700 Series PMs . . . . .	521
	Table 60: BTI800 Series PMs . . . . .	522
	Table 61: BTI7000 Series, BTI700 Series, BTI800 Series SLAs . . . . .	522
<b>Chapter 20</b>	<b>Appendix . . . . .</b>	<b>549</b>
	Table 62: BTI7000 Series Error Messages . . . . .	549
	Table 63: BTI700 Series Error Messages . . . . .	550
	Table 64: PSM Alarms . . . . .	551
	Table 65: BTI7800 Alarm Fields . . . . .	554
	Table 66: Physical PMs . . . . .	560

Table 67: SONET PMs . . . . .	561
Table 68: SDH PMs . . . . .	562
Table 69: OTN PMs . . . . .	563
Table 70: GE/FC/10GELAN PMs . . . . .	563
Table 71: Port PMs . . . . .	565
Table 72: OSC PMs . . . . .	566
Table 73: Wavelength Channel PMs . . . . .	567
Table 74: Physical PMs . . . . .	567
Table 75: OTN PMs . . . . .	568
Table 76: GE/10GE PMs . . . . .	569
Table 77: Ethernet L2 PMs . . . . .	569
Table 78: LAG PMs . . . . .	571
Table 79: ERPS PMs . . . . .	571
Table 80: Ethernet L2 PMs . . . . .	573
Table 81: Physical PMs . . . . .	574
Table 82: GE Layer 1 PMs . . . . .	575
Table 83: Ethernet L2 PMs . . . . .	575
Table 84: Optics PMs . . . . .	576
Table 85: OTU PMs . . . . .	577
Table 86: ODU PMs . . . . .	577
Table 87: Common Regex Constructs . . . . .	578





# About the Documentation

- Documentation and Release Notes on page xxi
- Documentation Conventions on page xxi
- Documentation Feedback on page xxiii
- Requesting Technical Support on page xxiv

## Documentation and Release Notes

---

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at <https://www.juniper.net/documentation/>.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at <https://www.juniper.net/books>.

## Documentation Conventions

---

Table 1 on page xxii defines notice icons used in this guide.

Table 1: Notice Icons







Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Table 2 on page xxii defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
<b>Bold text like this</b>	Represents text that you type.	To enter configuration mode, type the <b>configure</b> command:  user@host> <b>configure</b>
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> <b>show chassis alarms</b>  No alarms currently active
<i>Italic text like this</i>	<ul style="list-style-type: none"> <li>Introduces or emphasizes important new terms.</li> <li>Identifies guide names.</li> <li>Identifies RFC and Internet draft titles.</li> </ul>	<ul style="list-style-type: none"> <li>A policy <i>term</i> is a named structure that defines match conditions and actions.</li> <li><i>Junos OS CLI User Guide</i></li> <li>RFC 1997, <i>BGP Communities Attribute</i></li> </ul>
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name:  [edit] root@# <b>set system domain-name</b> <i>domain-name</i>

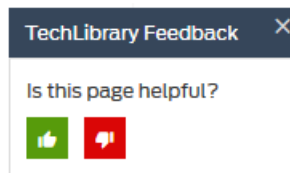
Table 2: Text and Syntax Conventions (continued)

Convention	Description	Examples
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"><li>To configure a stub area, include the <b>stub</b> statement at the <b>[edit protocols ospf area area-id]</b> hierarchy level.</li><li>The console port is labeled <b>CONSOLE</b>.</li></ul>
< > (angle brackets)	Encloses optional keywords or variables.	<b>stub &lt;default-metric <i>metric</i>&gt;;</b>
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	<b>broadcast   multicast</b>  <b>(<i>string1</i>   <i>string2</i>   <i>string3</i>)</b>
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	<b>rsvp { # Required for dynamic MPLS only</b>
[ ] (square brackets)	Encloses a variable for which you can substitute one or more values.	<b>community name members [ <i>community-ids</i> ]</b>
Indentation and braces ( { } )	Identifies a level in the configuration hierarchy.	<pre>[edit] routing-options {   static {     route default {       nexthop <i>address</i>;       retain;     }   } }</pre>
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"><li>In the Logical Interfaces box, select <b>All Interfaces</b>.</li><li>To cancel the configuration, click <b>Cancel</b>.</li></ul>
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select <b>Protocols&gt;Ospf</b> .

## Documentation Feedback

We encourage you to provide feedback so that we can improve our documentation. You can use either of the following methods:

- Online feedback system—Click TechLibrary Feedback, on the lower right of any page on the [Juniper Networks TechLibrary](#) site, and do one of the following:



- Click the thumbs-up icon if the information on the page was helpful to you.
- Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide feedback.
- E-mail—Send your comments to [techpubs-comments@juniper.net](mailto:techpubs-comments@juniper.net). Include the document or topic name, URL or page number, and software version (if applicable).

## Requesting Technical Support

---

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <https://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

## Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <https://www.juniper.net/customers/support/>
- Search for known bugs: <https://prsearch.juniper.net/>
- Find product documentation: <https://www.juniper.net/documentation/>
- Find solutions and answer questions using our Knowledge Base: <https://kb.juniper.net/>
- Download the latest versions of software and review release notes: <https://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://kb.juniper.net/InfoCenter/>

- Join and participate in the Juniper Networks Community Forum:  
<https://www.juniper.net/company/communities/>
- Create a service request online: <https://myjuniper.juniper.net>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://entitlementsearch.juniper.net/entitlementsearch/>

## Creating a Service Request with JTAC

You can create a service request with JTAC on the Web or by telephone.

- Visit <https://myjuniper.juniper.net>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <https://support.juniper.net/support/requesting-support/>.



## CHAPTER 1

# proNX Service Manager

- [About PSM on page 27](#)
- [PSM Overview on page 28](#)
- [Running with Multiple Servers on page 29](#)
- [Supported Network Elements on page 32](#)

## About PSM

---

The proNX Service Manager (PSM) provides comprehensive service provisioning, monitoring, and troubleshooting tools to allow you to efficiently manage network resources in a packet optical network. With its service-centric focus, PSM simplifies network operations and increases operational efficiency in tasks such as visualization and activation of services to troubleshooting and supporting end customers.

PSM is Java-based and uses a client-server architecture.

### PSM Client

The PSM client is a Java-based GUI that communicates with the PSM server using an HTTPS-based protocol to provide the full functionality of the proNX Service Manager. The PSM client software runs on the desktop or laptop of the technician or NOC staff.

### PSM Dashboard

The PSM Dashboard is a thin HTTPS Web-based client that is used to provide a quick view of the health of the managed network. It offers a subset of the functionality of the PSM client and runs on the desktop or laptop of the technician or NOC staff. The PSM Dashboard runs on supported browsers and does not require client software. For more information on the PSM Dashboard, see the *proNX Service Manager Dashboard User Guide*.

### PSM Server

The PSM server communicates with network elements using SNMP or NETCONF and runs on Red Hat (CentOS) Linux on standard x86-64 servers. PSM clients and PSM Dashboard users connect to the PSM server to manage the network elements in the network.

The number of clients and nodes supported is determined by the hardware, and a calculator is available to determine the correct hardware for specific deployments.

The PSM server has the following components:

- One or more Java-based processes (depending on the performance requirements of the platform)
- MySQL database (automatically backed up daily)

## Red Hat (CentOS) Linux

The PSM server is supported on Red Hat (CentOS) Linux. To facilitate configuration of the operating system, the PSM ISO includes a setup script that configures Red Hat (CentOS) Linux and installs the software packages required by the PSM server. For information on how to use this setup script to configure Red Hat (CentOS) Linux, see *Installing and Configuring Red Hat (CentOS) Linux*.

## Support for RADIUS Server

Included in the PSM server software package is a local instance of a RADIUS server implementation. When PSM is installed, the PSM server is configured by default to use this local RADIUS server to provide authentication and authorization mechanisms for access to PSM features.

## PSM Overview

---

The PSM server manages network elements using SNMP and NETCONF. The PSM client and the PSM Dashboard provide you with the user interface to interact with the PSM server.

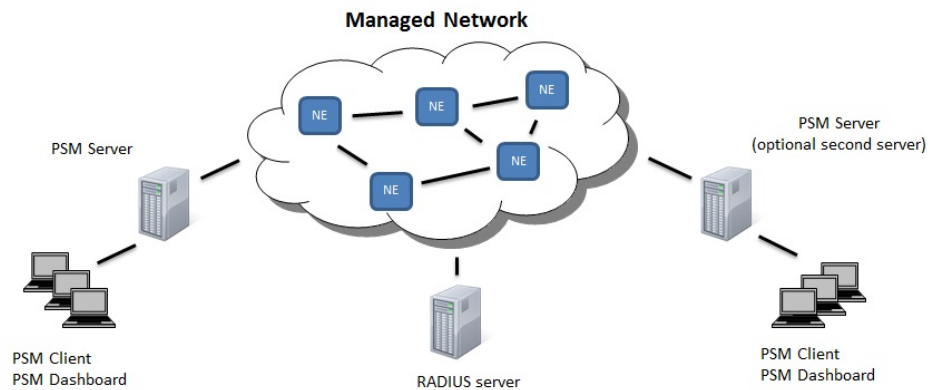
In the PSM paradigm, network element configuration data resides solely on the network elements themselves. The PSM server does not keep a separate network element configuration database. This absence of a centralized database allows PSM to achieve better scaling and better concurrency.

When management systems operate directly on configuration data stored on the network elements, there is added assurance that the data is accurate and up to date. Because there is only one set of data, issues with synchronizing an external copy of the data with the actual data on the network element do not exist. Furthermore, since the actual data is manipulated directly, it is a simple matter for the management software to detect and handle situations where multiple users attempt to make conflicting changes, regardless of whether the conflicting users are using the CLI, a separate nodal manager, or other PSM servers.

[Figure 1 on page 29](#) shows a network managed by two PSM servers and multiple clients, along with an external RADIUS server.



Figure 1: PSM Managed Network



When a server comes up, it registers itself as a trap listener on all network elements it is told to discover. It then receives traps from, and reports on, these network elements, and draws topology and discovers services based on configuration and operational data it reads from these network elements. This information is then made available to PSM clients that log in to this server. Clients logging in to a different server might see different network elements altogether, depending on what this other server is configured to discover.

## Running with Multiple Servers

- [Overview on page 29](#)
- [Running Multiple Servers Without Server Replication on page 30](#)
- [Running Multiple Servers with Server Replication on page 30](#)

### Overview

To provide a level of redundancy, PSM supports the use of multiple servers to manage a network.

In a multi-server configuration, each server receives traps from, and reports on, the network elements that it has discovered. The set of discovered network elements can be the same or can be different from server to server, depending purely on how you choose to divide your network for management. The servers can be geographically distinct for better disaster recovery or be part of a geographically-based management scheme.



**NOTE:** Some BTI Series network elements have limits on the number of PSM servers that can be used to manage them. See *PSM Server Requirements* for details.

Since the servers operate directly on configuration data stored on the network elements themselves, each server has the latest view, and is able to detect and recover from

conflicts (in the unlikely event that two or more servers are changing the same set of attributes on the same network element).

While the PSM server does not store network element configuration data, it does store configuration data associated with the PSM server itself. This PSM configuration data relates to user interface interactions and the presentation of information, and includes the following:

- users for the server
- the list of network elements to discover and domain/group membership, which relate to what network elements to manage and how they are organized
- alarm assignment/acknowledgment and maintenance modes, which relate to management actions that a user can take
- customer details and association, which can be optionally defined and associated with services
- profiles, which are network-wide to provide consistency across network elements
- various options related to the display of data, the locations of tools, and other attributes specific to the server

The PSM server stores this set of information in the local MySQL database, which is set up and initialized during the PSM server installation process, and which persists through PSM server software upgrades.

How this data behaves when you run with multiple servers depends on whether you choose to run these servers independently (without server replication), or loosely coupled (with server replication).

## Running Multiple Servers Without Server Replication

When you run multiple servers without server replication, each server is unaware of the other servers, and each has its own set of PSM configuration data.

The PSM configuration data that resides on the PSM server is not replicated nor synchronized with the PSM configuration data on the other servers.

For example, network element groups created on one server are not visible to the other servers, alarm assignment on one server is not visible to the other servers, and so forth.

With this approach, while you still achieve redundancy, you might have to recreate and/or reconcile your PSM configuration data when a server goes down.

## Running Multiple Servers with Server Replication

When you run multiple servers with server replication, some of the PSM configuration data is synchronized among all servers within the same server replication cluster. This data subset is called the replicated data.

Updates to the replicated data on one server are automatically conveyed to all other servers in the same cluster. For example, a network element group created on one server automatically appears on the other servers, an alarm assignment on one server

automatically appears on the other servers, and so forth. In this way, when a server goes down, you can simply log in to another server and continue working.

When enabling server replication on a server, you must explicitly specify the list of servers that belong to the same server replication cluster. A server replication cluster is a group of servers whose replicated data is synchronized among all its members. Not all servers in the network need to belong to the same server replication cluster. You can have more than one server replication cluster in the network.

When a server configured for server replication comes up, it seeks out other members in the cluster and retrieves their replicated data. The server then overwrites its own replicated data with the retrieved replicated data. In other words, the first server that comes up is assumed to possess the correct replicated data. Servers that come up subsequently acquire and adopt this replicated data, which ultimately comes from the first server. Once all servers are up, the relationship between servers is peer-to-peer. Changes made on one server are automatically multicasted to the other servers. Each server will always have the up-to-date view.

[Table 3 on page 31](#) presents a high level view of what PSM configuration data is replicated and what is not replicated. Items not in this list are also not replicated. More details on this replicated data are provided in the respective sections of this guide.

**Table 3: Replicated Data**

PSM configuration data	Replicated
NEs to discover	No  To support geographically-based management schemes, NE discovery is not replicated.
NE maintenance mode	Yes
NE group membership and group attributes	Yes
Ethernet domain membership	Yes
Acknowledged and/or assigned alarms	Yes
Customer information and customer-to-service mapping	Yes
Profile templates	Yes
Users	Yes  In order for user replication to work correctly, all servers in a cluster must use the same RADIUS server for authentication.
Various PSM user preferences and options that relate to the display and presentation of information	No

For information on how to configure server replication, see *Configuring Server Replication*.

## Supported Network Elements

---

You can use the proNX Service Manager to manage the following Juniper Networks devices:

- BTI7800 Series
- BTI7000 Series
- BTI800 Series
- BTI700 Series
- MX Series and PTX Series routers (basic support)
- QFX Series switches (basic support)

Management capabilities and device response vary depending on the device. Differences in support or behavior are stated in the respective procedures in this document.

The proNX Service Manager provides basic support for Juniper Networks MX Series and PTX Series routers and QFX Series switches. This includes basic discovery and retrieval of system information, alarm management, inventory, log collection, report generation, performance monitoring, and software configuration backup and restore.

Additionally, the proNX Service Manager supports the ability to configure a BTI7000 Series optical service with endpoints on select interfaces on MX Series and PTX Series routers and QFX Series switches. For more information, see [“Activating an Optical Service Between Transponder Interface Endpoints” on page 308](#).

To obtain a detailed list of all supported devices, see [“Viewing the List Of Supported Devices” on page 40](#).

To see what network element software releases are supported, see the *proNX Service Manager Release Notes*.

## CHAPTER 2

# Getting Started

- [Starting the PSM Client on page 33](#)
- [PSM Client Navigation on page 36](#)
- [Working with the PSM Client Window System on page 36](#)
- [Customizing the Quick Access Toolbar on page 38](#)
- [Displaying the Online Help on page 40](#)
- [Viewing the List Of Supported Devices on page 40](#)

### Starting the PSM Client

---

Use this procedure to start the PSM client on Windows, Linux, or OS X.

Before you can perform this procedure, you must install the client software. Refer to *Installing the PSM Client Using the Wizard* or *Installing the PSM Client Manually* for instructions on installing the client.

1. Launch the **psmclient** executable file as follows:

- Windows: navigate to the **bin** folder within the PSM client installation folder and double-click the **psmclient.exe** file. Alternatively launch the client from the Desktop icon or Start menu entry created by the PSM client installer.
- OS X or Linux: open a terminal window, navigate to the PSM client installation directory and launch from the command line: **bin/psmclient**. Alternatively launch the client from the Desktop icon created by the PSM client installer.

The PSM installation starts by displaying the splash screen.

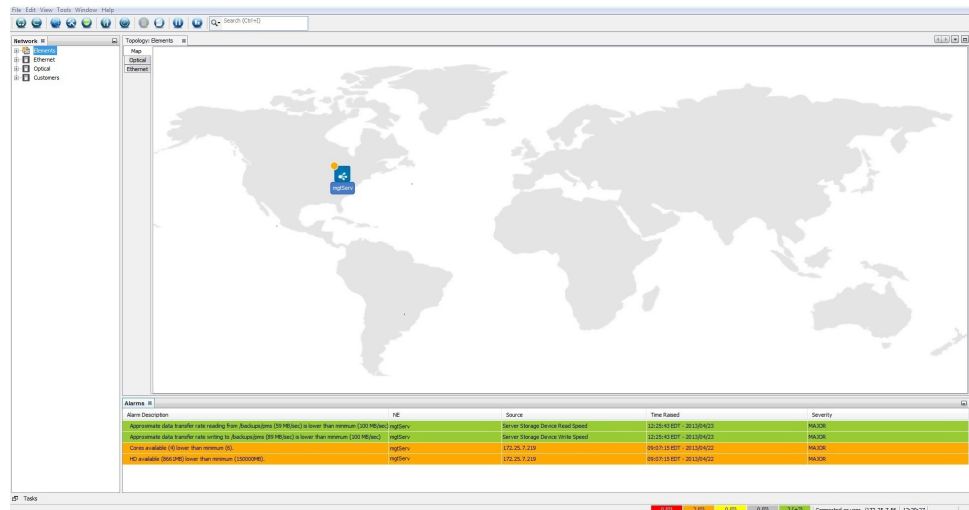


Then PSM displays the login screen.



2. In the **Server** field, enter the IP address for the PSM server, or choose a previously used server from the drop-down menu.
3. Enter the **Username** and **Password**.
4. Click **Login**.

After successful login, the PSM client navigation window is displayed. The following screen shows a newly installed server with no pre-discovered network elements.

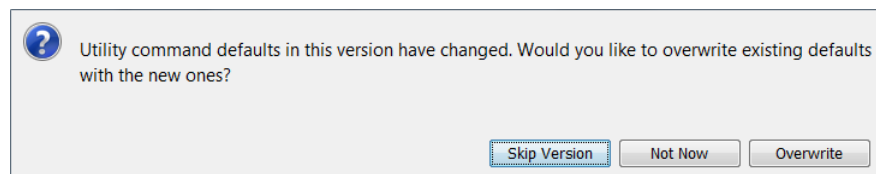


A "Connected to Server" indication is displayed in the lower right corner of the window. If connectivity to the server is lost, this changes to a "Connection to Server Lost" indication.



**NOTE:** Depending on the frequency with which the client and server check the path, it might take several minutes for a loss of connectivity to be detected and displayed.

If Juniper Networks has updated the utility software, you might see the following dialog in certain situations:



The utility software is the software defined in **Tools > Options > Utilities**. Choose:

- **Overwrite** if you have not changed any of the Type or Version **Default** settings. Choosing this option only overwrites the **Default** settings, and does not affect or overwrite the Type or Version-specific settings.
- **Not Now** if you have changed the **Default** settings and you want to save them before you overwrite them. To save the current **Default** settings, select **Tools > Options > Utilities** and click **Export** to save the settings (including the **Default** settings) to a zipped file. The **Default** settings can be found in `config\Preferences\com\btisystems\pronx\ems\client\preferences.properties` in the exported file. After you save the **Default** settings, re-launch the PSM client and choose **Overwrite** in the dialog.
- **Skip Versions** only if instructed to do so by Juniper Networks Support.

This procedure is complete.

## PSM Client Navigation

The proNX Service Manager client offers point-and-click navigation. The main entry screen is structured as shown in the following figure.

*Figure 2: Top Level Screen Layout for proNX Service Manager*



- Panel A provides information in a tree. Selecting an item from the tree has the effect of placing the information in other panels in context of the selection. In most situations, you will work with the Network tree panel, which lists network elements under management, services, and other information. You can expand the network elements in the tree to see their components. If the Network tree panel is closed, you can re-open it by selecting **View >Network >Network**.
- Panel B is the main panel where you perform most of your tasks. It provides a graphical view of network elements, services, and topology, and presents the configuration screens needed for your task.
- Panel C provides a detailed list of alarms, tasks or output (generated reports) depending on which tab in the lower left corner you select.
- Panel D provides a menu-based tool bar to access all of the PSM functions, and a quick access tool bar with buttons to access the common functions.



**NOTE:** The panels can be resized, minimized, closed, undocked, or moved. To return to the initial view, select **Window >Reset Windows**.

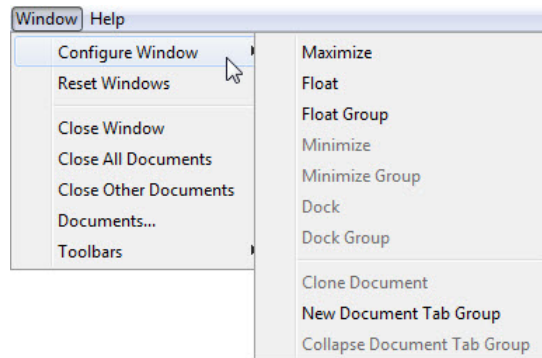
## Working with the PSM Client Window System

Use this procedure to dock, float (undock), maximize, minimize, drag-and-drop, or manipulate a window.

The PSM window system lets you maximize/minimize, dock/undock, and drag-and-drop windows. The PSM client leverages Java Swing, which is the standard UI toolkit on the Java desktop, and is used throughout the PSM client platform. This solution allows the portability of GUI components across all operating systems allowing Juniper Networks to offer the PSM client on common operating systems.

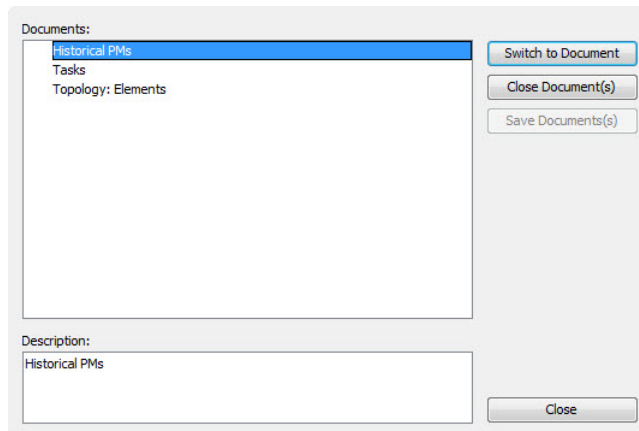


1. To dock, float, maximize or minimize a window, click inside the window and select **Window >Configure Window** from the main menu.



- a. Select **Maximize** to maximize the window. Clear it to restore the window to its regular size.
  - b. Select **Float** to undock the window. If the window has tabs, then this undocks the current tab.
  - c. Select **Float Group** to undock the window with all tabs intact.
  - d. Select **Minimize** to minimize the window.
  - e. Select **Dock** to dock the window.
  - f. Select **Dock Group** to dock the window with all tabs intact.
  - g. Select **New Document Tab Group** to create a new tab group in the current window. The current window is split into two side-by-side panels, with each panel having its own set of tabs.
  - h. Select **Collapse Document Tab Group** to combine the two tab groups back into one panel.
2. To drag-and-drop a window, click the tab that you want to move, and drag and drop it in another window.  
As you drag the tab, you will see a changing red outline showing the target window. Once the desired destination is outlined in red, release the mouse.
  3. To reset the windows back to their initial configuration, select **Window >Reset Windows**.
  4. To close the current window, select **Window >Close Window**, or simply click the x on the right side of the tab.
  5. To close the current window and all its tabs, select **Window >Close All Documents**.

6. To close all tabs in the current window except for the current tab, select **Window >Close Other Documents**.
7. To bring up the **Documents** dialog, select **Window >Documents....**



- a. To switch to a specific window, highlight its entry and select **Switch to Document**.
- b. To close a specific window, highlight its entry and select **Close Document(s)**.

## Customizing the Quick Access Toolbar

Use this procedure to customize the quick access toolbar.

The quick access toolbar is found at the top of the client display, and can be used to launch common tasks.

The following table lists the initial shortcut buttons on the toolbar. The toolbar can be customized with more or fewer buttons. The buttons provide a way to quickly access functions that are also available from the menu toolbar. A tool tip and in some cases, a shortcut key sequence, are displayed when you hover the mouse over a button.

**Table 4: Quick Access Toolbar Buttons**












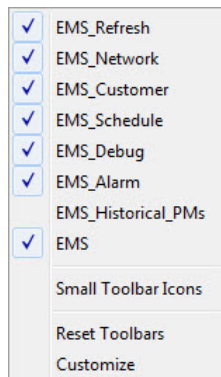
Button	Function
	<p>Refresh from Server</p> <p>The PSM client and the PSM server communicate at regular intervals to ensure the client has the most recent view of the network. Additionally, the server updates the client automatically when the server detects changes in the managed network. The <b>Refresh from Server</b> button provides a manual way for you to force the PSM client to request (and refresh itself with) the latest PSM server data.</p>

Table 4: Quick Access Toolbar Buttons (continued)

Button	Function
	<p>Resync Network</p> <p>The PSM server and the network elements that it manages communicate at regular intervals to ensure the server has the most recent view of the network. Additionally, the managed network elements update the server automatically when changes occur. The <b>Resync Network</b> button provides a manual way for you to force the PSM server to resynchronize itself with the managed network elements.</p>
	<p>Network Element Discovery</p> <p><a href="#">“Discovering Network Elements” on page 51</a></p>
	<p>Service Activation</p> <p><a href="#">“Activating an Optical Service in a BT17000 Network” on page 306</a></p> <p><a href="#">“Activating an Optical Service in a BT17800 Network” on page 319</a></p> <p><a href="#">“Activating a Transport Service” on page 328</a></p> <p><a href="#">“Activating an Ethernet Service” on page 348</a></p> <p><a href="#">“Activating a Pseudowire Service” on page 445</a></p>
	<p>Profile Manager</p> <p><a href="#">“Managing Profiles” on page 426</a></p>
	<p>Add Customer</p> <p><a href="#">“Adding a Customer” on page 454</a></p>
	<p>Schedule List</p> <p><a href="#">“Scheduling Network Element Discoveries” on page 57</a></p>
	<p>Save Configuration</p> <p><a href="#">“Saving Network Element Configuration Information” on page 545</a></p>
	<p>Archive Logs</p> <p><a href="#">“Exporting Client and Server Logs” on page 539</a></p>
	<p>Suspend Alarm Notifications</p> <p><a href="#">“Working with the Alarms Table” on page 462</a></p>
	<p>Historical PMs</p> <p><a href="#">“Collecting and Viewing Historical PMs” on page 531</a></p>

To customize the quick access toolbar:

1. Select **Window > Toolbars** from the main menu, or right-click the area to the right of the quick access toolbar.



- a. Click to toggle entries from the list of standard quick access buttons.
- b. To use the smaller toolbar icons, select **Small Toolbar Icons**. To use the regular toolbar icons, clear **Small Toolbar Icons**.
- c. To reset the toolbar to the initial setting, choose **Reset Toolbars**.
- d. To add other buttons or to create a new toolbar, choose **Customize** and select the buttons you want to be shown.

## Displaying the Online Help

---

Use this procedure to display the PSM online Help.

1. Select **Help > Open Help**.

The online Help is launched in your default Web browser.

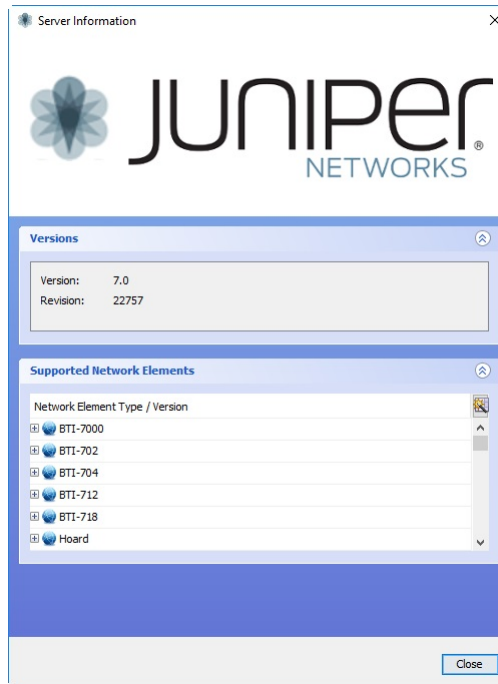
## Viewing the List Of Supported Devices

---

Use this procedure to view the list of devices supported by the proNX Service Manager.

1. From the top menu bar, select **Help > Server Info**.

The list of supported devices and their software releases are shown in the **Supported Network Elements** pane. For example:



2. To see the list of software versions supported for each device, expand the device type in the **Supported Network Elements** pane.



**NOTE:** See the *proNX Service Manager Release Notes* for the most up-to-date list of device software releases supported.

3. Use the scroll bar on the right side of the pane to scroll through the list of devices and versions supported.



## CHAPTER 3

# Managing PSM Users

- [Introduction on page 43](#)
- [Adding a User on page 44](#)
- [Modifying a User on page 46](#)
- [Deleting a User on page 49](#)
- [Editing User Attributes on the Local RADIUS Server on page 49](#)

## Introduction

---

PSM performs user authentication using either the local pre-packaged RADIUS server or external RADIUS servers. By default, PSM is configured to use the local pre-packaged RADIUS server.

To help you work with the local RADIUS server, PSM provides you with an interface to add, modify and delete users from the local RADIUS server database. This capability to make changes to the local RADIUS server database is supported even if you are not using the local RADIUS server for authentication. In this latter case, the changes have no effect on authentication, but are still applicable for creating users for tasks like assigning an alarm to a user.

You cannot use PSM to add, modify, or delete users from external RADIUS servers. An external RADIUS server is any RADIUS server that is not the local, co-resident RADIUS server. Note that the local, co-resident RADIUS server can act as an external RADIUS server to other PSM servers.

The above is true even if you run with server replication. When you run with server replication, you also cannot add, modify, or delete users from external RADIUS servers. In order to add, modify, or delete users, you must be logged in to the PSM server on which the RADIUS server is running.



**NOTE:** It is recommended that the same PSM login credentials (username and password) be added to the network elements under management. Some PSM tasks (including using the network element CLI) require the server to log in to the network element using the PSM user's login credentials.

For information on configuring PSM to work with RADIUS servers (local or external), see *RADIUS on PSM*.

## Adding a User

Use this procedure to add a user to the local RADIUS server database.

PSM provides you with an interface to add users to the local RADIUS server database. You cannot use this procedure to add a user to an external RADIUS server database. An external RADIUS server is any RADIUS server that is not the local, co-resident RADIUS server. Note that the local, co-resident RADIUS server can act as an external RADIUS server to other PSM servers.

The local co-resident RADIUS server can be used by both PSM and network elements for authentication and authorization of the same users. Since the privilege definitions for PSM and the network elements might differ, PSM automatically adds a set of equivalent privileges to the RADIUS database for that user ([Table 5 on page 44](#)). For example, if you add a user with the **NOC** privilege, PSM automatically configures the user with the equivalent **surveillance** and **viewer** privileges as well.

*Table 5: PSM Privilege Equivalencies*

PSM privileges	BTI7000, BTI7800 privileges	BTI800 privileges
Administrator	superuser	admin
Service Provider	provisioning	operator
NOC	surveillance	viewer



**NOTE:** You can always bypass PSM and add users to the local RADIUS database directly through the interface provided by the RADIUS server. If you do this, the users can still be modified in PSM.



To add a user:

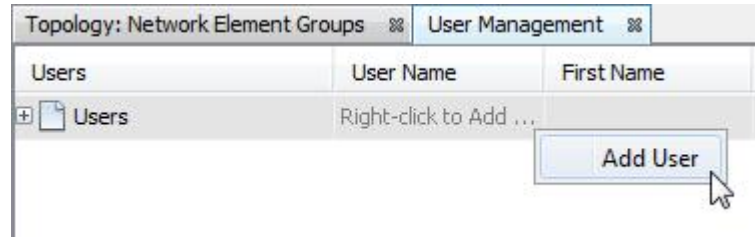
1. Choose **Edit > User Management** from the main menu.

The **User Management** window appears.

Topology: Elements Alarms Tasks User Management								
Users	User Name	First Name	Last Name	Email	Telephone Number	Role	Creation Date	Locally Managed User
Users	Right-click to A...							
user	user					Administr...	2013/12/13 12:57...	Yes

The Locally Managed User column indicates whether the user is in the local RADIUS server database (**yes**) or in another RADIUS server database (**no**). Users configured in an external RADIUS server appear in this list if PSM is using an external RADIUS server for authentication.

2. Right-click the **Users** row and choose **Add User**.



The **Add User** dialog box is displayed.

Add User

Username:

Password:

Confirm Password:

Role:

Administrator

First Name:

Last Name:

Email:

Telephone:

Cancel

OK

3. In the **Add User** dialog box, specify the following information.

- Username
- Password, can consist of alphanumeric characters and the following special characters:

! @ # \$ % ^ & ( ) \_ + [ ] { } . ~

- Confirm Password
  - Role, one of:
    - Administrator - this role has complete access to all functions
    - Service Provider - this role allows the user to create services, and has the following limitations:
      - The Service Provider role can read, create, and update everything, except device discoveries and scheduled device discoveries
      - The Service Provider role cannot create new users.
      - The Service Provider role can update its own user record, but no other user records. It also cannot change its own role.
      - The Service Provider role cannot move network element group members.
      - The Service Provider role cannot delete anything except for Bandwidth Profile Templates, Class Map Profile Templates, Service Policy (and Map) Profile Templates, and Customers.
    - NOC - this role provides read-only access
  - First name of the user (optional)
  - Last name of the user(optional)
  - Email address for the user (optional)
  - Telephone number for the user (optional)
4. Click **OK**.

The user is added to the local RADIUS server database.

---

## Modifying a User

Use this procedure to edit a user in the local RADIUS server database.

PSM provides you with an interface to modify users in the local RADIUS server database. You cannot use this procedure to add a user to an external RADIUS server database. An external RADIUS server is any RADIUS server that is not the local, co-resident RADIUS server. Note that the local, co-resident RADIUS server can act as an external RADIUS server to other PSM servers.

The local co-resident RADIUS server can be used by both PSM and network elements for authentication and authorization of the same users. Since the privilege definitions for PSM and the network elements might differ, PSM automatically adds a set of equivalent privileges to the RADIUS database for that user ([Table 6 on page 47](#)). For example, if you set a user's privilege to **NOC**, PSM automatically configures the RADIUS server with the equivalent **surveillance** and **viewer** privileges as well.

Table 6: PSM Privilege Equivalencies

PSM privileges	BTI7000, BTI7800 privileges	BTI800 privileges
Administrator	superuser	admin
Service Provider	provisioning	operator
NOC	surveillance	viewer



**NOTE:** You can always bypass PSM and edit users in the local RADIUS server database directly through the interface provided by the RADIUS server.

To modify a user:

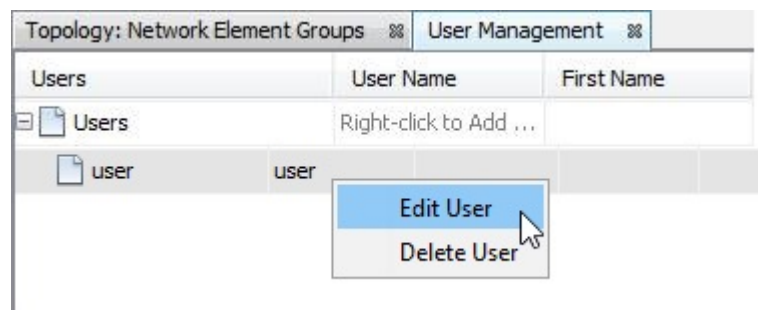
1. Choose **Edit >User Management** from the main menu.

The **User Management** window appears.

Topology: Elements Alarms Tasks User Management								
Users	User Name	First Name	Last Name	Email	Telephone Number	Role	Creation Date	Locally Managed User
Users	Right-click to A...							
user	user					Administr...	2013/12/13 12:57...	Yes

The Locally Managed User column indicates whether the user is in the local RADIUS server database (**yes**) or in another RADIUS server database (**no**). Users configured in an external RADIUS server appear in this list if PSM is using an external RADIUS server for authentication. You can use this procedure to edit locally managed users only.

2. Right-click the desired user's row and choose **Edit User**.



The **Edit User** dialog box is displayed.

3. In the **Edit User** dialog box, specify the following information as necessary.

- Username - this cannot be changed. To change the user name, you must create a new user with the desired name.
- Password, can consist of alphanumeric characters and the following special characters:

! @ # \$ % ^ & ( ) \_ + [ ] { } . ~

- Confirm Password
- Role, one of:
  - Administrator - this role has complete access to all functions
  - Service Provider - this role allows the user to create services, and has the following limitations:
    - The Service Provider role can read, create, and update everything, except device discoveries and scheduled device discoveries
    - The Service Provider role cannot create new users.
    - The Service Provider role can update its own user record, but no other user records. It also cannot change its own role.
    - The Service Provider role cannot move network element group members.
    - The Service Provider role cannot delete anything except for Bandwidth Profile Templates, Class Map Profile Templates, Service Policy (and Map) Profile Templates, and Customers.
  - NOC - this role provides read-only access
- First name of the user (optional)
- Last name of the user(optional)

- Email address for the user (optional)
  - Telephone number for the user(optional)
4. Click **OK**.

## Deleting a User

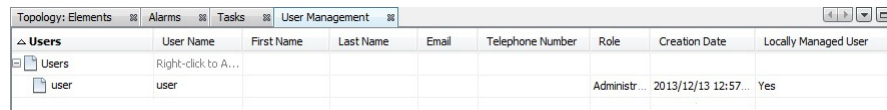
Use this procedure to delete a user from the local RADIUS server database.

You cannot use this procedure to delete users from an external RADIUS server database. An external RADIUS server is any RADIUS server that is not the local, co-resident RADIUS server. Note that the local, co-resident RADIUS server can act as an external RADIUS server to other PSM Servers.

To delete a user:

1. Choose **Edit >User Management** from the main menu.

The **User Management** window appears.

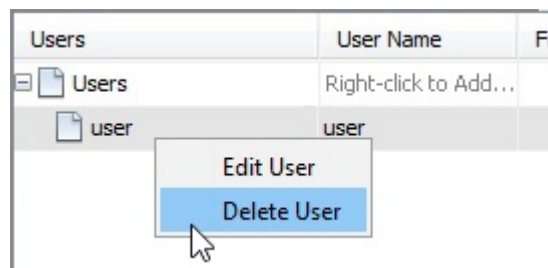


	User Name	First Name	Last Name	Email	Telephone Number	Role	Creation Date	Locally Managed User
Users	Right-click to Add...							
user	user					Administr...	2013/12/13 12:57...	Yes



**NOTE:** The **Locally Managed User** column indicates whether the user is in the local RADIUS server database (yes) or in an external RADIUS server database (no). You can only delete locally managed users.

2. Right-click the desired user's row and choose **Delete User**.



3. In the **Confirm User Deletion** dialog box, click **OK**.

The user is deleted from the local RADIUS server database.


## Editing User Attributes on the Local RADIUS Server

Use this procedure to set the idle timeout value for the user's CLI session.

If the user's CLI session is idle for the specified time, the user is automatically logged out. This attribute governs the CLI session only, and does not affect the user's PSM client session.

1. Select **Edit >Radius Attributes** from the main menu bar.

The **Radius Attributes** window appears.

Topology: Elements x User Management x Radius Attributes x			
Username	Attribute	Operation	Value
 user	Idle-Timeout	EQUAL	60

2. Right-click the user you want to edit and select **Edit Radius Attribute**.

The **Edit Radius Attribute** dialog appears.

Edit Radius Attribute

X

Username: user

Attribute: Idle-Timeout

Operation: EQUAL

Value: 60 secs

Cancel

OK

3. Set the idle timeout value.
4. Click **OK**.

## CHAPTER 4

# Managing Network Discovery and Ethernet Domains

- [Introduction on page 51](#)
- [Discovering Network Elements on page 51](#)
- [Undiscovering a Network Element on page 55](#)
- [Rediscovering a Network Element on page 55](#)
- [Polling Discovered Network Elements on page 55](#)
- [Ethernet Network Domains on page 56](#)
- [Scheduling Network Element Discoveries on page 57](#)

## Introduction

---

The first step to managing a network is to discover the network elements you want to manage. During discovery, PSM registers itself as a trap receiver and reads configuration and operational data from the network element. Discovered network elements are shown in the topology Map view. PSM uses SNMP (and NETCONF if applicable) to communicate with discovered network elements.

PSM supports the discovery of the following network elements:

- BTI7800 Series network elements
- BTI7000 Series network elements
- BTI800 Series network elements
- BTI700 Series network elements
- MX Series and PTX Series routers
- QFX Series switches

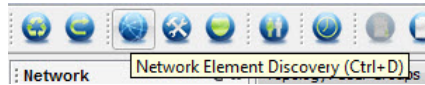
Additionally, PSM can discover any SNMP MIB-II compliant device.

## Discovering Network Elements

---

Use this procedure to discover network elements in the network you want to manage.

1. Select the **Network Element Discovery** button on the toolbar or choose **Tools > Network Element Discovery** from the menu.



The **Network Element Discovery** window is displayed, as shown below.

A screenshot of the 'Network Element Discovery' dialog box. It has a title bar and a main area with several sections: 'Discovery' with a text field for 'Discovery Criteria' and a dropdown for 'Management Domain'; 'Telnet/NETCONF' with fields for 'Username', 'Password', and 'Port'; 'SNMP' with fields for 'Write Community' and 'Port'; and 'Topology' with two checkboxes: 'Auto-Discovery of Connected Devices' and 'Configure Topology Discovery'. At the bottom are 'Cancel' and 'OK' buttons.

2. Enter the criteria with which to discover the network elements in the **Discovery Criteria** field.

**Table 7: Discovery Criteria**

Criteria	Format	Example
Group Name	Alphanumeric	Belfast
<p>The use of the group name as part of the network element discovery criteria allows you to specify a group of network elements for discovery. The group of network elements must have been previously created. See <a href="#">“Creating a New Group” on page 87</a>.</p> <p><b>NOTE:</b> Using the group name is not applicable when discovering network elements for the first time.</p>		
Host Name (DNS)	Alphanumeric	OTT-204-3



Table 7: Discovery Criteria (continued)

Criteria	Format	Example
IP address	List separated by comma or single entry	172.27.1.1, 172.27.1.2
	Address range	172.27.7.100-110
	All devices in a subnet	172.27.7.255

3. Optionally, specify the Ethernet **Management Domain**.

Domains are used when creating Ethernet services. For more information on domains, see [“Ethernet Network Domains” on page 56](#).

If you do not plan on creating Ethernet services, you do not need to specify a domain.

4. Optionally, select Automatically Configure JUNOS if you want PSM to automatically configure a Juniper Networks router or switch for NETCONF and SNMP access from PSM.

When selected, PSM configures the router or switch to accept NETCONF requests from the specified **Port** and sets the SNMP write community string to **private**.

5. Optionally, specify the NETCONF parameters if the network element you are discovering supports NETCONF.

You can specify the NETCONF **Username**, **Password**, and **Port**, or you can leave them blank to use the defaults. The defaults are set to match the defaults on the devices being managed.

6. Optionally, specify the SNMP parameters.

You can specify an SNMP **Write Community** string and a **Port**, or you can leave them blank to use the defaults. The default write community string is **private**. The default port is **161**.



**NOTE:** Because PSM uses SNMP for the initial communications with the network element, the SNMP parameters must be correct even if PSM is using NETCONF to manage the network element. Additionally, some devices require SNMP for trap server registration.

7. Optionally, select **Auto-Discovery of Connected Devices** if you want PSM to automatically discover all network elements connected to the network element you are discovering.

If you select this option, PSM will automatically discover all connected network elements in a BT17000 Series DOL network, and all connected network elements in a BT17800 Series ROADM network or a BT17800 Series transport network .

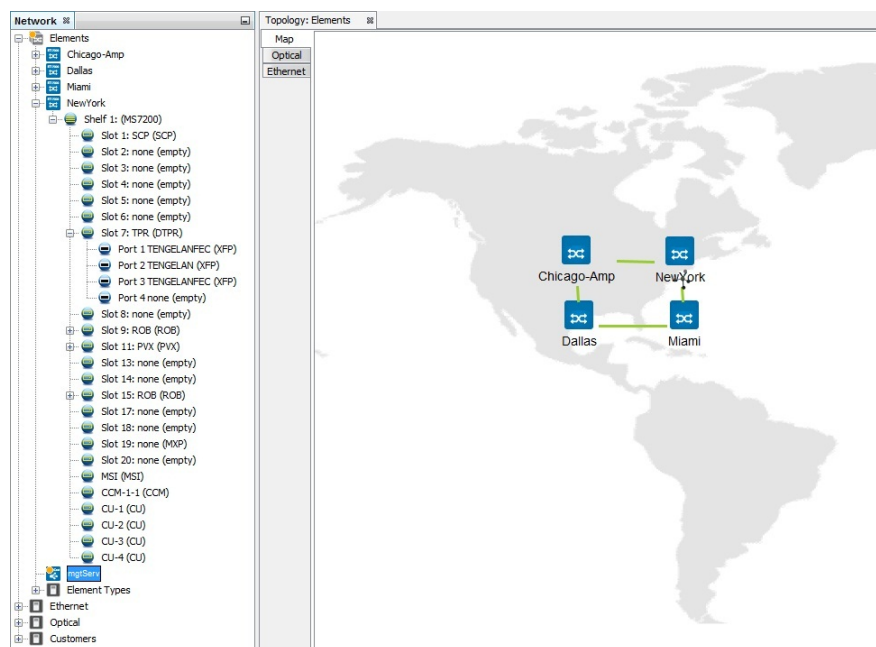
8. Optionally, select **Configure Topology Discovery** if you want to enable LLDP on the NE.

If you select this option, PSM will enable LLDP on the NE after the NE is discovered. If you do not select this option, PSM will not enable LLDP on the NE after the NE is discovered. In this latter case, the LLDP setting on the NE is left unchanged.

This setting applies to BT17000, BT1800, and BT1700 network elements only.

9. Click **OK** to start device discovery.

The following figure shows PSM when network elements are discovered successfully.



The Elements branch in the Network tree can be expanded to show all the components on the network element.


If PSM is unsuccessful in discovering a network element, the font below the network element icon is red. Common reasons for failure include invalid credentials or port numbers, or if the network element cannot be reached.



**NOTE:** The first discovery of a new network element type or version might take longer than subsequent discoveries. The reason for this is that PSM builds a database schema for each new network element type or version it encounters.

## Undiscovering a Network Element

Use this procedure to undiscover a network element.


Discovered network elements can be undiscovered, which deregisters PSM as a trap receiver and removes the network element from under PSM management. Undiscovered network elements continue to appear in PSM, but with a distinctive  icon.

1. Right-click the network element you want to undiscover and select **Discovery >Undiscover**.

The **Undiscover** confirmation dialog appears:



2. Click **OK** to confirm.

The network element is no longer under PSM management, and is shown with a  icon. You can leave the network element as is, or you can completely remove it from view.

3. To remove the NE completely from view, right-click the NE and select **Remove from Group**.

## Rediscovering a Network Element

Use this procedure to rediscover a network element.

Discovered network elements can be rediscovered, which manually forces PSM to retrieve information from the network elements being rediscovered. Rediscovering a network element is usually not required under normal situations because the network element updates PSM asynchronously with any changes as they occur.

1. Right-click the network element you want to rediscover and select **Discovery >Rediscover**.

PSM rediscovers the network element.

## Polling Discovered Network Elements

PSM supports an automatic NE polling operation that is not user configurable. The server checks IP, SNMP and/or NETCONF connectivity with each network element every 2 minutes. If the checks fail, the text beside the NE in the Network tree, and beneath the NE in the Topology Map view, turns red and the NE is declared unreachable.

## Ethernet Network Domains

---

PSM uses the concept of Ethernet network domains to support one PSM server managing more than one Ethernet network. A domain is a mechanism used to segregate network elements in diverse networks that are not interconnected, and where there is reuse of service VLAN IDs. This allows for the proper handling of reused service VLAN IDs in service visualization and activation operations.

Network elements can be added to an Ethernet domain during network element discovery. Ethernet domains are not used and do not need to be defined for optical networks.



**NOTE:** Ethernet domains are part of the replicated data set when running with multiple servers. For more information on replicated data, see [“Running Multiple Servers with Server Replication” on page 30](#).

- [Creating an Ethernet Domain on page 56](#)
- [Checking Domain Membership for a Network Element on page 57](#)

### Creating an Ethernet Domain

Use this procedure to create an Ethernet domain for an Ethernet network.

During a discovery operation, if the specified domain does not already exist, it is created, and all devices discovered during that operation are added to it. Domains appear in the **Ethernet** branch of the network tree when Ethernet services are created.

If you do not explicitly specify a domain, all devices discovered during this operation will be assigned to the **Default** domain.

1. From the main menu, choose **Tools >Network Element Discovery**.
2. Enter a name for the domain in the **Domain** field of the **Network Element Discovery** window.

The domain name is case insensitive. You must not create multiple domains where the domain names differ only in the case. For example, if you create a domain called **Belfast**, you must not create a new domain called **belfast** as this differs only in case with the existing **Belfast** domain name.

3. Enter the discovery criteria.
4. Click **OK**.

The discovered network elements are added to the new domain.



**NOTE:** Once a new domain is created, it cannot be deleted.



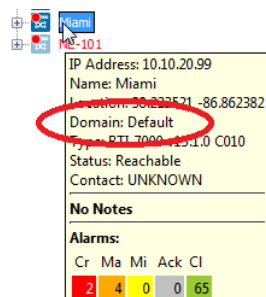
**NOTE:** To move a network element from one domain to another, simply discover the network element again and specify the desired domain. Moving NEs between domains might cause VLAN ID conflicts. If the same VLAN ID exists in two domains and an NE with one of those VLAN IDs in one domain is moved to the other domain, the services associated with the VLAN ID on the NE being moved are no longer recognized. Conflicting VLAN IDs should be resolved before NEs are moved between domains.

## Checking Domain Membership for a Network Element

Use this procedure to check what domain a network element belongs to.

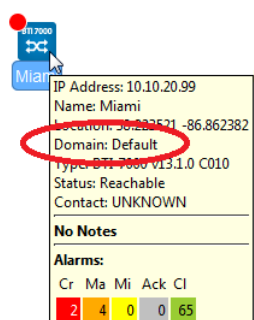
1. Hover over the network element in the Network tree.

For example:



2. Alternatively, hover over the network element in the Topology view.

For example:



## Scheduling Network Element Discoveries

You can schedule the prONX Service Manager to rediscovers network elements periodically.



**NOTE:** You do not normally need to schedule discoveries because the network elements automatically update PSM of any changes.

- [Scheduling a Network Element Discovery Task on page 58](#)
- [Viewing Scheduled Tasks on page 61](#)
- [Deleting Scheduled Tasks on page 62](#)

## Scheduling a Network Element Discovery Task

Use this procedure to schedule a discovery task for a network element.

1. From the main menu, choose **Edit > Schedules**.

The **Scheduler** window is displayed.

Topology: Network Element Groups Scheduler		
Schedules	Domain	Schedule
Discovery Schedules	Right-click to Add a schedule.	
10.1.108.1-20	Default	Scheduled from 03/16/12 8:00 AM
172.27.7.101-120	Be1fast	Scheduled from 04/01/12 7:00 AM

2. In the **Scheduler** window, right-click the **Discovery Schedules** entry in the table and choose **Add Schedule**. The **Scheduling** dialog window is displayed.

The **Network Element Discovery** dialog window is shown with the following fields and options:

- Discovery Criteria:** 10.1.213.1
- Ethernet Domain:** (empty dropdown)
- Advanced...** button

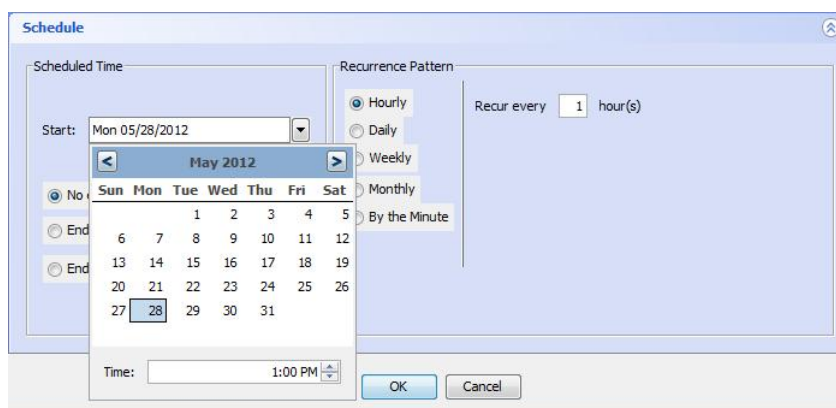
The **Schedule** sub-dialog is also visible, showing:

- Scheduled Time:**
  - Start:** Thu 04/11/2013
  - Start time set to:** 3:00 PM
  - No end date** (selected)
  - End after:** 10 occurrences
  - End by:** Fri 04/12/2013
- Recurrence Pattern:**
  - Hourly** (selected)
  - Recur every 1 hour(s)
  - Other options: Daily, Weekly, Monthly, By the Minute

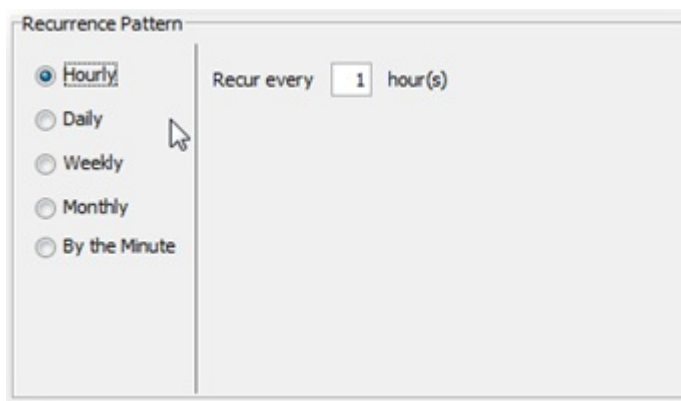
**OK** and **Cancel** buttons are at the bottom right.

3. Specify the discovery criteria as described in [“Discovering Network Elements” on page 51](#).

4. Specify the start date and time using the calendar drop-down list shown below.



- a. Select the current day or a date in the future in the calendar. If you select a date in the past, the discovery runs immediately.
  - b. Specify the start time in the **Time** field below the calendar.
5. An end date is optional. To set an end date, use the buttons in the lower left corner of the **Schedule** section to set a specific end date, or to set the schedule to end after a defined number of occurrences.
6. The **Recurrence Pattern** panel lets you set a schedule to recur at a specific interval, as follows:
  - a. Hourly – The schedule executes at the start time selected and recurs for the number of hours specified, until the end date is reached.



- b. Daily – The schedule executes at the start time selected and recurs for the number of days specified, until the end date is reached.

Recurrence Pattern

☐ Hourly
☒ **Daily**
☐ Weekly
☐ Monthly
☐ By the Minute

Recur every  day(s)

- c. Weekly – The schedule executes at the start time selected and recurs for the number of weeks specified, on the specific day of the week selected, until the end date is reached.

Recurrence Pattern

☐ Hourly
☐ Daily
☒ **Weekly**
☐ Monthly
☐ By the Minute

Recur every  week(s) on:

☐ Sunday
☐ Monday
☒ **Tuesday**
☐ Wednesday
☐ Thursday
☐ Friday
☐ Saturday

- d. Monthly – The schedule executes at the start time selected and recurs for the number of months specified, on the specific day of the month selected, until the end date is reached.



Recurrence Pattern

☐ Hourly  
☐ Daily  
☐ Weekly  
☒ Monthly  
☐ By the Minute

Day  of every  month(s)

- e. By the Minute – The schedule executes at the start time selected and recurs for the number of minutes specified, until the end date is reached.



**CAUTION:** Use this feature sparingly as it could overload the server needlessly depending on the frequency chosen and the task to be executed.

Recurrence Pattern

☐ Hourly  
☐ Daily  
☐ Weekly  
☐ Monthly  
☒ By the Minute

Recur every  minutes

7. When you are done, click **OK**.

The new discovery task is added to the **Schedules** table.

Topology: Cache_Bypass   Scheduler		
Schedules	Domain	Schedule
Discovery Schedules	Right-click to Add a schedule.	
10.1.105.5	Default	Scheduled from 04/24
10.1.108.1-20	Default	Scheduled from 03/16
172.27.7.101-120	Be1fast	Scheduled from 04/01

## Viewing Scheduled Tasks

To view a scheduled task for a network element:

1. Access the **Scheduler** screen using the toolbar button, or from the main menu choose **Edit > Schedules**.



The **Scheduler** tab is displayed:

Topology: Network Element Groups Scheduler		
Schedules	Domain	Schedule
Discovery Schedules	Right-click to Add a schedule.	
10.1.108.1-20	Default	Scheduled from 03/16/12 8:00 AM
172.27.7.101-120	Be1fast	Scheduled from 04/01/12 7:00 AM

2. In the **Scheduler** tab, expand the entries in the schedule list to view all the tasks currently scheduled on the server.

The following table describes the scheduler parameters.

**Table 8: Scheduler Tab**

Column name	Description
Schedules	Displays the scheduled task criteria
Domain	Displays the domain within which the task should execute
Schedule	Displays a summary of the schedule details for the task that was set up

## Deleting Scheduled Tasks

To delete a scheduled task for a network element:

1. Click the **Schedules** icon. The **Scheduler** tab appears.
2. Expand the **Discovery Schedules** entry to display the schedule you want to delete.
3. Right-click the schedule you want to delete, and choose **Delete Schedule**. A confirmation dialog appears.
4. Click **OK**. The scheduled task is deleted.

## CHAPTER 5

# Managing Network Topology

- [Introduction on page 63](#)
- [Icons and Definitions on page 63](#)
- [Understanding the Network Topology View on page 65](#)
- [Learning the Network Topology on page 72](#)
- [Network Element Groups and Sites on page 86](#)
- [Changing the Background View on page 91](#)

## Introduction

---

The proNX Service Manager provides a view of the network, including topology for supported network elements. The topology window is the main window you see when logging on to PSM. PSM displays all discovered network elements and, additionally, displays topology for the following:

- BTI7800 Series network elements
- BTI7000 Series network elements
- BTI800 Series network elements
- BTI700 Series network elements
- MX Series and PTX Series routers and QFX Series switches attached to a BTI7000 Series optical network using manual topology specification (Remote IDs) on supported interfaces. See [“Nodal Management for Juniper Networks Routers and Switches” on page 257](#) for the list of supported interfaces.

## Icons and Definitions

---

Topology map icons appear in the topology Map view. Service icons appear in the different service views.

*Table 9: Topology Map Icons*

Icon	Description
	A network element.

---

Table 9: Topology Map Icons (continued)







Icon	Description
	A router.
	Multiple connections (links) between network elements. To determine whether to display this icon, PSM counts the connections for all layers currently being displayed. For this icon to be meaningful, ensure that you only select a single layer in the topology Map view. Otherwise, PSM displays this multi-link icon when there is a single connection at more than one layer (e.g. a connection at layer 0 and a connection at layer 1).
	A link down-up indication next to a link to indicate that the link has recently gone down and come back up. The length of time that this indication is displayed is configurable ( <a href="#">“Setting Topology Display Options” on page 276</a> ).
	A link connecting network elements in a split ROADM node configuration.
	A replication cluster member. When server replication is enabled and working, this is found on the PSM server you are logged on to, and on all members of the same server replication cluster.
	A network element that has been marked. See <a href="#">“Marking or Unmarking a Network Element” on page 112</a> .

Table 10: Service Icons


















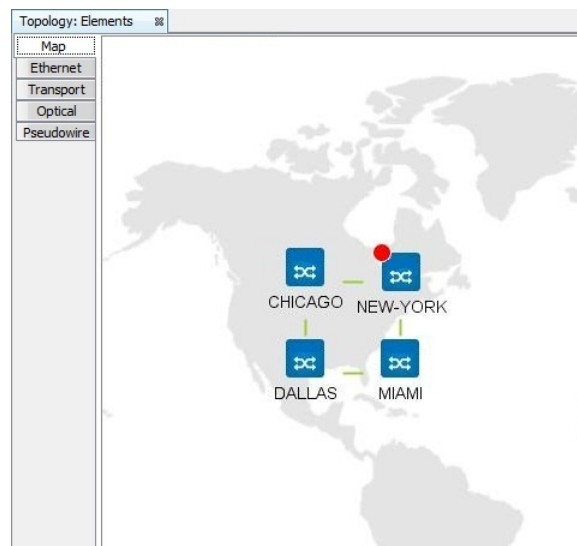
Icon	Description
<b>General service icons</b>	
	A network element.
	A module, appears when expanding a network element in a service.
	A service endpoint.  This is also used to indicate a Transport or Ethernet service in the Transport or Ethernet branches of the Network tree.
	A multi-layer service.
	Logical connection between an endpoint and the network element or module.
<b>Optical service icons</b>	
	ROADM Node: a collection of modules providing add/drop/passthrough capability.

Table 10: Service Icons (continued)

Icon	Description
	Line Amplifier Node: a collection of modules providing line amplification between two spans.
	Line Equalizing Node: a collection of modules providing channel equalization between two spans.
	ROADM Terminal Node: a collection of modules providing add/drop capability with channel equalization in a linear span.
	An optical service endpoint.  This is also used to indicate an Optical service in the Optical or Transport branches of the Network tree. In the Transport branch, this indicates the transport service component of an optical service with transponder interface endpoints. See <a href="#">"Activating an Optical Service Between Transponder Interface Endpoints" on page 308</a> .
	Fiber connection between nodes (with span length displayed in kilometers).
	A link connecting network elements in a split ROADM node configuration.
<b>Ethernet service icons</b>	
	A UNI endpoint.
	An NNI endpoint.
	An RPL link passing traffic in an ERPS service.
	A blocked RPL link in an ERPS service.
	A failed link in an ERPS service.

## Understanding the Network Topology View

PSM provides a main **Topology** window that displays network elements and links in the managed network. The topology overlays a background image that can be changed to suit your particular needs. The **Topology** window is the initial view you see when first logging on to the PSM server. You can always go back to the **Topology** window from other windows by choosing **View >Network >Topology**.



In the upper left corner, you can select from the following topology views:

- **Map:** The topology **Map** view is used to display the topology of the network. PSM builds the topology map based on discovered information as well as through manual specification. Manual specification allows you to supplement the discovered view to suit your needs.
- **Ethernet:** The Ethernet services view is used to display the topology of a specific Ethernet service. To see a service, select the desired Ethernet service from the Network tree. For more information on the Ethernet services view, see [“Managing Ethernet Services” on page 337](#).
- **Transport:** The Transport services view is used to display the topology of a specific transport service. To see a service, select the desired transport service from the Network tree. For more information on the Transport services view, see [“Transport Services” on page 323](#).
- **Optical:** The Optical services view is used to display the topology of a specific optical service. To see a service, select the desired optical service from the Network tree. For more information on the Optical services view, see [“Optical Services” on page 301](#).
- **Pseudowire:** The Pseudowire services view is used to display the topology of a specific pseudowire service. To see a service, select the desired pseudowire service from the Network tree. For more information on the Pseudowire services view, see [“Managing Pseudowire Services” on page 441](#).

The topology **Map** view shows the following:

- discovered network elements
- network element groups that have been created previously (see [“Network Element Groups and Sites” on page 86](#))
- external devices that have links to discovered network elements
- links provisioned between any of the following: NEs, NE groups, or external devices



**NOTE:** An external device is a device that is unmanaged by PSM. PSM provides the capability to display such devices in the topology Map view.

Additionally, the view provides various visual cues, as follows:

- The color of the link indicates whether the link is up or down. Green indicates that the link is up. Red indicates that the link is down.
- A link between a managed device and an external (unmanaged) device is grey if the port status on the managed device is up. It is red if the port status on the managed device is down.
- In a multi-link representation where multiple connections are represented by a single link, red takes precedence over green which takes precedence over grey.
- The color of the font below the NE icon indicates whether the NE is reachable or not. Black indicates the NE is reachable. Red indicates the NE is not reachable.
- The presence of a dot on the upper left corner of the NE icon indicates the existence of outstanding alarms. Red indicates the existence of outstanding critical alarms. Amber indicates the existence of outstanding major alarms. Yellow indicates the existence of outstanding minor alarms. When multiple levels of alarm severity exist, the color reflects the level of the most severe alarm. The absence of a dot indicates no outstanding alarms.

## Layer Views

You can select which layer to view in the topology map.

From the upper right corner of the topology **Map** view, click to enable or disable the desired layer. The selections are not mutually exclusive. You can select multiple layers to view concurrently.

**Physical**  
Layer 0  
Layer 1  
Layer 2  
Layer 3

- **Physical:** This view shows all the physical layer connectivity (that is, fibers). This is the default view.
- **Layer 0:** This view shows the fibers connected to optical layer equipment. Optical layer equipment consists of ROADMs, multiplexer/demultiplexers, and DWDM line amplifiers. This view is the same as the **Physical** layer view for the network elements shown.
- **Layer 1:** This view shows transport layer connectivity (for example, SONET/SDH connectivity). This view might be different from the **Physical** layer view.

- **Layer 2:** This view shows Ethernet layer connectivity. This view might be different from the **Physical** layer view.
- **Layer 3:** This view is not supported.

Only the connectivity for the selected layer(s) is shown.

You can also control whether connectivity to external devices is shown for the selected layer(s). To show or hide connectivity to external devices, right-click the background in the topology Map view and toggle between **Show Unknown Links** and **Hide Unknown Links**.

## Network Element and Link Details

Information can be obtained by hovering over or right-clicking certain objects in the view. When hovering over a network element, the information displayed includes the IP address, the name and type of network element, the software version it is running, notes, an alarm summary, and other information. Details on how to interpret the alarm summary can be found in [“Understanding the Alarms Summary Bar” on page 466](#).

*Figure 3: Hovering Over a Network Element*



When hovering over a PSM server, similar information is displayed. In addition to information found when hovering over a network element, there is an indication to show whether this server is part of a server replication cluster. If this server is part of a server replication cluster, and this is the server to which you are currently logged in, the display includes a listing of the other cluster member(s) ([Figure 4 on page 69](#)). If this server is part of a server replication cluster, but is not the server to which you are currently logged in, the display indicates that the server is a cluster member (with no IP addresses displayed). See [“Running Multiple Servers with Server Replication” on page 30](#) for details on server replication.

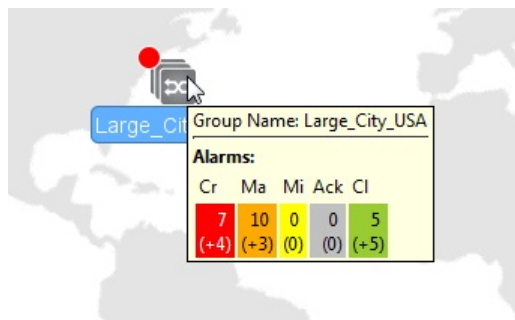


Figure 4: Hovering Over a PSM Server

IP Address: 172.25.7.219				
Name: mgtServ				
Location:				
Domain: Default				
Type: WideCastOS v1.34.1				
Status: Reachable				
Contact: root@localhost				
Cluster Members: 10.64.6.64				
<hr/>				
<b>Notes:</b>				
Postal Code:				
Longitude:				
Latitude:				
<hr/>				
<b>Alarms:</b>				
Cr	Ma	Mi	Ack	Cl
0	0	0	3	2

When hovering over a network element group, an alarm summary is displayed.

Figure 5: Hovering Over a Network Element Group



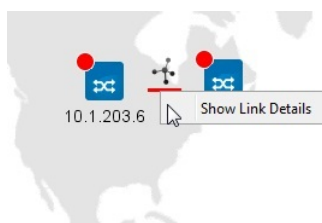
Group Name: Large\_City\_USA

**Alarms:**

Cr	Ma	Mi	Ack	CI
7	10	0	0	5
(+4)	(+3)	(0)	(0)	(+5)

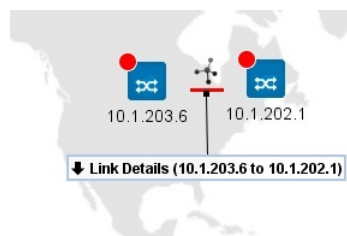
When right-clicking on a link, an option is presented to **Show Link Details**.

Figure 6: Show Link Details



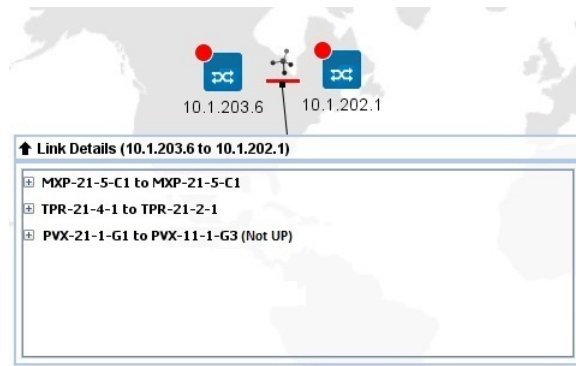
When selecting that option, a **Link Details** data widget title bar is presented.

Figure 7: Link Details Data Widget Title Bar



When clicking on the **Link Details** title bar, a **Link Details** window is presented.

*Figure 8: Link Details Data Widget Window*



Each connection can be expanded to show detailed link information. [Table 11 on page 70](#) shows the type of information that can be displayed. The actual information displayed depends on the type of network element and port. Not all attributes are supported on every network element. [Figure 9 on page 71](#) through [Figure 14 on page 72](#) show examples of the link information provided. Some attributes are optional and are only shown if they are configured.

*Table 11: Link Details*

Attribute	Description
<b>General</b>	
Network Element	The network element name or IP address
Port	The port identifier (in the native syntax for the network element)
ID	The optional port identifier (freeform text)
Custom	The optional custom fields for the port (freeform text)
State	The port state (available for managed devices only). The state is shown as UNKNOWN if the device does not provide state information, such as is the case with multiplexers/demultiplexers, which are passive devices.
<b>Optical</b>	
Span Length	The span length of the fiber
Max Span Loss	The maximum span loss supported on the fiber
Max Span Loss Alarm Threshold	The maximum span loss alarm threshold on the fiber
Channel Count	The number of optical channels provisioned on the fiber

Table 11: Link Details (continued)

Attribute	Description
<b>Transponding and Muxponding</b>	
Protocol	The protocol
Wavelength	The wavelength
Line Mapping	The line mapping (muxponding)

Figure 9: BTI7000 Series DOL-DOL Link Details Data Widget

↑ Link Details (DALLAS to MIAMI)		
<b>Network Element</b>	DALLAS	MIAMI
<b>Port</b>	ROB-1-17-L1	ROB-1-7-L1
<b>State</b>	Up - NR	Up - NR
<b>Span Length</b>	0 km	0 km
<b>Max Span Loss</b>	35.0 dB	35.0 dB
<b>Max Span Loss Alarm Threshold</b>	0.0 dB	0.0 dB
<b>Channel Count</b>	2	2

Figure 10: BTI7000 Series PVX-PVX Link Details Data Widget

↑ Link Details (NEWYORK to 10.1.202.1)		
<b>Network Element</b>	NEWYORK	10.1.202.1
<b>Port</b>	PVX-1-11-G11	PVX-11-1-G3
<b>ID</b>	47684	47684
<b>Custom 1</b>	Bronx-476	Bronx-484
<b>State</b>	Up - NR	Down - AU,SGEO

Figure 11: BTI7000 Series Transponder-Transponder Link Details Data Widget

↑ Link Details (10.1.203.6 to 10.1.202.1)		
<b>Network Element</b>	10.1.203.6	10.1.202.1
<b>Port</b>	TPR-21-4-1	TPR-21-2-1
<b>ID</b>	38742	38742
<b>Custom 1</b>	Man-445	Man-493
<b>Protocol</b>	STM64FEC	STM64FEC
<b>Wavelength</b>	1310.0 nm	1310.0 nm
<b>State</b>	Down - AU,AINS,SGEO	Down - AU,SGEO

Figure 12: BTI7000 Series Muxponder-Muxponder Link Details Data Widget

Link Details (10.1.203.6 to 10.1.202.1)		
Network Element	10.1.203.6	10.1.202.1
Port	MPX-21-5-C1	MPX-21-5-C1
ID	58743	58743
Custom 1	Man-876	Man-389
Protocol	GE	GE
Wavelength	1550.0 nm	1550.0 nm
State	Down - AU,AINS,SGEO	Down - AU,SGEO

Figure 13: MX Series Router Transponder to BTI7000 Series DOL Link Details Data Widget

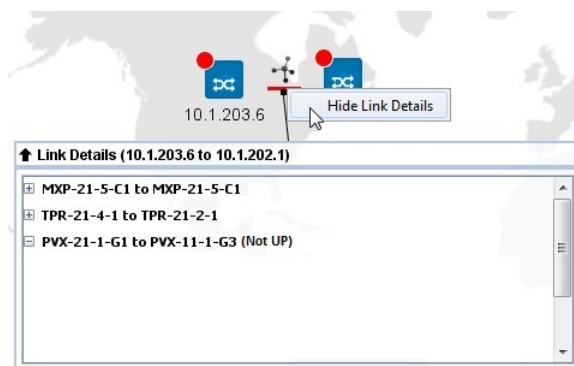
Link Details (10.228.207.1 to 10.228.207.2)		
Network Element	10.228.207.1	10.228.207.2
Port	et-4/0/0	D96MD-0-1-340
State	Unknown	Unknown
Channel Count	1	1

Figure 14: External Device to BTI7000 Series PVX Link Details Data Widget

Link Details (10.10.1.57 to MIAMI)		
Network Element	10.10.1.57	MIAMI
Port	EXT-2-3-5	PVX-1-5-G1
ID 1		35256
Custom 1		MIAMI
State		Down - AUMA,MT,MEA,FLT

You can hide **Link Details** by right-clicking on the same link and selecting **Hide Link Details**, or optionally, right-clicking anywhere in the background and selecting **Hide All Link Details**.

Figure 15: Hide Link Details



## Learning the Network Topology

PSM learns the topology of the network in different ways:

- For optical links on ROADM nodes, PSM learns the optical topology automatically from the DOL or ROADM neighbor information tables retrieved from the nodes. See [“Deriving Optical Topology Using DOL or ROADM Data” on page 73](#).
- For layer 1 (physical) Ethernet links on BTI7800 NEs with LLDP snooping enabled, PSM learns the layer 1 topology automatically from the snooped LLDP information retrieved from the NEs. See [“Deriving Layer 1 Topology Using Snooped LLDP Data” on page 73](#).
- For layer 2 Ethernet links on NEs with LLDP enabled, PSM learns the Ethernet topology automatically from the LLDP neighbor tables retrieved from the NEs. See [“Deriving Ethernet Topology Using LLDP Data” on page 74](#).
- Additionally, PSM supports a manual specification method that allows you to specify the topology directly for BTI7000 Series and BTI800 Series network elements. See [“Deriving Topology Using Remote IDs” on page 74](#). This is the method you use for specifying the transport topology in a BTI7000 Series network.
- [Deriving Optical Topology Using DOL or ROADM Data on page 73](#)
- [Deriving Layer 1 Topology Using Snooped LLDP Data on page 73](#)
- [Deriving Ethernet Topology Using LLDP Data on page 74](#)
- [Deriving Topology Using Remote IDs on page 74](#)

## Deriving Optical Topology Using DOL or ROADM Data

BTI Series ROADM nodes advertise and identify themselves to their optical neighbors by exchanging information over the optical service channel (OSC). Each node builds a table of its neighbors. PSM uses this information to build and display an accurate, up-to-date optical topology of the network.

## Deriving Layer 1 Topology Using Snooped LLDP Data

LLDP snooping allows transport equipment to snoop LLDP frames on Ethernet links.

Some Ethernet devices discover their Ethernet neighbors using the Link Layer Discovery Protocol (LLDP). LLDP runs over Ethernet and allows devices to advertise and identify themselves to their peers.

When these devices are connected across a transport network, the transport equipment can snoop passing LLDP frames to determine the identity of the attached devices. If the transport equipment is managed by PSM, PSM can then use this information to show connectivity between the transport equipment and the attached Ethernet device.

This capability to snoop LLDP frames is supported for network elements running the following releases:

- BTI7800 release 4.1 or higher



**NOTE:** LLDP snooping must be enabled on the Ethernet interface on the device. See [“Editing an Interface” on page 205](#) for information on how to enable LLDP snooping on a BTI7800 UFM interface.

## Deriving Ethernet Topology Using LLDP Data

Some BTI Series network elements can be configured to discover their Ethernet neighbors using the Link Layer Discovery Protocol (LLDP). LLDP runs over Ethernet, and allows network elements to advertise and identify themselves to their peers. Each NE builds a table of its Ethernet neighbors that PSM can retrieve. PSM uses this information to build and display an accurate, up-to-date Ethernet topology of the network.

This capability is supported in PSM for network elements running the following releases:

- BTI7000 Series release 10.3 or higher
- BTI700 Series release 1.5 or higher (BTI718E all releases)
- BTI800 Series release 1.1 or higher

PSM can only display this topology if the NEs have been configured to use LLDP. You can configure LLDP on the NEs directly using the proNX 900 or the CLI. Alternatively, you can use PSM to enable LLDP on the NEs during initial NE discovery. For information on how to do this, see [“Discovering Network Elements” on page 51](#).

Be aware that this method produces an Ethernet topology of the network, which might not necessarily reflect the physical topology. Where the two topologies do not align, you can use manual specification (that is, Remote IDs) to change the discovered Ethernet topology to align with the physical topology if desired.

## Deriving Topology Using Remote IDs

PSM allows you to specify the topology manually hop by hop through the use of the Remote ID, a parameter that you configure on a supported port to indicate the identity of the port attached to the other end of the fiber. There are a number of reasons for specifying the topology in this manner:

1. To include topology that is not automatically discovered, such as connections between transport equipment (for example, transponder to transponder for BTI7000 Series equipment) and connections between transport equipment and optical equipment (for example, transponder to multiplexer/demultiplexer)
2. To change an automatically-discovered topology to align with the actual physical topology, such as changing the discovered Ethernet topology to show connectivity to transport or optical equipment
3. To include topology to external equipment

The ability to configure Remote IDs is supported in PSM for network elements running the following releases:

- BTI7000 Series release 9.2.0 or higher
- BTI800 Series release 1.1 or higher

The Remote ID is a string that references the remote end of the connection (fiber). The string is not used by the NE itself, but is read and correlated by PSM to determine the connection endpoints. For this reason, the accuracy with which PSM derives the topology

is dependent on proper configuration of this field. If improperly configured, the topology shown by PSM might not reflect the actual topology.

The NE treats the configuration of the Remote ID as an opaque string and does not otherwise perform any syntactical or semantic checking on the configured value. All syntactical and semantic checking is performed by PSM.

Remote ID configuration can be bookended or singled-ended:

- **Bookended:** the Remote ID is configured at both ends of the connection (to point to each other). This is mandatory when both endpoints support Remote ID configuration. PSM validates the Remote ID configuration and raises an alarm if the validation fails. See [“Detecting Remote ID Errors” on page 85](#) for more information.
- **Single-ended:** the remote ID is configured at only one end of the connection (to point to the other end). This is the only possible method when only one endpoint supports Remote ID configuration. In this situation, PSM uses the Remote ID configured at one end to derive the topology. PSM does not require information from the other endpoint except to perform limited validation in specific situations. See [“Detecting Remote ID Errors” on page 85](#) for more information.

Because the Remote ID is used to specify the physical fiber connectivity, you should typically configure the Remote IDs when the actual fibers are installed. Not only will this allow PSM to display the topology correctly, but it will also allow you to activate supported services with endpoints referenced by the Remote IDs.

The following table shows where the Remote ID can be configured and what endpoint it can reference.

Remote ID can be configured on:	Remote ID can reference:
BTI7000 Series muxponder, transponder, DOL, and packetVX ports, and BTI800 Series ports  For DOL ports, the Remote ID can be configured as follows: <ul style="list-style-type: none"> <li>• You can configure the Remote ID on a BTI7000 Series DOL multiplexer/demultiplexer channel port or on a BTI7000 Series DOL ROADM module Alien/C2 port to point to attached equipment (for example, PVX or MX Series or PTX Series or QFX Series port). This configures the connectivity from the attached equipment to the DOL network.</li> <li>• Additionally, you can configure the Remote ID on the BTI7000 Series DOL ROADM module Alien/C2 port to show a split ROADM node. In this situation, you cannot use the ROADM module C2 port as an optical service endpoint. See <a href="#">“Configuring a Split ROADM Node” on page 176</a>.</li> </ul>	BTI7000 Series muxponder, transponder, DOL, and packetVX ports, and BTI700 Series, BTI800 Series, BTI7800 Series, and supported interfaces on MX Series and PTX Series routers and QFX Series switches, and external device ports  For the list of supported interfaces on Juniper Networks routers and switches, see <a href="#">“Nodal Management for Juniper Networks Routers and Switches” on page 257</a> .  For information on connecting to an external device port, see <a href="#">“Viewing External Devices” on page 85</a> .

### Remote ID Format

PSM provides great flexibility on how you build your topology with Remote IDs. As long as the Remote ID configuration conforms to the required syntax, and as long as the Remote IDs at each end refer to each other (for bookended configurations), PSM will

display the connection. Therefore, you must provision the Remote ID with great care or the topology might not turn out as you intend.

The general format of the Remote ID is as follows:

**<IP Address>-<Circuit Pack Type>-<Shelf>-<Slot>-<Port>**

where the **<IP Address>** is the remote IP address of the connection in dotted decimal notation, the **<Circuit Pack Type>** is the type of card at the remote location, and **<Shelf>**, **<Slot>**, and **<Port>** represent the shelf, slot, and port identifiers of the remote end.

The following table shows how the Remote ID is constructed for the different types of endpoints. All characters in the syntax are case-insensitive.



**NOTE:** This table lists the values that PSM considers to be valid (for the purpose of determining whether or not to raise an "Invalid Remote ID" alarm). PSM does not check the specified Remote ID against the actual NE being referenced for this alarm. Not all values that PSM considers to be valid are applicable for certain circuit pack types. See [“Detecting Remote ID Errors” on page 85](#) for more information on how PSM determines what is considered valid.

Remote Endpoint	Remote IP	Circuit Pack Type	Shelf-Slot-Port	Example
BT17000 Series muxponder	IP address in dotted decimal notation	MXP	<shelf>--<slot>-L<n>	10.1.121.24-MXP-11-3-L2
			<shelf>--<slot>-C<n>	10.1.121.24-MXP-11-3-C2
	NOTE: The remote NE must be a discovered network element.			
BT17000 Series transponder	IP address in dotted decimal notation	TPR, WM, WR, WT	<shelf>-<slot>-<port>	10.1.121.24-TPR-1-3-3
	NOTE: The remote NE must be a discovered network element.			
BT17000 Series packetVX	IP address in dotted decimal notation	PVX	<shelf>--<slot>-X<n>	10.1.121.24-PVX-21-3-X2
			<shelf>--<slot>-G<n>	10.1.121.24-PVX-21-3-G7
	NOTE: The remote NE must be a discovered network element.			



Remote Endpoint	Remote IP	Circuit Pack Type	Shelf-Slot-Port	Example
BTI7000 Series multiplexer/demultiplexer	IP address in dotted decimal notation  <b>NOTE:</b> The remote NE must be a discovered network element.	D32MD1 to D32MD4  D40MD  D96MD	<shelf>-<slot>-CH<n>	10.1.121.24-D40MD-0-1-CH280
BTI7000 Series ROADM	IP address in dotted decimal notation  <b>NOTE:</b> The remote NE must be a discovered network element.	ROB	<shelf>-<slot>-C2	10.1.121.24-ROB-1-3-C2  For information on where to use this, see <a href="#">“Configuring a Split ROADM Node”</a> on page 176.
BTI7800 Series UFM	IP address in dotted decimal notation  <b>NOTE:</b> The remote NE must be a discovered network element.	OTU4  OCH	<del>&lt;shelf&gt;-&lt;slot&gt;-EC&lt;port&gt;</del>  <shelf>-<slot>-<Port Group>-<Xcvr Port>-<Fiber Port>.<OCH>	10.228.220.71-OTU4-1-5-1-1  10.228.220.71-OCH-1-14-2-1-2.1
BTI800 Series	IP address in dotted decimal notation  <b>NOTE:</b> The remote NE must be a discovered network element.	BTI800	<shelf>-<slot>-G<n>	10.1.111.4-BTI800-1-2-G3
MX Series or PTX Series or QFX Series	IP address in dotted decimal notation  <b>NOTE:</b> The remote NE must be a discovered network element.	JUNOS	<del>&lt;PPC&gt;-&lt;PCMC&gt;-&lt;port&gt;</del>	10.1.111.5-JUNOS-1-0-0
BTI700 Series	IP address in dotted decimal notation	BTI700	not validated	10.1.121.24-BTI700-1-1-6-X  A BTI700 Series NE is treated like an external device and requires a trailing -X or -x in the Remote ID. See <a href="#">“Viewing External Devices”</a> on page 85 for more details on external devices.
External	IP address in dotted decimal notation	EXT	not validated	10.1.121.24-EXT-2-3-6-X  An external device requires a trailing -X or -x in the Remote ID. See <a href="#">“Viewing External Devices”</a> on page 85 for more details on external devices.

## Remote ID Configuration

PSM provides a GUI-driven method to configure the Remote ID. The benefit of this approach is that you do not need to know the remote ID syntax in order to construct the remote ID. [Figure 16 on page 78](#) shows the Remote ID configuration dialog:

Figure 16: Provision Remote Port ID



**NOTE:** The Remote ID configuration attributes might change depending on the CP Type that you select.

The meanings of the attributes are as follows:

- **Local Port ID** This displays the local port identifier. This attribute cannot be changed.
- **Remote Id** This is the Remote ID that is currently set. This field cannot be changed directly. It is changed by editing the individual components of the Remote ID through the various drop-down menus.
- **Hostname/IP Address** Set the hostname or IP address of the remote endpoint. For convenience, completion suggestions are provided based on the discovered network elements.
- **CP Type** Set the circuit pack type (or BT17800 UFM interface name) from the drop-down menu.



**NOTE:** Only the circuit pack types described in [“Remote ID Format” on page 75](#) are supported.

- **Shelf, Slot, Port** Set the shelf, slot, and port indexes respectively.
- **BIC** Set the BIC (subslot) if referencing an OTU4 interface on a BTI7800UFM.
- **Fiber Port, OCH** Set the Fiber Port (subport) and OCH (channel) if referencing an OCH interface on a BTI7800UFM.
- **Alien** This specifies whether the remote ID refers to an external device. This is usually used when configuring a Remote ID to point to a BTI700 Series or third-party device. Selecting this attribute causes an -X to be appended to the end of the Remote ID.
- **Bidirectional** This option allows you to specify whether you want PSM to automatically set the remote ID on the remote port to point back to this local port. This attribute should only be selected if the circuit pack type is one of **MXP, TPR, WR, WM, WT, PVX, ROB, BTI800**. You cannot select both **Alien** and **Bidirectional** at the same time.

This dialog can be reached through the Network tree ([“Setting the Remote ID” on page 79](#), [“Setting the Remote ID on a Multiplexer/Demultiplexer” on page 80](#), [“Setting the Remote ID on a ROADM C2 Port” on page 82](#)) or through the NE Shelf view ([“Setting the Remote ID from the Shelf View” on page 129](#)).

If you are familiar with the Remote ID syntax, you can set the Remote ID in a freeform manner within certain nodal provisioning windows for BTI7000 Series ports. This is shown in various places in [“Nodal Management for BTI7000 Series Network Elements” on page 134](#).

### Setting the Remote ID

Use this procedure to set the Remote ID on the following ports from the Network tree:

- a BTI7000 Series transponder, muxponder, or packetVX port
- a BTI800 Series port

1. Expand the network element in the Network tree to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.
3. Expand a module to show the ports in that module.
4. Right-click a provisioned port and select **Remote ID >Provision**.

The **Provision Remote Port ID** dialog appears.

5. Configure the Remote ID as described in [“Remote ID Configuration” on page 78](#).
6. Click **OK**.



**NOTE:** If you select **Bidirectional** and you specify a Remote ID that cannot be reconciled, PSM will be unable to configure the remote endpoint, and the task will fail.

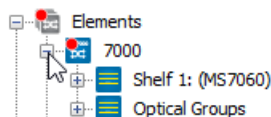


**NOTE:** The task might fail if you try to use this procedure on a card that has not been provisioned.

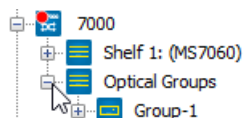
### Setting the Remote ID on a Multiplexer/Demultiplexer

Use this procedure to set the Remote ID on a BTI7000 Series multiplexer/demultiplexer port from the Network tree.

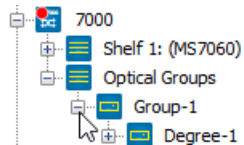
1. Expand the network element in the Network tree to show the equipment in that NE.



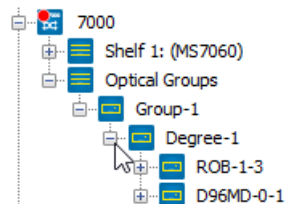
2. Expand the Optical Groups branch to see the configured optical groups.



3. Expand an optical group to show the degrees in that optical group.

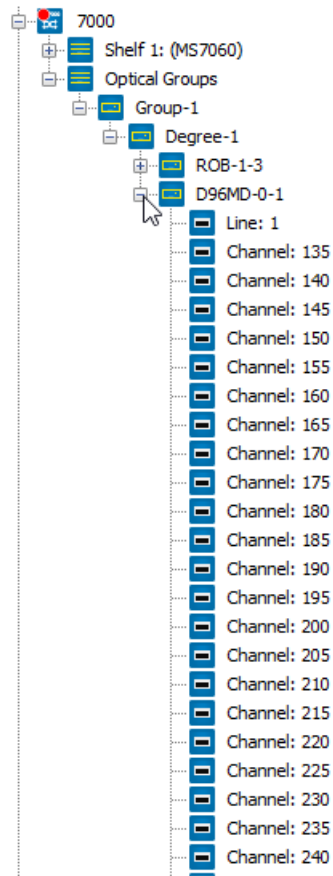


4. Expand a degree to show the multiplexer/demultiplexer for that degree.



5. Expand the multiplexer/demultiplexer to show the ports/channels on that multiplexer/demultiplexer.

Each port on the multiplexer/demultiplexer is named by its frequency. For example, channel 235 on the multiplexer/demultiplexer represents the port with frequency 192.35 THz (1558.58 nm).



6. Right-click a port/channel and select **Remote ID >Provision**.

The **Provision Remote Port ID** dialog appears.

7. Configure the Remote ID as described in [“Remote ID Configuration”](#) on page 78.

8. Click **OK**.



**NOTE:** If you select **Bidirectional** and you specify a Remote ID that cannot be reconciled, PSM will be unable to configure the remote endpoint, and the task will fail.



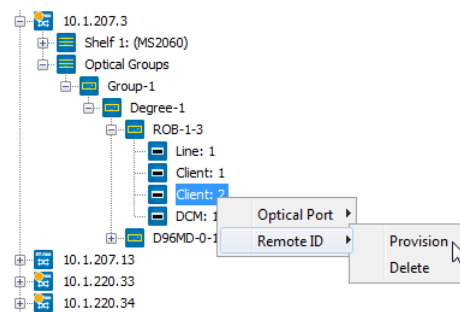
**NOTE:** The task might fail if you try to use this procedure on a card that has not been provisioned.

### Setting the Remote ID on a ROADM C2 Port

Use this procedure to set the Remote ID on a BT17000 Series ROADM C2 port from the Network tree. This procedure can be used to create a split ROADM node. For more information, see [“Configuring a Split ROADM Node” on page 176](#).

1. Expand the network element in the Network tree.
2. Expand the Optical Groups branch to see the configured optical groups.
3. Expand an optical group to see the degrees in that group.
4. Expand a degree to see the ROADM module in that degree.
5. Expand the ROADM module to see the ports in that module.
6. Right-click the Client: 2 port and select **Remote ID > Provision**.

*Figure 17: Selecting the C2 Port*



The **Provision Remote Port ID** dialog appears.

7. Configure the Remote ID as described in [“Remote ID Configuration” on page 78](#).
8. Click **OK**.



**NOTE:** If you select Bidirectional and you specify a Remote ID that cannot be reconciled, PSM will be unable to configure the remote endpoint, and the task will fail.



**NOTE:** The task might fail if you try to use this procedure on a card that has not been provisioned.

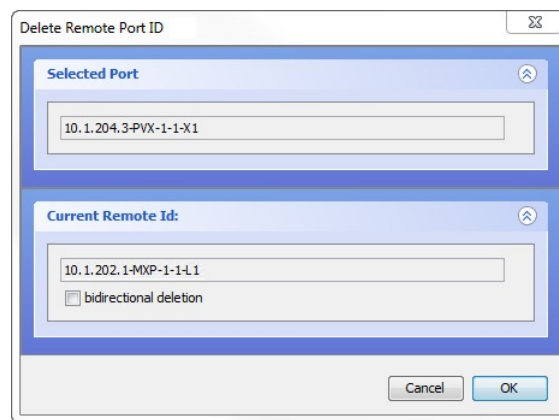
## Deleting the Remote ID

Use this procedure to delete the Remote ID from an existing port on a BTI7000 Series or BTI800 Series network element.

There are different ways by which you can delete the Remote ID. You can delete the Remote ID from the Network tree or from the NE shelf view or from nodal provisioning windows. This procedure describes how to delete the Remote ID from the Network tree. For information on deleting the Remote ID from the shelf view, see [“Deleting the Remote ID from the Shelf View” on page 130](#). The Remote ID can also be deleted in a freeform manner within certain nodal provisioning windows. This is shown in various places in [“Nodal Management for BTI7000 Series Network Elements” on page 134](#).

1. Expand the network element in the Network tree view to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.
3. Expand a module to show the ports in that module.
4. Right click a provisioned port and select **Remote ID >Delete**.

The **Delete Remote Port ID** dialog appears.



5. To delete the remote ID at both endpoints, select **bidirectional deletion**.
6. Click **OK**.

## Interactions with LLDP

PSM can display Ethernet connections using either LLDP or Remote ID. This section only applies to those BTI Series network elements that support LLDP and Remote IDs. See [“Deriving Ethernet Topology Using LLDP Data” on page 74](#) for the list of supported network elements.

In general, LLDP provides a more accurate representation of the Ethernet topology because LLDP-derived topology is learned rather than manually provisioned. However, since LLDP provides the Ethernet topology rather than the physical topology, you can use remote IDs to change the topology view to reflect the physical topology if desired.

When LLDP is enabled and the Remote ID is configured, the following rules apply:



**NOTE:** An incorrect Remote ID in the table refers to either a syntactically-invalid Remote ID or a Remote ID that leads to a Remote ID mismatch condition.

**Table 12: When LLDP is Enabled and Remote ID is Configured**

Configuration Scenario	Topology Shown	Explanation
The Remote IDs at both ends correctly point to a BT17000 Series packetVX, BT1700 Series device, or a BT1800 Series device.	LLDP	This situation occurs when you want to represent a direct connection (fiber) between two Ethernet devices. In such a case, LLDP should have provided the correct information, and therefore PSM assumes the LLDP topology is correct. If the Remote ID topology differs from the LLDP topology, PSM raises an "NE Link Mismatch" alarm.
The Remote IDs at both ends correctly point to a muxponder, a transponder, a multiplexer/demultiplexer, or an external device (that is, MXP, TPR, WM, WR, WT, D32MD1, D32MD2, D32MD3, D32MD4, D40MD, D96MD, EXT).	Remote ID	This situation occurs when you want to change the LLDP view to align with the physical topology. This is the primary use case for configuring remote IDs when LLDP is enabled.  <b>NOTE:</b> <sup>1</sup> Be aware that you might run into situations where PSM displays a broken path due to incorrect Remote ID configuration on the second or subsequent hops, up to and including the penultimate hop.
The Remote ID at one end correctly points to a muxponder, a transponder, a multiplexer/demultiplexer, or an external device (that is, MXP, TPR, WM, WR, WT, D32MD1, D32MD2, D32MD3, D32MD4, D40MD, D96MD, EXT) but the Remote ID at the other end does not, either because it is incorrect, or because it points correctly to a packetVX, BT1700 Series device, or a BT1800 Series device.	LLDP and Remote ID	PSM cannot determine which is the actual physical topology, so it displays both as best as it can.
The Remote ID at one end correctly points to a packetVX, BT1700 Series device, or a BT1800 Series device, but the Remote ID at the other end is incorrect.	LLDP	PSM assumes the LLDP topology is the physical topology, and raises an "NE Link Mismatch" alarm.
The Remote IDs at both ends are incorrect.	LLDP	PSM cannot resolve the Remote IDs, and assumes the LLDP topology is the physical topology.



## Viewing External Devices

PSM provides the capability to display external devices in the topology **Map** view if the external device is connected to a network element that supports remote IDs. An external device is any device that is unmanaged by PSM.

PSM displays an external device whenever an EXT-formatted Remote ID has been provisioned on a discovered network element. A Remote ID in the form **<IP Address>-EXT-<Shelf>-<Slot>-<Port>-<X|x>** denotes an external device at the remote end of the connection. The trailing X is case-insensitive.

When PSM encounters an EXT-formatted Remote ID (for example, **10.1.121.24-EXT-1-3-2-x**), it creates an icon for the specified IP address if one does not already exist, and draws a link from the network element in which this Remote ID has been provisioned to the external device.



**NOTE:** PSM has no way of verifying if the Remote ID is properly referencing the external device.

The external device is displayed as an undiscovered network element. You manipulate the external device in the same way you manipulate an undiscovered network element, such as editing notes or adding or removing the device from groups.

You can delete an external device as you delete an undiscovered network element, but the external device will reappear when PSM performs a topology refresh and reprocesses all the configured Remote IDs. To delete an external device permanently, you must first delete it from the Remote ID on all network elements that reference this external device. You can then proceed to delete the external device by right-clicking the device and selecting **delete**.

## Detecting Remote ID Errors

PSM performs validation of the Remote ID during topology discovery.

The following errors are detected:

- PSM raises an "Invalid Remote ID" alarm upon detection of malformed fields. The alarm is raised against the port where the invalid Remote ID was found. Specifically, PSM performs the following (case-insensitive) syntax checks:
  - ensures the IP address is of the form **<0-255>.<0-255>.<0-255>.<0-255>**
  - ensures the circuit pack type is **<MXP | TPR | WR | WM | WT | D32MD1 | D32MD2 | D32MD3 | D32MD4 | D40MD | D96MD | PVX | BTI800 | JUNOS | BTI700 | EXT>**
  - ensures that both **BTI700** and **EXT** circuit pack types contain a trailing case-insensitive **-x**
  - ensures the shelf index is **<0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 11 | 21 | 31>** for all devices other than for **BTI700** and **EXT** devices
  - ensures the slot index is **<0-20>** for all devices other than for **BTI700** and **EXT** devices

This alarm does not identify contextual errors, such as a Remote ID referring to an impossible port identifier for that circuit pack type (for example, port **24** on a device with only two ports).

- PSM raises a "Remote ID Mismatch" alarm as follows:
  - Bookended: PSM correlates both ends of the connection and raises this alarm if the Remote IDs at the two ends are not referring to each other. This alarm implicitly identifies contextual errors such as when a Remote ID refers to an impossible port.
  - Single-ended: In the specific situation where the Remote ID is configured on a BT17000 Series DOL multiplexer/demultiplexer channel port and points to a supported UFM interface on a discovered BT17800 or points to a supported interface on a discovered MX Series or PTX Series router or QFX Series switch, PSM checks the wavelength at the remote endpoint as follows:

If the supported interface is on a tunable transceiver, PSM validates the wavelength configured on the interface with the wavelength associated with the multiplexer/demultiplexer port. If the wavelengths do not match, PSM raises an alarm and does not display the link in the topology view.

In all other cases, including configurations where the supported interface is on a fixed-wavelength transceiver or where the Remote ID is configured on a port that is not a BT17000 Series DOL multiplexer/demultiplexer channel port, PSM does not validate the wavelength at the remote endpoint.



**NOTE:** For bookended configurations, PSM cannot detect configuration errors where the Remote IDs are properly formed and referencing each other, but where no connection is actually provisioned between the stated endpoints.

---



**NOTE:** For single-ended configurations, PSM cannot detect configuration errors where the same Remote ID is configured on more than one port (in other words, where multiple ports point to the same remote port).

---

## Network Element Groups and Sites

---

A large network might consist of hundreds of network elements. Working with these network elements in a single flat topology **Map** might be impractical. To reduce clutter in the **Map** view, the proNX Service Manager allows you to arrange network elements into hierarchical groups. A group is represented by a single icon.

Network elements not belonging to any user-created group are placed in a default top level group. This top level container group is represented by the **Elements** entry in the **Network** tree view. All network elements contained at this level in the hierarchy are displayed in the top level **Map** view. You can assign network elements to groups during discovery, or you can move network elements to groups that you have created at a later stage.

PSM stores group associations in its database. This allows group associations to persist across PSM software upgrades.

Groups are hierarchical. For example, you can create a group called WALL\_ST that is inside a group called LOWER\_MANHATTAN that in turn is inside a group called MANHATTAN.

The lowest form of a group is called a site. A site is intended to represent network elements at the same location. For example, you can create a site called NYSE inside the WALL\_ST group. A site can be inside a group but a site cannot be nested in another site. Groups and sites share the same namespace.

The namespace for a group or a site is local to its location in the Network tree. In other words, you can create multiple WALL\_ST groups in different parts of the tree, but at each location in the tree, you can only have one group or site called WALL\_ST.



**NOTE:** Network element groups and sites are part of the replicated data set when running with multiple servers. For more information on replicated data, see [“Running Multiple Servers with Server Replication” on page 30](#).

- [Creating a New Group on page 87](#)
- [Moving Network Elements, Groups, And/or Sites to a Different Group on page 88](#)
- [Adding Network Elements to a New Group or Site on page 88](#)
- [Adding Groups And/or Sites to a New Group on page 89](#)
- [Navigating Between Parent and Child Groups on page 89](#)

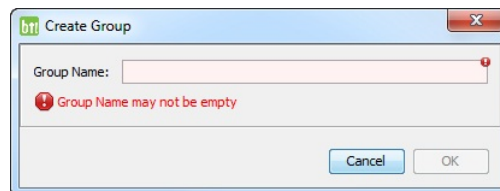
## Creating a New Group

Use this procedure to create a new group.

1. In the **Elements** branch in the **Network** tree view, perform one of the following actions:
  - Right click the **Elements** entry and select **Create Group** to create a new group at the top level of the tree.
  - Right click an existing group and select **Create Group** to create a new group nested inside that existing group.

You can also create a new group by right clicking an existing group in the topology **Map** view and selecting **Create Group**.

2. A pop-up dialog appears in which you can enter a name for the new group.



Enter a name and select **OK**. The name must be unique for all groups and sites at that location in the tree.

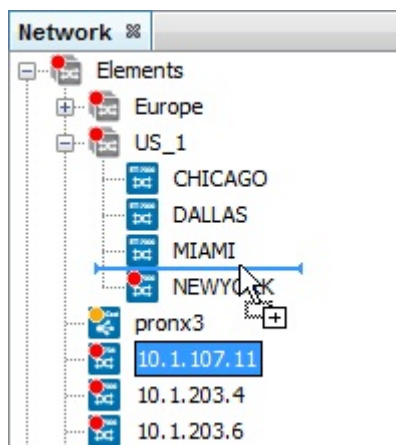


**NOTE:** Network element groups and sites are part of the replicated data set when running with multiple servers.

## Moving Network Elements, Groups, And/or Sites to a Different Group

Use this procedure to move network elements, groups, and/or sites to a different group.

1. Select the network elements, groups, and/or sites in the **Elements** branch of the **Network** tree view.
2. Click and drag the selections to the desired group as shown below.



**NOTE:** If you no longer want a network element to be part of any user-defined group, move it back to the top level Elements group.



**NOTE:** Network element groups and sites are part of the replicated data set when running with multiple servers. If a server in the cluster has not discovered the network elements being moved, that server will show the destination group with these network elements undiscovered.

## Adding Network Elements to a New Group or Site

Use this procedure to add network elements to a new group or to a new site.

This procedure creates a group or a site, and populates it with network elements in one step. You cannot use this procedure to add network elements to an existing group or site.

1. Select one or more network elements from the same level in the topology **Map** view or in the **Elements** branch of the **Network** tree view. Right click and choose **Add to... >Group** or **Add to... >Site** as desired.
2. A pop-up dialog appears in which you can enter a name for the group or site. Enter the name and click **OK**. The name must be unique for all groups and sites at that location in the tree.



**NOTE:** Network element groups and sites are part of the replicated data set when running with multiple servers. If a server in the cluster has not discovered the network elements being added, that server will show the new group or site with these network elements undiscovered.

## Adding Groups And/or Sites to a New Group

Use this procedure to add groups and/or sites to a new group.

This procedure creates a group and populates it with other groups and/or sites in one step. You cannot use this procedure to add groups and/or sites to an existing group.

1. Select one or more groups and/or sites from the same level in the topology **Map** view or in the **Elements** branch of the **Network** tree view. Right click and choose **Add to New Group**.
2. A pop-up dialog appears in which you can enter a name for the group. Enter the name and click **OK**. The name must be unique for all groups and sites at that location in the tree.

The new group is created at that location and the selected groups and/or sites are moved into it.



**NOTE:** Network element groups and sites are part of the replicated data set when running with multiple servers.

## Navigating Between Parent and Child Groups

Use this procedure to navigate between a child view of network elements inside a group and a parent view of the group itself.

1. To view the contents of a group in the topology **Map** view, select the group in the **Elements** branch of the **Network** tree view or double-click the group in the topology **Map** view.

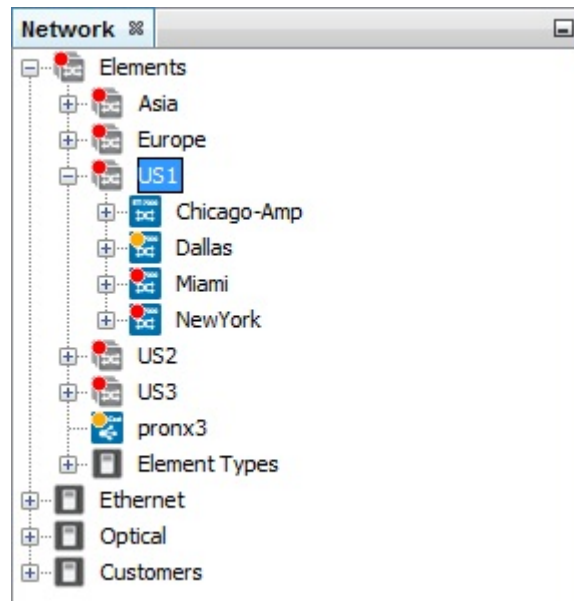


Figure 18: Map View Of Group Contents



**NOTE:** Network element groups are part of the replicated data set when running with multiple servers. You might see undiscovered network elements in this view if this group was created on another server and if your server has not been configured to discover the network elements in that group.

2. To go back to the parent, right-click in the background of the child and select **Show Parent**.

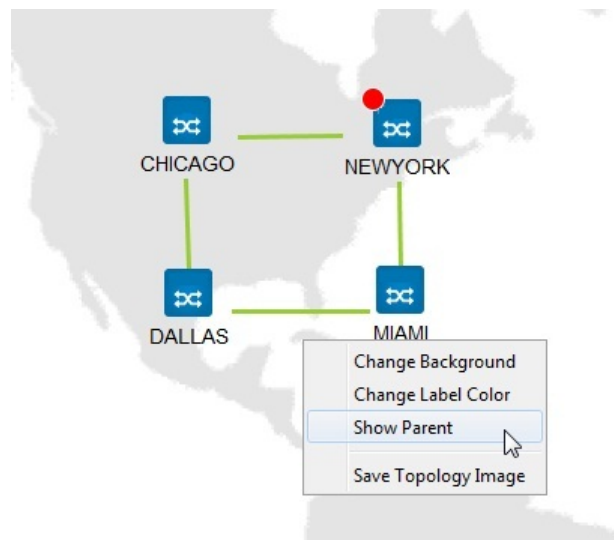


Figure 19: Map View Of Parent



## Changing the Background View

Use this procedure to change the background view in the topology window.



**NOTE:** The background view is part of the replicated data set when running with multiple servers. For more information on replicated data, see [“Running Multiple Servers with Server Replication”](#) on page 30.

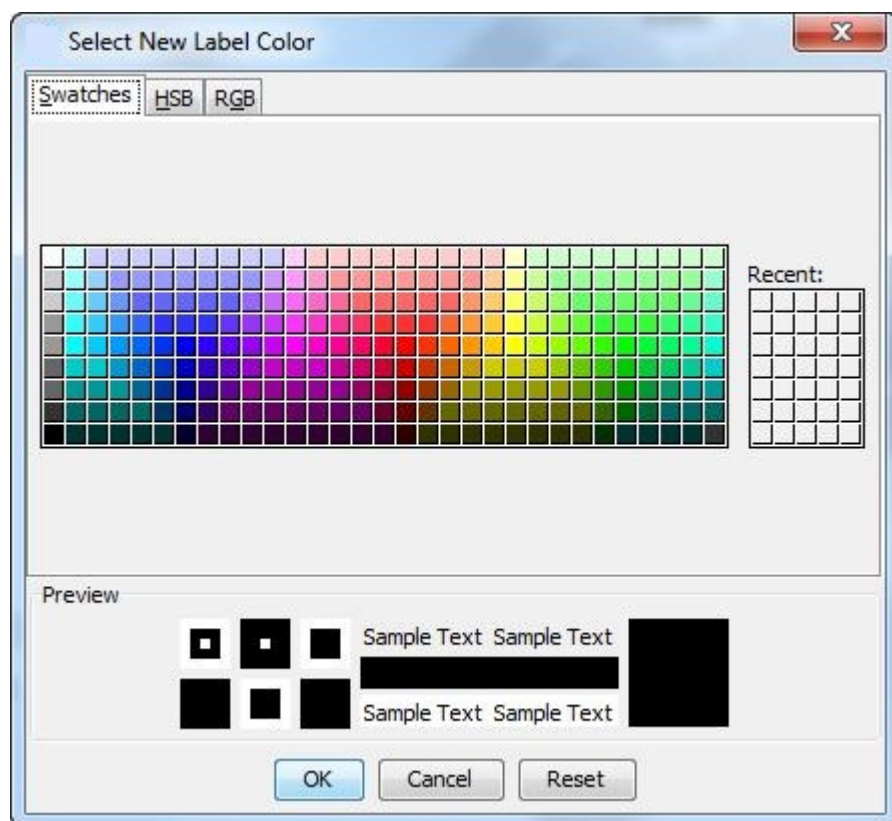
1. To change map view elements, right-click anywhere on the background map to display the menu as shown.



2. To change the default background map:
  - a. Create a .gif, .jpg or .png image that you want as your background.
  - b. Click **Change Background** in the menu shown above and navigate to the image you want as your background.
  - c. Click **Open**. The new background image displays in the map view. The tool automatically saves the new image file in the **backgrounds** folder in your PSM Client installation directory chain.
3. Changing the default background map might also require changing the default text color of the elements. To change the color of the text under each element in the map view:



- a. Click **Change Label Color**. The "Select New Label Color" window appears as shown.



- b. Choose a color category using the tabs Swatches, HSB or RGB.
- c. Click a text color and click **OK**. The text under each element in the map view changes to the selected color.
- d. To revert to the default text color, click **Reset**.



## CHAPTER 6

# Working with Network Elements

- [Editing Notes for a Network Element on page 95](#)
- [Identifying Services Associated with a Network Element on page 96](#)
- [Viewing Network Element Inventory Information on page 97](#)
- [Searching for a Network Element on page 99](#)
- [Managing Information for a Network Element on page 100](#)
- [Enabling or Disabling Network Element Maintenance Modes on page 111](#)
- [Marking or Unmarking a Network Element on page 112](#)
- [Enabling or Disabling Provisioning Mode on a Network Element on page 113](#)
- [Connecting to the CLI on a Network Element on page 114](#)
- [Provisioning OSPF on a BT17000 Series Management Network on page 114](#)
- [Configuring In-Band Management on a BT17800 Network Element on page 122](#)

### Editing Notes for a Network Element

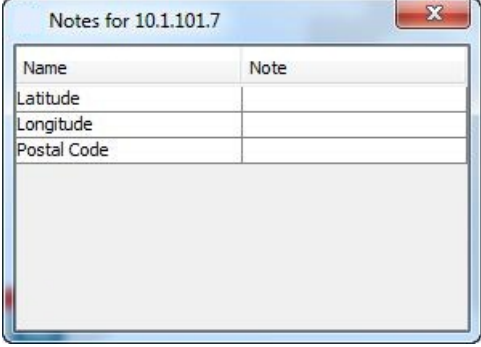
---

Use this procedure to add, delete, or modify notes on a discovered or undiscovered network element.

Notes are informational text that can be used to describe a network element.

1. To access the Notes window for an NE, right-click the NE in the Network tree or in the Topology Map view and choose **Node >Notes >Edit**.

The Notes window is displayed.

A screenshot of a window titled "Notes for 10.1.101.7". The window has a close button (X) in the top right corner. Inside the window, there is a table with two columns: "Name" and "Note". The table has four rows: "Latitude", "Longitude", "Postal Code", and a row with a large empty text area below it. The "Name" column is on the left and the "Note" column is on the right.

Name	Note
Latitude	
Longitude	
Postal Code	
<div></div>	

2. As desired, enter values for the existing note types (Longitude, Latitude, Postal Code) by clicking in the **Note** field and typing your data.
3. To add a new note, right-click the window and choose **New**.

A new row named **New Meta Key** is displayed. Click inside the **New Meta Key** box and enter a name for the new note. In the **Note** column, enter the applicable information. The new note is stored on the server.
4. To delete a note, right-click the note and choose **Delete**.

## Identifying Services Associated with a Network Element

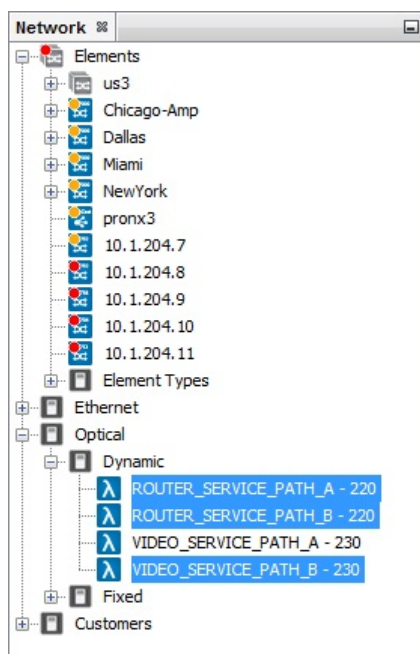
---

Use this procedure to determine the services that are associated with a network element.

proNX Service Manager allows the user to identify which services are associated with a network element, and copy the names of the services to a clipboard on their local drive. This feature is useful when alarms are raised against an NE and you want to identify which services are affected. It is also useful when performing maintenance on an NE to know which services the NE is part of to prevent a disruption of service.

1. To identify the services that an NE is part of, right-click the NE in the Network tree or in the Topology Map view, and choose **Select Services**.

The services that the NE is a member of are highlighted in the Services section of the Network tree view as shown in the following image. The first service highlighted in the tree view is also displayed in the Topology view.



2. To copy the names of the services associated with an NE to a clipboard on your local drive, right-click one of the highlighted services in the Network tree view and choose **Copy Name**.
3. Open the notepad or clipboard application on your local drive, and select paste.

## Viewing Network Element Inventory Information

Use this procedure to display inventory information for the managed network.

1. To view inventory information for the devices in your network, from the main menu choose **View>Network->Inventory**.

Figure 20: Network Inventory

Topology: Elements		Inventory	
System Name	System Location	Row Type	Version
172.27.7.116	NYC	BTI-718E	2.0
172.27.7.117	Ottawa	BTI-718E	2.0
10.127.11.11	Ottawa	BTI-7000	10.4.0 TPCLI 20
10.1.203.1	Ottawa	BTI-7000	10.4.0 C003
Chicago-Amp	Ottawa	BTI-7000	10.3.0 C007
Dallas	Ottawa	BTI-7000	10.3.0 C007
East	Ottawa	BTI-7000	10.3.0 C007
Miami	Ottawa	BTI-7000	10.3.0 C007
NewYork	Ottawa	BTI-7000	10.3.0 C007
Main Shelf 7200	MS-1		
7060 COOLING UNIT	FAN SLOT	CU	
7060 System Control Processor	SLOT-1-1	SCP	
7200 COMMON COMMUNICATION MODULE	SI-1-1	CCM	
7060 COOLING UNIT	FAN SLOT	CU	
7060 COOLING UNIT	FAN SLOT	CU	
7060 COOLING UNIT	FAN SLOT	CU	
10-PORT 10G MULTIPROTOCOL MUXPONDER - SDH EXT TEMP (ECI)	SLOT-1-19	MXP	
XFP	XFP-1-19-2	XFP	
XFP	XFP-1-19-1	XFP	
SFP	SFP-1-19-9	SFP	
SFP	SFP-1-19-12	SFP	
SFP	SFP-1-19-11	SFP	
SFP	SFP-1-19-10	SFP	
40ch DWDM - 2D ROADM	SLOT-1-15	ROB	
40ch DWDM - 2D ROADM	SLOT-1-9	ROB	
Dual 10G Multiprotocol Transponder	SLOT-1-7	DTPR	
12 PORT PACKETVX SERVICE AGGREGATION MODULE (2 XFP PORTS)	SLOT-1-11	PVX	
7200 MAIN SHELF INTERFACE	SI-1	MSI	

Figure 21: Network Inventory for PSM Server

Topology: Elements		Inventory	
System Name	System Location	Row Type	Version
mgtServ		WideCastOS	1.34.1
Processors			
GenuineIntel: Intel(R) Xeon(R) CPU E5540 @ 2.53GHz			
GenuineIntel: Intel(R) Xeon(R) CPU E5540 @ 2.53GHz			
GenuineIntel: Intel(R) Xeon(R) CPU E5540 @ 2.53GHz			
GenuineIntel: Intel(R) Xeon(R) CPU E5540 @ 2.53GHz			
RAM Storage			
7516MB			
Network Interfaces			
lo - 100Mb/s			
eth0 - 0Mb/s			
bond0 - 100Mb/s			
Fixed Storage			
/ - 8661MB			
/backups - 15717MB			
/boot - 1007MB			
/home - 15717MB			
/tmp - 10488MB			
/var - 15717MB			
/var/log - 31434MB			

- To select what inventory information to show, right-click the title bar and select or clear the headings to obtain the view that you desire.

<input checked="" type="checkbox"/>	HW REV: Hardware Revision
	Part Number: Part Number
<input checked="" type="checkbox"/>	PEC: PEC
<input checked="" type="checkbox"/>	Row Type: Row Type
<input checked="" type="checkbox"/>	Serial: Serial Number
	Shelf Id: Shelf Id
<input checked="" type="checkbox"/>	System Location: System Location
<input checked="" type="checkbox"/>	System Name
	Vendor: Vendor
<input checked="" type="checkbox"/>	Version: Software Version
	Wavelength: Wavelength

## Searching for a Network Element

Use this procedure to search for a network element.

1. Type a search string in the **Search** field in the toolbar. The results are displayed as you type.

You can search based on NE name, IP address, group, site, or service type. You can also search for unreachable network elements by typing in **unreachable** in the text box.

Figure 22: Searching for an IP Address

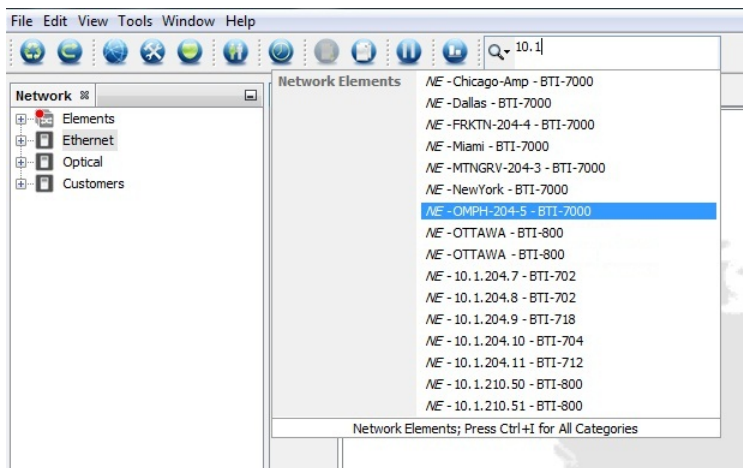


Figure 23: Selecting the Search Category

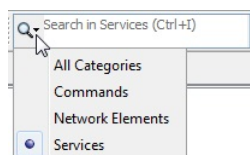
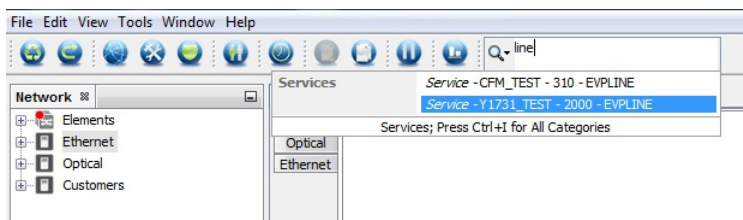


Figure 24: Searching for a Service Type



The search results are highlighted in the Network tree and Topology Map view.

## Managing Information for a Network Element

Use this procedure to view or update system-related information for an individual network element.

1. Right-click a network element in the Network tree or in the Topology Map view, and then select **System Info**.

The **System Info** tab appears.



The screenshot displays the configuration interface for a network element. On the left is a sidebar with tabs: System, Management, SNMP, Time/Date/NTP, and Craft Eth/Serial. The main area is divided into two sections: 'System Settings' and 'System Wide Settings'.

**System Settings**

**System Information**

Name: BTI7000	Location: BTI
Uptime: 5 days, 3:33:30	
Vendor: BTI Systems.	Active SW Version: 9.2.1 C001
Model: BTI 7060	Inactive SW Version: 9.2.0 C007
Serial Number: SE10500149 (SCP)	
Element Number: 0	Site Number: 0
Contact: UNKNOWN	

**System Wide Settings**

**System Wide Information**

Auto-Provisioning Mode: Auto In-Service

Auto-In Service Timer: 0 days 8 hours 0 minutes

Auto Deprovisioning Timer: 0 days 0 hours 0 minutes

Filter Plate Detection: Off

2. Click one of the following tabs to view or change information for the selected topic.

- **System**
- **Management**
- **SNMP**
- **Time/Date/NTP**
- **Craft Eth/Serial**



**NOTE:** Depending on the network element type, some fields can be edited, some cannot be edited, and some do not apply to that type. The information that cannot be edited, or that is not applicable, is greyed out.

Table 13: System Info Tab for BTI7000 Series NE

Panel Name	Description	Parameters
System	Provides access to general information.	<ul style="list-style-type: none"><li>• <b>System Settings</b><ul style="list-style-type: none"><li>• Name</li><li>• Location</li><li>• Uptime - not editable</li><li>• Vendor - not editable</li><li>• Model - not editable</li><li>• Active SW Version - not editable</li><li>• Inactive SW Version - not editable</li><li>• Serial Number - not editable</li><li>• Element Number</li><li>• Site Number</li><li>• Contact</li></ul></li><li>• <b>System Wide Settings</b><ul style="list-style-type: none"><li>• Auto-Provisioning Mode - this is the AINS mode</li><li>• Auto-In Service Timer</li><li>• Auto Deprovisioning Timer - not applicable for NEs running release 8.2 and higher</li><li>• Filler Plate Detection</li><li>• Customer Logging Facility ID</li></ul></li></ul>

Table 13: System Info Tab for BTI7000 Series NE (continued)

Panel Name	Description	Parameters
<b>Management</b>	<p>Provides access to management information.</p> <p><b>NOTE:</b> When Management information for an NE is modified, the NE is deleted from PSM and rediscovered using the updated settings.</p>	<ul style="list-style-type: none"> <li>• <b>Management Settings</b> <ul style="list-style-type: none"> <li>• Outband IP Address</li> <li>• Outband IP Mask</li> <li>• System Gateway</li> <li>• Mac Address - not editable</li> </ul> </li> <li>• <b>OSC Settings</b> <ul style="list-style-type: none"> <li>• Enable OSC 1 Port</li> <li>• Enable OSC 2 Port</li> <li>• Secondary Gateway</li> </ul> </li> <li>• <b>OSPF Management: OSPF</b> <ul style="list-style-type: none"> <li>• Router ID</li> <li>• Route Redistribution</li> <li>• Area ID</li> <li>• State</li> <li>• Delete OSPF</li> <li>• Add OSPF</li> </ul> </li> <li>• <b>OSPF Management: OSPF Interfaces</b> <ul style="list-style-type: none"> <li>• This is the list of OSPF interfaces configured on the network element.</li> <li>• Add, edit, or delete interfaces as desired.</li> </ul> </li> <li>• <b>OSPF Management: LSDB</b> <ul style="list-style-type: none"> <li>• This is the link state database. It is read-only.</li> </ul> </li> <li>• <b>OSPF Management: Neighbors</b> <ul style="list-style-type: none"> <li>• This is the list of OSPF neighbors. It is read-only.</li> </ul> </li> </ul> <p><b>NOTE:</b> For more information on provisioning OSPF, see <a href="#">“Provisioning OSPF on a BTI7000 Series Management Network” on page 114</a></p>
<b>SNMP</b>	<p>Provides access to read-only community and trap receiver information.</p>	<ul style="list-style-type: none"> <li>• <b>Communities</b> <ul style="list-style-type: none"> <li>• Private - not editable</li> <li>• Public - not editable</li> </ul> </li> <li>• <b>Trap Receivers</b> <ul style="list-style-type: none"> <li>• Trap Receivers - not editable</li> <li>• IP Address - not editable</li> <li>• Community - not editable</li> <li>• Version - not editable</li> <li>• Port - not editable</li> <li>• Notification - not editable</li> </ul> </li> </ul>

Table 13: System Info Tab for BTI7000 Series NE (continued)

Panel Name	Description	Parameters
<b>Time/Date/NTP</b>	Provides access to time, date, and NTP (Network Timing Protocol) settings.	<ul style="list-style-type: none"> <li>• <b>Time and Date Settings</b> <ul style="list-style-type: none"> <li>• Adjust time for daylight savings changes</li> <li>• Time</li> <li>• Time Zone</li> <li>• Date</li> </ul> </li> <li>• <b>NTP Settings</b> <ul style="list-style-type: none"> <li>• Poll Period</li> <li>• Authorization Key (0 to 65535)</li> <li>• Sync State - not editable</li> <li>• Stratum - not editable</li> <li>• Reference IP - not editable</li> <li>• NTP Associations (NTP Client IP addresses)</li> </ul> </li> </ul>
<b>Craft Eth/Serial</b>	Provides access to Craft Ethernet and Craft Serial information.	<ul style="list-style-type: none"> <li>• <b>Craft Serial Settings</b> <ul style="list-style-type: none"> <li>• Baud Rate</li> <li>• Data Bits</li> <li>• Parity</li> <li>• Stop Bits</li> </ul> </li> <li>• <b>Craft Ethernet Settings</b> <ul style="list-style-type: none"> <li>• Craft IP Address</li> <li>• Craft Mask</li> <li>• Media Rate - not editable</li> <li>• Custom</li> <li>• Craft MAC Address - not editable</li> <li>• Broadcast Address - not editable</li> <li>• Interface Speed - not editable</li> <li>• MTU Size - not editable</li> </ul> </li> </ul>

Table 14: System Info Tab for BT17800 Series NE

Panel Name	Description	Parameters
<b>System</b>	Provides access to general information.	<ul style="list-style-type: none"> <li>• <b>System Settings</b> <ul style="list-style-type: none"> <li>• Name</li> <li>• Location</li> <li>• Uptime - not editable</li> <li>• Vendor - not editable</li> <li>• Model - not editable</li> <li>• Active SW Version - not editable</li> <li>• Inactive SW Version - not applicable</li> <li>• Serial Number - not applicable</li> <li>• Element Number - not applicable</li> <li>• Site Number - not applicable</li> <li>• Contact</li> </ul> </li> <li>• <b>System Wide Settings</b> <ul style="list-style-type: none"> <li>• Auto-Provisioning Mode - this is the AINS mode</li> <li>• Auto-In Service Timer</li> <li>• Auto Deprovisioning Timer - not applicable</li> <li>• Filler Plate Detection - not applicable</li> <li>• Customer Logging Facility ID</li> </ul> </li> </ul>
<b>Management</b>	Provides access to management information.  <b>NOTE:</b> When Management information for an NE is modified, the NE is deleted from PSM and rediscovered using the updated settings.	<ul style="list-style-type: none"> <li>• <b>Management Settings</b> The following are the out-of-band management settings:               <ul style="list-style-type: none"> <li>• Outband IP Address - not editable</li> <li>• Outband IP Mask - not editable</li> <li>• System Gateway - not editable</li> <li>• Mac Address - not applicable</li> </ul> </li> <li>• <b>In-band Management Settings</b> This panel displays the in-band management interfaces.               <ul style="list-style-type: none"> <li>• Add or delete interfaces as desired.</li> <li>• Proxy ARP</li> <li>• IS-IS and NET</li> </ul> <b>NOTE:</b> For more information on provisioning in-band management, see <a href="#">“Configuring In-Band Management on a BT17800 Network Element” on page 122</a> </li> </ul>
<b>SNMP</b>	Provides access to read-only community and trap receiver information.	<ul style="list-style-type: none"> <li>• <b>Communities</b> <ul style="list-style-type: none"> <li>• Private - not editable</li> <li>• Public - not editable</li> </ul> </li> <li>• <b>Trap Receivers</b> <ul style="list-style-type: none"> <li>• Trap Receivers - not editable</li> <li>• IP Address - not editable</li> <li>• Community - not editable</li> <li>• Version - not editable</li> <li>• Port - not editable</li> <li>• Notification - not editable</li> </ul> </li> </ul>

Table 14: System Info Tab for BT17800 Series NE (continued)

Panel Name	Description	Parameters
<b>Time/Date/NTP</b>	Provides access to time, date, and NTP (Network Timing Protocol) settings.	<ul style="list-style-type: none"> <li>• <b>Time and Date Settings</b> <ul style="list-style-type: none"> <li>• Adjust time for daylight savings changes - not editable</li> <li>• Time - not editable</li> <li>• Time Zone - not editable</li> <li>• Date - not editable</li> </ul> </li> <li>• <b>NTP Settings</b> <ul style="list-style-type: none"> <li>• NTP Status - not editable</li> <li>• NTP Servers - not editable</li> </ul> </li> </ul>

Table 15: System Info Tab for BT1800 Series NE

Panel Name	Description	Parameters
<b>System</b>	Provides access to general information.	<ul style="list-style-type: none"> <li>• <b>System Settings</b> <ul style="list-style-type: none"> <li>• Name</li> <li>• Location</li> <li>• Uptime - not editable</li> <li>• Vendor - not editable</li> <li>• Model - not editable</li> <li>• Active SW Version - not editable</li> <li>• Inactive SW Version - not applicable</li> <li>• Serial Number - not applicable</li> <li>• Element Number - not applicable</li> <li>• Site Number - not applicable</li> <li>• Contact</li> </ul> </li> <li>• <b>System Wide Settings</b> - not applicable</li> </ul>
<b>Management</b>	Provides read-only access to management information.	<ul style="list-style-type: none"> <li>• <b>Management Settings</b> <ul style="list-style-type: none"> <li>• Outband IP Address - not editable</li> <li>• Outband IP Mask - not editable</li> <li>• System Gateway - not editable</li> <li>• Mac Address - not editable</li> </ul> </li> <li>• <b>In-band Settings</b> <ul style="list-style-type: none"> <li>• IP Address - not editable</li> <li>• IP Mask - not editable</li> <li>• Outer VLAN Name - not editable</li> <li>• Inner VLAN Name - not editable</li> <li>• Network Address - not editable</li> <li>• Mac Address - not editable</li> <li>• Outer VLAN Id (Priority) - not editable</li> <li>• Inner VLAN Id (Priority) - not editable</li> </ul> </li> </ul>

Table 15: System Info Tab for BT1800 Series NE (continued)

Panel Name	Description	Parameters
<b>SNMP</b>	Provides access to read-only community and trap receiver information.	<ul style="list-style-type: none"> <li>• <b>Communities</b> <ul style="list-style-type: none"> <li>• Private - not editable</li> <li>• Public - not editable</li> </ul> </li> <li>• <b>Trap Receivers</b> <ul style="list-style-type: none"> <li>• Trap Receivers - not editable</li> <li>• IP Address - not editable</li> <li>• Community - not editable</li> <li>• Port - not editable</li> </ul> </li> </ul>
<b>Time/Date/NTP</b>	Provides access to time and date settings.	<ul style="list-style-type: none"> <li>• <b>Time and Date Settings</b> <ul style="list-style-type: none"> <li>• Time</li> <li>• Time Zone</li> <li>• Date</li> </ul> </li> <li>• <b>NTP Settings</b> <p><b>NOTE:</b> You must disable NTP on the BT1810 prior to making any changes.</p> <p><b>NOTE:</b> NTP is always enabled on the BT1805, BT1821, and BT1822 devices.</p> <ul style="list-style-type: none"> <li>• Poll Period - read-only for the BT1805, BT1821, and BT1822.</li> <li>• Status - read-only for the BT1805, BT1821, and BT1822.</li> <li>• Preferred Server</li> <li>• Server1 IP Address</li> <li>• Server2 IP Address</li> <li>• Server3 IP Address</li> </ul> </li> </ul>
<b>Craft Eth/Serial</b>	Provides read-only access to Craft Serial information.	<ul style="list-style-type: none"> <li>• <b>Craft Serial Settings</b> <ul style="list-style-type: none"> <li>• Baud Rate - not editable</li> <li>• Data Bits - not editable</li> <li>• Parity - not editable</li> <li>• Stop Bits - not editable</li> </ul> </li> </ul>

Table 16: System Info Tab for MX Series and PTX Series Routers and QFX Series Switches

Panel Name	Description	Parameters
<b>System</b>	Provides access to general information.	<ul style="list-style-type: none"> <li>• <b>System Settings</b> <ul style="list-style-type: none"> <li>• Name</li> <li>• Location</li> <li>• Uptime - not applicable</li> <li>• Vendor - not applicable</li> <li>• Model - not applicable</li> <li>• Active SW Version - not applicable</li> <li>• Inactive SW Version - not applicable</li> <li>• Serial Number - not applicable</li> <li>• Element Number - not applicable</li> <li>• Site Number - not applicable</li> <li>• Contact</li> </ul> </li> </ul>
<b>Management</b>	Not supported.	
<b>SNMP</b>	Not supported.	
<b>Time/Date/NTP</b>	Not supported.	
<b>Craft Eth/Serial</b>	Not supported.	

Table 17: System Info Tab for BT1700 Series NE

Panel Name	Description	Parameters
<b>System</b>	Provides access to general information.	<ul style="list-style-type: none"> <li>• <b>System Settings</b> <ul style="list-style-type: none"> <li>• Name</li> <li>• Location</li> <li>• Uptime - not editable</li> <li>• Vendor - not editable</li> <li>• Model - not editable</li> <li>• Active SW Version - not editable</li> <li>• Inactive SW Version - not applicable</li> <li>• Model - not editable</li> <li>• Serial Number - not editable</li> <li>• Element Number - not applicable</li> <li>• Site Number - not applicable</li> <li>• Contact</li> </ul> </li> <li>• <b>System Wide Settings</b> - not applicable</li> </ul>
<b>Management</b>	Provides read-only access to management information.	<ul style="list-style-type: none"> <li>• <b>Management Settings</b> <ul style="list-style-type: none"> <li>• Outband IP Address - not editable</li> <li>• Outband IP Mask - not editable</li> <li>• System Gateway - not editable</li> <li>• Mac Address - not editable</li> </ul> </li> </ul>



Table 17: System Info Tab for BTI700 Series NE (continued)

Panel Name	Description	Parameters
<b>SNMP</b>	Provides access to read-only community and trap receiver information.	<ul style="list-style-type: none"> <li>• <b>Communities</b> <ul style="list-style-type: none"> <li>• Private - not editable</li> <li>• Public - not editable</li> </ul> </li> <li>• <b>Trap Receivers</b> <ul style="list-style-type: none"> <li>• Trap Receivers - not editable</li> <li>• IP Address - not editable</li> <li>• Community - not editable</li> <li>• Version - not editable</li> <li>• Port - not editable</li> <li>• Notification - not applicable</li> </ul> </li> </ul>
<b>Time/Date/NTP</b>	Provides access to time, date, and NTP (Network Timing Protocol) settings.	<ul style="list-style-type: none"> <li>• <b>Time and Date Settings</b> <ul style="list-style-type: none"> <li>• Adjust time for daylight savings changes - not applicable</li> <li>• Time</li> <li>• Time Offset - not editable</li> <li>• Date</li> </ul> </li> <li>• <b>NTP Settings (BTI700 Series except for BTI718E)</b> <ul style="list-style-type: none"> <li>• NTP VLANs - with Mode set to Client <ul style="list-style-type: none"> <li>• Mode set to Client</li> <li>• NTP Server IP</li> <li>• Static IP Address in CIDR notation (e.g. 10.0.0.1/24)</li> <li>• Time Flag</li> <li>• Time Offset</li> </ul> </li> <li>• Non NTP VLANs - with Mode set to None <ul style="list-style-type: none"> <li>• Mode set to None</li> <li>• NTP Server IP - not applicable</li> <li>• Static IP Address in CIDR notation (e.g. 10.0.0.1/24)</li> <li>• Time Flag - not applicable</li> <li>• Time Offset - not applicable</li> </ul> </li> </ul> </li> <li>• <b>NTP Settings (BTI718E)</b> <ul style="list-style-type: none"> <li>• Sntp Master - not editable</li> <li>• Sntp Stratum - not editable</li> <li>• Sntp Server Send Interval - enter the power (of 2) seconds (e.g. enter 4 for 2<sup>4</sup> seconds)</li> <li>• Sntp Client Send Interval - enter the power (of 2) seconds</li> <li>• Peer - can add or delete a peer; cannot edit an existing peer</li> <li>• Peer Work Mode - not editable</li> <li>• Peer IP - specify for a new peer; not editable for an existing peer</li> <li>• Peer SNTP Version - not editable</li> <li>• Peer ReceivedTime - not editable</li> </ul> </li> </ul>

Table 18: System Info Tab for OPS, EDFA, and RAMAN Devices

Panel Name	Description	Parameters
<b>System</b>	Provides access to general information.	<ul style="list-style-type: none"> <li>• <b>System Settings</b> <ul style="list-style-type: none"> <li>• Name</li> <li>• Location</li> <li>• Uptime - not editable</li> <li>• Vendor - not editable</li> <li>• Model - not editable</li> <li>• Active SW Version - not editable</li> <li>• Inactive SW Version - not applicable</li> <li>• Model - not editable</li> <li>• Serial Number - not editable</li> <li>• Element Number - not applicable</li> <li>• Site Number - not applicable</li> <li>• Contact</li> </ul> </li> <li>• <b>System Wide Settings</b> - not applicable</li> </ul>
<b>Management</b>	Provides read-only access to management information.	<ul style="list-style-type: none"> <li>• <b>Management Settings</b> <ul style="list-style-type: none"> <li>• Outband IP Address - not editable</li> <li>• Outband IP Mask - not editable</li> <li>• System Gateway - not editable</li> <li>• Mac Address - not editable</li> </ul> </li> </ul>
<b>SNMP</b>	Provides read-only access to community and trap receiver information.	<ul style="list-style-type: none"> <li>• <b>Communities</b> - not editable</li> <li>• <b>Trap Receivers</b> - not editable</li> </ul>
<b>Time/Date/NTP</b>	Provides read-only access to time and date settings.	<ul style="list-style-type: none"> <li>• <b>Time and Date Settings</b> - not editable</li> </ul>

Table 19: System Info Tab for PSM Server

Panel Name	Description	Parameters
<b>System</b>	Provides access to general information.	<ul style="list-style-type: none"> <li>• <b>System Settings</b> <ul style="list-style-type: none"> <li>• Name - not editable</li> <li>• Location - not editable</li> <li>• Uptime - not editable</li> <li>• Vendor - not editable</li> <li>• Model - not editable</li> <li>• Active SW Version - not editable</li> <li>• Element Number - not editable</li> <li>• Site Number - not editable</li> <li>• Contact - not editable</li> </ul> </li> </ul>

Table 19: System Info Tab for PSM Server (continued)

Panel Name	Description	Parameters
Management	Provides read-only access to IP information.	<ul style="list-style-type: none"> <li>• <b>Management Settings</b> <ul style="list-style-type: none"> <li>• Outband IP Address - not editable</li> <li>• Outband IP Mask - not editable</li> <li>• System Gateway - not editable</li> <li>• Mac Address - not editable</li> </ul> </li> </ul>
SNMP	Not supported.	
Time/Date/NTP	Not supported.	
Craft Eth/Serial	Not supported.	

3. Click **Apply Changes** to save the settings or **Discard Edits** to revert to the previous settings.

## Enabling or Disabling Network Element Maintenance Modes

Use this procedure to enable or disable maintenance modes for a network element.

Network elements can be placed into one of three maintenance modes:

- **Maintenance** - When a network element is placed into Maintenance mode, all communications between PSM and the network element are disabled with the exception of alarms, which continue to be processed.
- **Out of Service** - When a network element is placed in Out of Service mode, all communications between PSM and the network element are disabled (including alarms).
- **Quiet** - When a network element is placed into Quiet mode, alarms are not processed.



**NOTE:** These modes are internal to PSM, and govern how PSM responds to and acts on network element messages. These modes are not set on the actual network elements themselves.



**NOTE:** Maintenance modes are part of the replicated data set when running with multiple servers. For more information on replicated data, see [“Running Multiple Servers with Server Replication”](#) on page 30.

1. To place one or more network elements into a maintenance mode:

- a. Select the network element(s) in the Network tree or in the Topology Map view, then right-click and choose **Mode >Maintenance Mode**, **Mode >Out of Service**, or **Mode >Quiet**.



**NOTE:** Modes are mutually exclusive. Only one mode can be selected at a time.

- b. Click **OK** in the ensuing dialog to confirm the action.

The NE(s) is placed in the specified mode and shown in a lighter shade.

2. To confirm that the NE(s) is in the desired mode, hover over the NE.

In the tooltip that appears, check the setting under **Mode**.

3. To disable a maintenance mode on one or more network elements:

- a. Select the network element(s) in the Network tree or in the Topology Map view, then right-click and select **Mode >Disable Maintenance Mode**, **Mode >Disable Out of Service**, or **Mode >Disable Quiet**, as applicable.

The NE(s) is shown back in its regular shade.

---

## Marking or Unmarking a Network Element

---

Use this procedure to mark or unmark a network element. A marked network element



allows you to visually distinguish that network element from other network elements, such as to highlight an important node or nodes in the network, or to flag a node to other users in the system.



**NOTE:** Marking is implemented as a mode, which is part of the replicated data set when running with multiple servers. For more information on replicated data, see [“Running Multiple Servers with Server Replication” on page 30](#).

1. To mark one or more network elements:

- a. Select the network element(s) in the Network tree or in the Topology Map view, then right-click and choose **Mode >Marked**.



**NOTE:** Modes are mutually exclusive. Only one mode can be selected at a time.

- b. Click **OK** in the ensuing dialog to confirm the action.

The NE(s) is now shown with a mark in the Topology Map view and in the Network tree.

2. To remove a mark on one or more network elements:
  - a. Select the network element(s) in the Network tree or in the Topology Map view, then right-click and select **Mode >Disable Marked**.

The NE(s) is shown with the mark removed.

## Enabling or Disabling Provisioning Mode on a Network Element

Use this procedure to enable or disable provisioning mode on a network element. If you configure a network element while provisioning mode is enabled, you will be able to see the new configuration data in PSM very quickly (without having to wait for the asynchronous update from the NE). Note that you might have to Refresh from Server to update the client view if you do not want to wait for the client view to be updated automatically.

In general, only one NE in the managed network should be in provisioning mode at any given time.



**NOTE:** Provisioning mode is part of the replicated data set when running with multiple servers. For more information on replicated data, see [“Running Multiple Servers with Server Replication” on page 30](#).

1. To enable provisioning mode on a network element:
  - a. Select the network element in the Network tree or in the Topology Map view, then right-click and choose **Mode >Provisioning >5 Minutes, 10 Minutes, or 15 Minutes**.



**NOTE:** Provisioning mode settings are mutually exclusive. Only one time period can be selected.

- b. Click **OK** in the ensuing dialog to confirm the action.

PSM enables provisioning mode for the selected NE for the specified time period.

2. To disable provisioning mode on a network element:
  - a. Select the network element in the Network tree or in the Topology Map view, then right-click and select **Mode >Provisioning >Disable 5 Minutes, Disable 10 Minutes, or Disable 15 Minutes**, as applicable.

PSM disables provisioning mode for the selected NE.

## Connecting to the CLI on a Network Element

---

Use this procedure to connect to the CLI on a network element.



**NOTE:** To connect to the CLI, you must first set up the appropriate command and command parameters. See [“Setting Utility Executables” on page 280](#).

1. Right-click a network element in the Network tree or in the topology Map view and select **Utilities > CLI**.

The CLI is launched using the application specified in [“Setting Utility Executables” on page 280](#).

## Provisioning OSPF on a BTI7000 Series Management Network

---

- [Adding OSPF Management on page 114](#)
- [Editing OSPF Management Settings on page 115](#)
- [Deleting OSPF Management on page 116](#)
- [Adding an OSPF Management Interface on page 117](#)
- [Editing an OSPF Management Interface on page 119](#)
- [Deleting an OSPF Management Interface on page 121](#)

### Adding OSPF Management

Use this procedure to add OSPF to the management network of a BTI7000 Series network element.

1. Right-click a network element in the Network tree or in the Topology Map view, and then select **System Info**.

The **System Info** window appears.

2. Click the **Management** tab to see the management parameters.

The Management panel appears.

The screenshot shows three stacked configuration panels in a web interface:

- Management Settings:** Contains 'Management Information' with fields for Outband IP Address (10.10.20.202), Outband IP Mask (255.192.0.0), System Gateway (10.1.1.1), and MAC Address (00:14:d0:30:c9:0d).
- OSC Settings:** Contains 'OSC Information' with checkboxes for 'Enable OSC 1 Port' and 'Enable OSC 2 Port' (both unchecked), and a 'Secondary Gateway' field (0.0.0.0).
- OSPF Management:** Has tabs for 'OSPF', 'OSPF Interfaces', 'LSDB', and 'Neighbors'. The 'OSPF' tab is active, showing fields for Router ID, Route Redistribution (a dropdown menu), Area ID (0.0.20.208), and a 'State Management' section with a 'State' dropdown menu set to 'Enabled'. An 'Add OSPF' button is at the bottom left.

3. Select **Add OSPF** to add OSPF.



**NOTE:** If OSPF has previously been added, the Add OSPF button is not available for selection.

4. Configure OSPF parameters as follows:
  - **Router ID:** Specify the OSPF router identifier.
  - **Route Redistribution:** Use the drop-down menu to specify how routes are redistributed.
  - **Area ID:** Specify the OSPF area identifier.
  - **State:** Set to **Enabled** or **Disabled**.
5. When you are finished, click **Apply Changes**.

## Editing OSPF Management Settings

Use this procedure to edit OSPF management settings on a BT17000 Series network element.

1. Right-click a network element in the Network tree or in the Topology Map view, and then select **System Info**.

The **System Info** window appears.

2. Click the **Management** tab to see the management parameters.

The Management panel appears.

The screenshot shows the 'Management Settings' window with three main sections:

- Management Settings**: Contains 'Management Information' with fields for Outband IP Address (10.1.212.1), Outband IP Mask (255.192.0.0), System Gateway (10.1.1.1), and MAC Address (00:14:d0:00:2c:28).
- OSC Settings**: Contains 'OSC Information' with checkboxes for 'Enable OSC 1 Port' and 'Enable OSC 2 Port', and a 'Secondary Gateway' field (0.0.0.0).
- OSPF Management**: Contains tabs for 'OSPF', 'OSPF Interfaces', 'LSDB', and 'Neighbors'. The 'OSPF' tab is active, showing fields for Router ID (10.1.212.1), Route Redistribution (None), Area ID (0.0.20.208), and State Management (State: Disabled). A 'Delete OSPF' button is at the bottom.

3. Configure OSPF parameters as follows:
  - **Router ID**: Specify the OSPF router identifier.
  - **Route Redistribution**: Use the drop-down menu to specify how routes are redistributed.
  - **Area ID**: The OSPF area identifier is read-only. It is set when you initially add OSPF management.
  - **State**: Set to **Enabled** or **Disabled**.
4. When you are finished, click **Apply Changes**.

## Deleting OSPF Management

Use this procedure to delete OSPF from the management network on a BTI7000 Series network element.



1. Right-click a network element in the Network tree or in the Topology Map view, and then select **System Info**.

The **System Info** window appears.

2. Click the **Management** tab to see the management parameters.

The Management panel appears.

The screenshot shows the 'Management Settings' window with three main sections:

- Management Information:** Contains fields for Outband IP Address (10.1.212.1), Outband IP Mask (255.192.0.0), System Gateway (10.1.1.1), and MAC Address (00:14:d0:00:2c:28).
- OSC Settings:** Contains checkboxes for 'Enable OSC 1 Port' and 'Enable OSC 2 Port', and a 'Secondary Gateway' field (0.0.0.0).
- OSPF Management:** Contains tabs for 'OSPF', 'OSPF Interfaces', 'LSDB', and 'Neighbors'. The 'OSPF' tab is active, showing fields for Router ID (10.1.212.1), Route Redistribution (None), Area ID (0.0.20.208), and a 'State Management' section with a 'State' dropdown set to 'Disabled'. A 'Delete OSPF' button is at the bottom left.

3. Click **Delete OSPF**.
4. Click **Yes** in the confirmation dialog.
5. When you are finished, click **Apply Changes**.

## Adding an OSPF Management Interface

Use this procedure to add an OSPF management interface to a BTI7000 Series network element.

### Prerequisites:

- The desired GCC and ODCC interfaces are created. See [“Provisioning GCC” on page 165](#) and [“Editing OSC Parameters in an Optical Group” on page 177](#) respectively.

1. Right-click a network element in the Network tree or in the Topology Map view, and then select **System Info**.

The **System Info** window appears.

2. Click the **Management** tab to see the management parameters.

The Management panel appears.

**Management Settings**

Management Information

Outband IP Address: 10.1.212.1      System Gateway: 10.1.1.1

Outband IP Mask: 255.192.0.0      MAC Address: 00:14:d0:00:2c:28

**OSC Settings**

OSC Information

Enable OSC 1 Port: ☐      Enable OSC 2 Port: ☐      Secondary Gateway: 0.0.0.0

**OSPF Management**

OSPF    OSPF Interfaces    LSDB    Neighbors

Router ID: 10.1.212.1

Route Redistribution: None

Area ID: 0.0.20.208

State Management

State: Disabled

Delete OSPF

3. Select the **OSPF Interfaces** tab.

A list of OSPF interfaces is shown.

4. Click **Add** to add a new OSPF interface.

The **Add OSPF Interface** dialog appears.

5. Configure the OSPF interface parameters as follows:
  - **Source:** Specify the interface from the drop-down menu. Only interfaces that can be configured for OSPF are shown.
  - **Hello Interval:** Set the OSPF hello interval.
  - **Retransmit Interval:** Specify the OSPF retransmit interval.
  - **Priority:** Set the priority.
  - **Dead Interval:** Set the dead interval.
  - **Transmit Delay:** Set the transmit delay.
  - **State:** Set to **Enabled** or **Disabled**.
6. When you are finished, click **Apply Changes**.

## Editing an OSPF Management Interface

Use this procedure to edit an OSPF management interface on a BT17000 Series network element.

1. Right-click a network element in the Network tree or in the Topology Map view, and then select **System Info**.

The **System Info** window appears.

2. Click the **Management** tab to see the management parameters.

The Management panel appears.

The screenshot shows three stacked configuration panels in a web interface:

- Management Settings:** Contains fields for Outband IP Address (10.1.212.1), System Gateway (10.1.1.1), Outband IP Mask (255.192.0.0), and MAC Address (00:14:d0:00:2c:28).
- OSC Settings:** Contains checkboxes for Enable OSC 1 Port and Enable OSC 2 Port (both unchecked), and a Secondary Gateway field (0.0.0.0).
- OSPF Management:** Has tabs for OSPF, OSPF Interfaces, LSDB, and Neighbors. The OSPF tab is active, showing Router ID (10.1.212.1), Route Redistribution (None), Area ID (0.0.20.208), and a State Management section with a State dropdown set to Disabled. A Delete OSPF button is at the bottom left.

3. Select the **OSPF Interfaces** tab.

A list of OSPF interfaces is shown.

4. Right-click an interface and select **Edit**.

The **Edit OSPF Interface** dialog appears.

The screenshot shows the 'Edit OSPF Interface' dialog box with the following fields and values:

- Source:** OSPF-1-3-0 (dropdown menu)
- Priority:** 1
- Hello Interval:** 10
- Dead Interval:** 40
- Retransmit Interval:** 5
- Transmit Delay:** 1
- State Management:** State dropdown set to Enabled

Buttons at the bottom: Cancel and OK.

5. Configure the OSPF interface parameters as follows:

- **Source:** This is the identifier of the interface being edited. It is read-only.
- **Hello Interval:** Set the OSPF hello interval.
- **Retransmit Interval:** Specify the OSPF retransmit interval.
- **Priority:** Set the priority.
- **Dead Interval:** Set the dead interval.

- **Transmit Delay:** Set the transmit delay.
- **State:** Set to **Enabled** or **Disabled**.

Click **OK** to close the **Edit OSPF Interface** dialog.

- When you are finished, click **Apply Changes**.

## Deleting an OSPF Management Interface

Use this procedure to delete an OSPF management interface on a BT17000 Series network element.

- Right-click a network element in the Network tree or in the Topology Map view, and then select **System Info**.

The **System Info** window appears.

- Click the **Management** tab to see the management parameters.

The Management panel appears.

The screenshot shows the **Management Settings** window with three main sections:

- Management Information:** Contains fields for Outband IP Address (10.1.212.1), Outband IP Mask (255.192.0.0), System Gateway (10.1.1.1), and MAC Address (00:14:d0:00:2c:28).
- OSC Settings:** Contains fields for Enable OSC 1 Port (unchecked), Enable OSC 2 Port (unchecked), and Secondary Gateway (0.0.0.0).
- OSPF Management:** Contains tabs for OSPF, OSPF Interfaces, LSDB, and Neighbors. The OSPF tab is active, showing Router ID (10.1.212.1), Route Redistribution (None), Area ID (0.0.20.208), and State Management (State: Disabled). A **Delete OSPF** button is at the bottom left.

- Select the **OSPF Interfaces** tab.

A list of OSPF interfaces is shown.

- Select an interface and click **Delete**.

5. Click **Yes** in the confirmation dialog.
6. When you are finished, click **Apply Changes**.

## Configuring In-Band Management on a BTI7800 Network Element

Use this procedure to configure in-band management on a BTI7800 network element.

Prerequisites:

- Ensure there is at least one optical interface configured. The BTI7800 supports in-band management on its optical interfaces only.

1. Right-click a network element in the Network tree or in the Topology Map view, and then select **System Info**.

The **System Info** window appears.

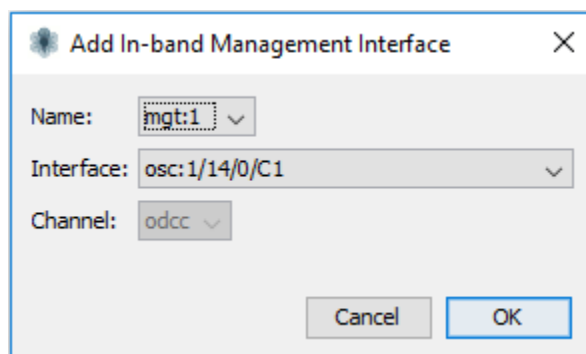
2. Click the **Management** tab to see the management parameters.

The Management panel appears.

The screenshot shows the 'Management Settings' window. The left sidebar has tabs for System, Management, SNMP, Time/Date/NTP, and Craft/EtherSerial. The 'Management' tab is active. The main content area is split into two panels. The top panel, 'Management Information', contains four input fields: 'Outband IP Address' (10.228.221.33), 'System Gateway' (10.228.0.1), 'Outband IP Mask' (255.255.0.0), and 'MAC Address' (N/A). The bottom panel, 'In-band Management', contains a table with columns 'Name', 'Interface', 'Type', and 'Channel'. Below the table are checkboxes for 'Proxy ARP' and 'IS-IS', and a 'NET:' field. 'Add' and 'Delete' buttons are also present.

3. To add a management interface:

- a. Click **Add** to bring up the Add In-band Management Interface dialog.



The dialog box titled "Add In-band Management Interface" contains three dropdown menus: "Name" with "mgt:1" selected, "Interface" with "osc:1/14/0/C1" selected, and "Channel" with "odcc" selected. At the bottom right are "Cancel" and "OK" buttons.

- b. Use the drop-down menu to specify the **Name** of the management interface you want to add.
- c. Use the drop-down menu to specify the actual **Interface** for this management interface.



**NOTE:** The BT17800 supports in-band management connectivity over the ODCC Channel only.

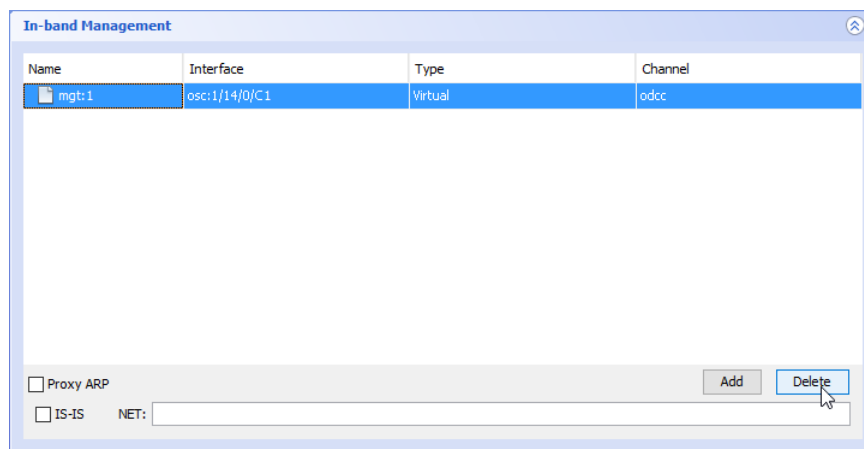
- d. Click **OK**.

The Add In-band Management Interface dialog closes and the new interface is shown in the in-band management interface list.

Repeat this step as necessary to add additional management interfaces.

4. To delete a management interface:

- a. Select an interface from the list of in-band management interfaces and click **Delete**.



The "In-band Management" window displays a table with the following data:

Name	Interface	Type	Channel
mgt:1	osc:1/14/0/C1	Virtual	odcc

Below the table are checkboxes for "Proxy ARP" and "IS-IS", a "NET:" field, and "Add" and "Delete" buttons. A mouse cursor is pointing at the "Delete" button.

- b. Click **Yes** in the confirmation dialog.

The selected interface is removed from the in-band management interface list.

Repeat this step as necessary to delete additional management interfaces.

5. Select or clear **Proxy ARP** to enable or disable proxy ARP.

Proxy ARP allows the BTI7800 to respond to ARP requests on the external system management interface on behalf of same-subnet network elements reachable through in-band channels.

6. Select or clear **IS-IS** to enable or disable IS-IS routing on the management interfaces.



**NOTE:** IS-IS is supported on BTI7800 release 4.1 and higher.

7. If you enable IS-IS, then specify the network entity title (**NET**).

The network entity title consists of a 3-octet area address, a 6-octet system identifier, and a 1-octet NSAP selector (which must be 00): aa.aaaa.ssss.ssss.ssss.00

- aa.aaaa - 6 hexadecimal digits for the area (consisting of a 2-digit format identifier followed by a domain)
- ssss.ssss.ssss - 12 hexadecimal digits for the system identifier, which must be unique to the area

8. When you are finished, click **Apply Changes**.



## CHAPTER 7

# Working with the Shelf View

- [Introduction on page 125](#)
- [Displaying Network Elements in the Shelf View on page 125](#)
- [Displaying Alarms from the Shelf View on page 129](#)
- [Setting the Remote ID from the Shelf View on page 129](#)
- [Deleting the Remote ID from the Shelf View on page 130](#)

### Introduction

---

PSM can display a visual representation of a discovered network element, along with visual indications of alarmed ports or components on that shelf. If the selected network element is unreachable, PSM displays the last known state for that element.

PSM supports the Shelf view for the following:

- BT17800 Series network elements
- BT17000 Series network elements
- BT1800 Series network elements
- BT1700 Series network elements
- MX Series and PTX Series routers
- QFX Series switches

### Displaying Network Elements in the Shelf View

---

Use this procedure to display the shelf view for a network element.

1. To display the shelf view of an NE, right-click the NE in either the Network tree or the topology Map view and choose **Node >View**.

If one or more alarms exist on a component, the component is colored red (critical), amber (major), or yellow (minor) to indicate the highest severity alarm on that component.

The following figures show the shelf view for various network elements.

Figure 25: Shelf View for a BT17814 Network Element

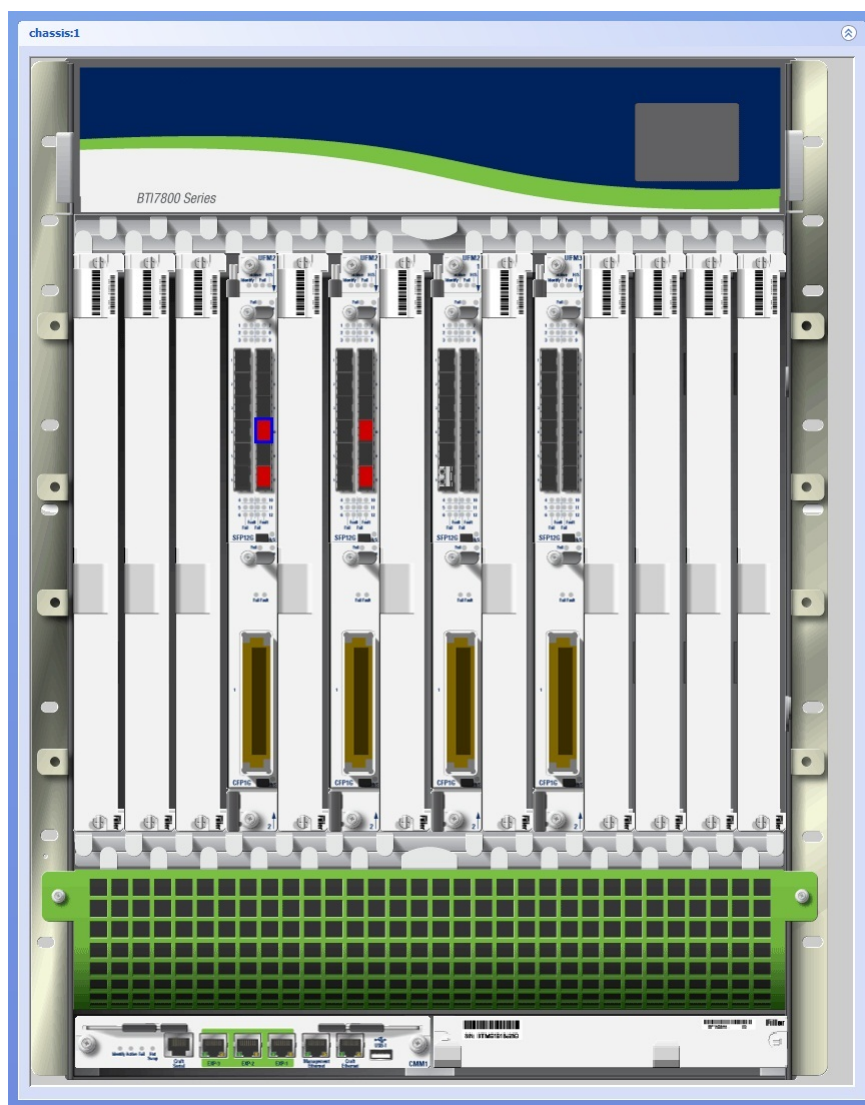


Figure 26: Shelf View for an MX240 Router



Figure 27: Shelf View for a BTI7200 Network Element

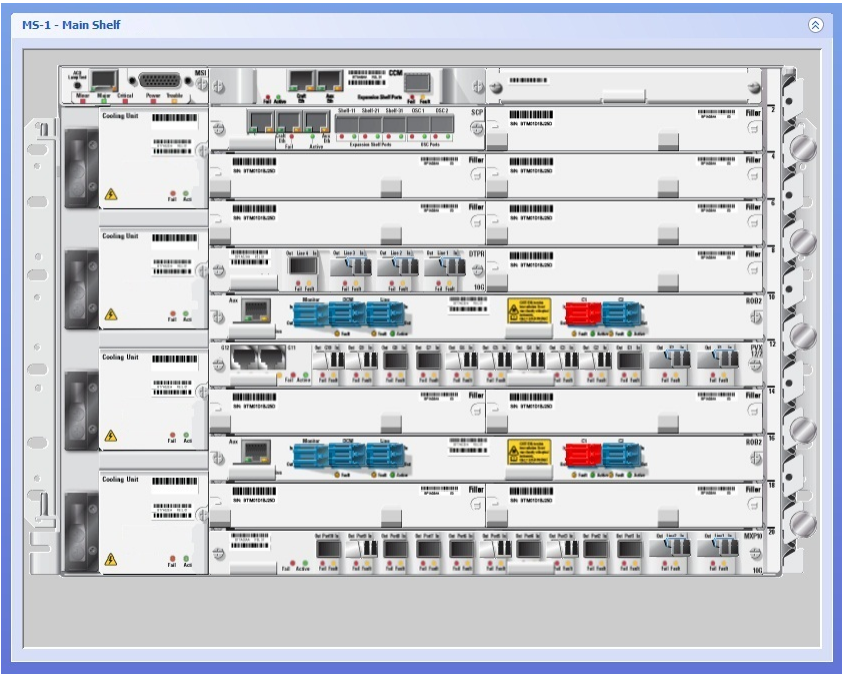


Figure 28: Shelf View for a BTI718E Network Element

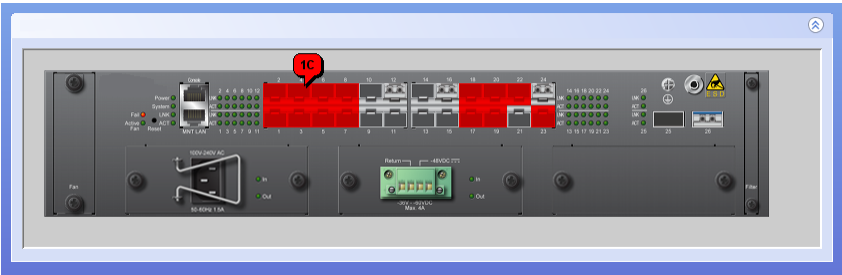


Figure 29: Shelf View for a BT1805 Network Element



Figure 30: Shelf View for a BT1810 Network Element

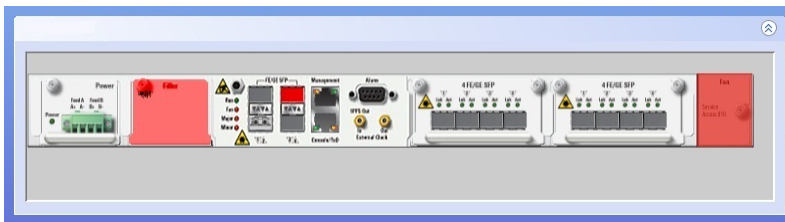
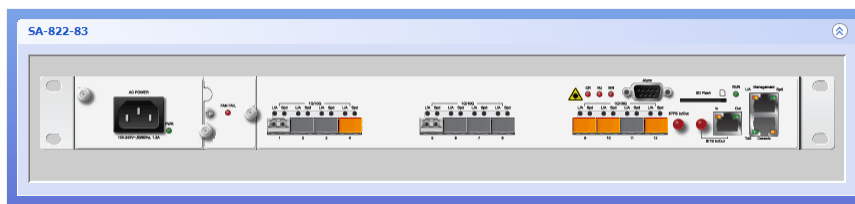


Figure 31: Shelf View for a BT1821 Network Element

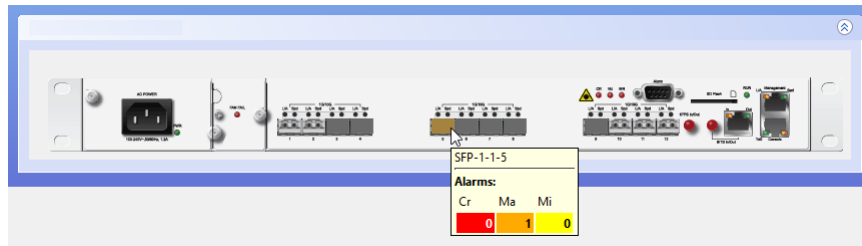


Figure 32: Shelf View for a BT1822 Network Element



**NOTE:** You can also use Quick View to bring up the Shelf view. First, select the network element in the Network tree, and then depress <ctl> <alt> v. The shelf view comes up in a modal window. To close the modal window, click anywhere outside the modal window.

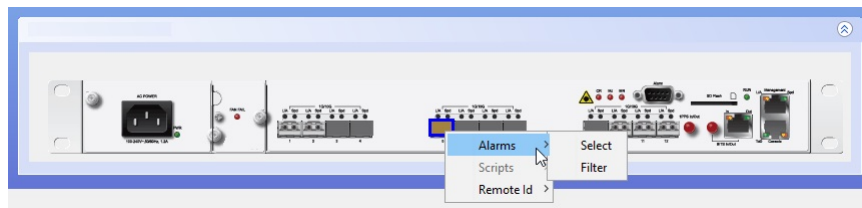
2. Hover over the alarmed component to see an alarm summary.



## Displaying Alarms from the Shelf View

Use this procedure to display the outstanding alarms on the selected component in the Shelf view.

1. To display alarm details for the alarmed component from the Shelf view, right-click the alarmed component and choose **Select** or **Filter**.



When **Select** is chosen, the alarms pane appears with the alarm(s) for the selected component highlighted. When **Filter** is chosen, PSM applies a filter to the alarms pane to show only alarms for the selected component. For information on managing alarms, see *Introduction*.

## Setting the Remote ID from the Shelf View

Use this procedure to set the Remote ID on an existing port in the Shelf view.

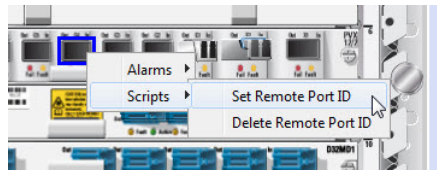
This is supported on BT17000 Series and BT1800 Series NEs only. For more information on Remote IDs, see “[Deriving Topology Using Remote IDs](#)” on page 74.



**NOTE:** PSM connects to the NE using the login credentials that you supplied when you connected to the PSM server. Therefore this NE must be configured with those same login credentials for this procedure to be successful.

To use this procedure, the cards and ports must already be provisioned.

1. To set the Remote ID on a port, right-click the port and choose **Remote Id > Set Remote Port Id**.



The **Set Remote Port ID** dialog appears.

 A screenshot of the 'Set Remote Port ID' dialog box. The dialog has two main sections: 'Local Port ID' and 'Far End'. The 'Local Port ID' section contains a text field with the value '10.10.20.99-PVX-1-13-X2'. The 'Far End' section contains a 'Remote Id:' text field, 'Clear' and 'Reset' buttons, and an 'Edit' section. The 'Edit' section includes fields for 'Hostname/IP Address', 'CP Type' (a dropdown menu), 'Shelf' (a dropdown menu), 'Slot' (a dropdown menu), 'Port' (a text field), and checkboxes for 'Alien' and 'Bidirectional'. At the bottom of the dialog are 'Cancel' and 'OK' buttons.

2. Configure the Remote ID. See [“Remote ID Configuration”](#) on page 78 for an explanation of the attributes.
3. Click OK.



**NOTE:** If you select **Bidirectional** and you specify a Remote ID that cannot be reconciled, PSM will be unable to configure the remote endpoint, and the task will fail.



**NOTE:** The task might fail if you try to use this procedure on a card that has not been provisioned.

## Deleting the Remote ID from the Shelf View

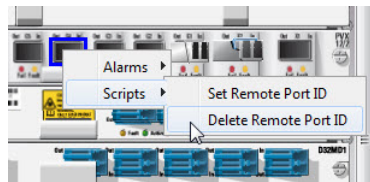
Use this procedure to delete the Remote ID from a port in the Shelf view.

This is supported on BTI7000 Series and BTI800 Series NEs only.

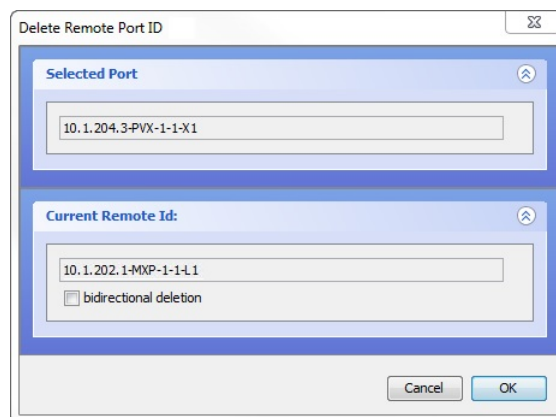


**NOTE:** PSM connects to the NE using the login credentials that you supplied when you connected to the PSM server. Therefore the NE must be configured with those same login credentials for this procedure to be successful.

1. To delete the Remote ID, right-click the port and choose **Remote Id >Delete Remote Port Id**.



The **Delete Remote Port ID** dialog appears.



2. To delete the remote ID at both endpoints, select **bidirectional deletion**.
3. Click **OK**.





## CHAPTER 8

# Nodal Management

- [Introduction on page 133](#)
- [Nodal Management for BTI7000 Series Network Elements on page 134](#)
- [Nodal Management for BTI7800 Series Network Elements on page 181](#)
- [Nodal Management for Juniper Networks Routers and Switches on page 257](#)
- [Nodal Management for BTI800 Series Network Elements on page 265](#)

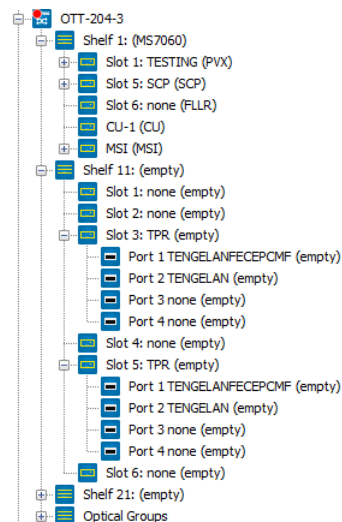
## Introduction

---

PSM supports nodal management for the BTI7000 Series, BTI7800 Series, and BTI800 Series (enable/disable only) equipment, and limited management of MX Series and PTX Series routers and QFX Series switches.

When a network element is discovered, PSM displays the network element and all of its components in the Network tree. This includes all provisioned and installed components, all auto-provisioned components, and all pre-provisioned components (when operators provision equipment in advance of hardware installation).

The Network tree lists the components hierarchically. You can expand a component to see contained components, or minimize a component to hide its contents.



PSM provides an indication of whether a component has been provisioned and/or has been installed. A provisioned component has its mnemonic displayed (e.g. **TPR**). An unprovisioned component is shown with a **none** indication. A component that has been physically installed is shown with its hardware mnemonic in parentheses (e.g. **(DTPR)**). A component that has not been installed is displayed with an **(empty)** indication.

You can use PSM to provision installed components or to pre-provision components. There is a short delay from the time you finish configuring a component to the time when the configuration appears in the Network tree. PSM only displays the new configuration in the Network tree when the network element reports its changes to PSM as part of the regular notification process. To see the changes in PSM immediately, place the network element into provisioning mode before making the changes. See [“Enabling or Disabling Provisioning Mode on a Network Element”](#) on page 113.



**NOTE:** This document only provides a cursory explanation of the various configuration parameters. For a more detailed explanation, consult the documentation suite for the respective products.

---

## Nodal Management for BTI7000 Series Network Elements

---

Nodal management for the BTI7000 Series network elements is generally performed using the proNX 900. In some situations, however, it might be possible for you to use PSM to configure the BTI7000 Series network elements directly.

This section describes how to launch the proNX 900 from PSM, and then describes the nodal provisioning that you can perform directly using PSM.

- [Launching the proNX 900 Node Controller on page 134](#)
- [Provisioning a BTI7000 Series Shelf on page 135](#)
- [Provisioning a Slot on a BTI7000 Series Shelf on page 137](#)
- [Provisioning a Transponder on a BTI7000 Series Shelf on page 139](#)
- [Provisioning a Muxponder on a BTI7000 Series Shelf on page 150](#)
- [Provisioning a multiplexer/demultiplexer on a BTI7000 Series Shelf on page 163](#)
- [Provisioning GCC on a BTI7000 Series Network Element on page 165](#)
- [Viewing Port PMs on a BTI7000 Series Network Element on page 166](#)
- [Provisioning the BTI7000 Series Dynamic Optical Layer \(DOL\) on page 168](#)
- [Enabling or Disabling a Port on page 180](#)

### Launching the proNX 900 Node Controller

Use this procedure to launch the proNX 900 Node Controller.

The proNX 900 Node Controller is the nodal manager for the BTI7000 Series network elements.



**NOTE:** The proNX 900 Node Controller might not be supported on all PSM Client platforms. See the *BTI7000 Series Common Equipment Installation Guide* for a list of platforms that support the proNX 900 Node Controller.

#### Prerequisites:

- The proNX 900 Node Controller software that is compatible with the network elements in your network must be installed on your local computer.
- 1. To launch the proNX 900, right-click a network element in the Network tree view or Topology Map view, and choose **Node Controller**.

The proNX 900 Node Controller splash screen displays. This procedure is complete.

If you get an error message indicating that the PSM Client cannot find the proNX 900 application software (executable file) on your local computer, configure the proNX 900 as described in [“Configuring the proNX 900 Node Controller”](#) on page 282.



**NOTE:** Information on how to use the proNX 900 can be found in the BTI7000 Series documentation suite.

## Provisioning a BTI7000 Series Shelf

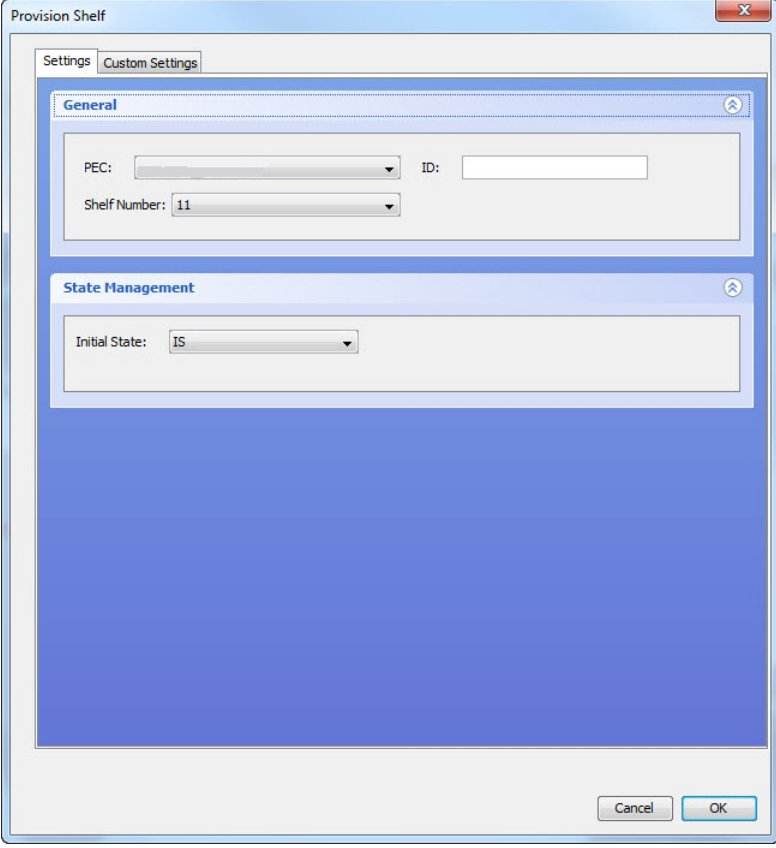
### Adding a Shelf

Use this procedure to add a new shelf on a BTI7000 Series network element.

1. Right-click a network element in the Network tree view or in the topology Map view and select **Node > Shelf > Provision**.

The **Provision Shelf** dialog appears:

*Figure 33: BT17000 Series Provision Shelf*



The image shows a 'Provision Shelf' dialog box with a title bar and a close button. It has two tabs: 'Settings' and 'Custom Settings'. The 'Settings' tab is active and contains two sections: 'General' and 'State Management'. The 'General' section has three fields: 'PEC:' with a drop-down menu, 'ID:' with a text input field, and 'Shelf Number:' with a drop-down menu showing '11'. The 'State Management' section has one field: 'Initial State:' with a drop-down menu showing 'IS'. At the bottom right are 'Cancel' and 'OK' buttons.

2. Configure the shelf as follows:
  - **PEC** Select the PEC from the list of available PECs in the drop-down menu.
  - **Shelf Number** Select the shelf number from the drop-down menu. The drop-down menu only displays the shelf numbers that are available and not already in use.
  - **ID** Optionally, enter a string identifying the shelf.
  - **Initial State** Specify whether the initial state of the shelf is **IS** (in-service) or **OOS** (out-of-service).
3. Optionally, specify the **Custom** fields. These fields are for operator use and are opaque to the system.
  - a. Click the **Custom Settings** tab.
  - b. In the **Custom Settings** panel, specify the **Custom 1**, **Custom 2**, and **Custom 3** settings as desired.
4. When you are finished, click **OK**.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View >Server >Tasks** window. The new provisioning appears in the Network tree view a short while after the task completes successfully.

### Deleting a Shelf

---

Use this procedure to delete a shelf on a BTI7000 Series network element.

#### Prerequisites:

All components on the shelf must be deleted before you can delete the shelf.

1. Expand the network element in the Network tree view to show the shelves in that NE.
2. Right-click a shelf and select **Shelf >Delete**.
3. Click **OK** in the **Delete Shelf** confirmation dialog.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View >Server >Tasks** window. The new provisioning appears in the Network tree view a short while after the task completes successfully.

## Provisioning a Slot on a BTI7000 Series Shelf

### Adding a Module

---

Use this procedure to add a new module on a BTI7000 Series shelf.

1. Expand the network element in the Network tree view to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.
3. Right-click an unprovisioned slot and select **Slot >Provision** to add a module in that slot.

The **Provision Slot** dialog appears:

Figure 34: BT17000 Series Provision Slot

The screenshot shows the 'Provision Slot' configuration window. It has a title bar with a maximize button. Below the title bar are two tabs: 'Settings' and 'Custom Settings'. The 'Settings' tab is selected. Inside the 'Settings' tab, there is a 'General' section with a blue header and a close button. It contains the following fields:

- Name :** A dropdown menu showing 'C1ADM'.
- PEC/CLEI Code :** A dropdown menu showing 'BP1A32AA-01'.
- Shelf Number :** A text input field containing '1'.
- Slot Number :** A text input field containing '3'.
- ID :** An empty text input field.

Below the 'General' section is a 'State Management' section with a blue header and a close button. It contains:

- Initial State:** A dropdown menu showing 'IS'.

At the bottom right of the window are 'Cancel' and 'OK' buttons.

4. Configure the slot as follows:
  - **Name** Select the module type from the list of available module types in the drop-down menu.
  - **PEC/CLEI Code** Select the PEC from the list of available PECs for the selected module type.
  - **Shelf Number** and **Slot Number**- These read-only fields display the shelf and slot numbers for the slot you selected.
  - **ID** Optionally, specify an identifier for the module.
  - **Initial State** Specify the initial state of the module.
5. Optionally, specify the **Custom** fields. These fields are for operator use and are opaque to the system.
  - a. Click the **Custom Settings** tab.
  - b. In the **Custom Settings** panel, specify the **Custom 1**, **Custom 2**, and **Custom 3** settings as desired.
6. When you are finished, click **OK**.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View > Server > Tasks** window. The new provisioning appears in the Network tree view a short while after the task completes successfully.

### Deleting a Module

---

Use this procedure to delete a module on a BTI7000 Series shelf.

#### Prerequisites:

All components in the module must be deleted before you can delete the module.

1. Expand the network element in the Network tree view to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.
3. Right-click a provisioned slot and select **Slot > Delete**.
4. Click **OK** in the **Delete Slot** confirmation dialog.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View > Server > Tasks** window. The new provisioning appears in the Network tree view a short while after the task completes successfully.

## Provisioning a Transponder on a BTI7000 Series Shelf

PSM supports provisioning of the Dual 2.5G, Dual 4G, 10G, and Dual 10G multiprotocol transponders.

This section contains the following topics:

- [Provisioning Ports on a BTI7000 Series Transponder on page 139](#)
- [Provisioning Cross-connects on a BTI7000 Series Transponder on page 143](#)
- [Provisioning Line Protection Groups on a BTI7000 Series Transponder on page 145](#)
- [Provisioning Client Protection Groups on a BTI7000 Series Transponder on page 148](#)

To add a transponder, follow the steps in “[Adding a Module](#)” on [page 137](#) and select the desired transponder from the PEC drop-down list.

### Provisioning Ports on a BTI7000 Series Transponder

---

BTI7000 Series transponders consist of 2 or 4 ports divided equally between client and line ports.

#### ***Adding a Transponder Port***

Use this procedure to add a new port on a BTI7000 Series transponder.

1. Expand the network element in the Network tree view to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.
3. Expand a transponder to show the ports in that transponder.
4. Right click an unprovisioned port and select **Transceiver > Provision** to add a port on that transponder.

The **Provision/Edit Transceiver** dialog appears:

*Figure 35: BTI7000 Series Provision/Edit Transceiver*

The screenshot shows the 'Provision/Edit Transceiver' dialog box for the BTI7000 Series. The 'Settings' tab is selected, displaying various configuration options. The 'Settings' section includes dropdown menus for Protocol, Wavelength, Fault Propagation Shutdown, Loopback Status, and Laser Control, as well as checkboxes for Phy PM Thld Mon and SD Bit Error Rate. There are also text input fields for Vendor Part Number 1, 2, and 3, Loopback Action, Transceiver PEC, Tx Trace Id, ExpectedTraceId, and Rx Trace Id. The 'Timers' section features an 'AINS Timer' configuration with a timer set to 0 days, 8 hours, and 0 minutes. The 'State Management' section shows an 'Admin State' dropdown menu set to 'AINS'. At the bottom right, there are 'Cancel' and 'OK' buttons.

5. Configure the port as follows:
  - **Protocol** Select the protocol from the list of available protocols in the drop-down menu.
  - **Phy PM Thld Mon** Enable or disable monitoring of PM thresholds.
  - **SD Bit Error Rate** Optionally, select the signal degrade bit error rate.
  - **Vendor Part Number 1 to 3** Optionally, specify the vendor part numbers.



- **Laser Control** Select **Auto** to let software control the laser. Select **Manual On** to turn on the laser. Select **Manual Off** to turn off the laser.
  - **Wavelength** Specify the wavelength to use. Set to **NONE** for copper.
  - **Fault Propagation Shutdown** Enable or disable FPSD. If you enable FPSD, you must also set **Laser Control** to **Auto** and **Wavelength** to a value other than **NONE**.
  - **Loopback Status** This attribute cannot be set when adding a port.
  - **Loopback Action** This attribute cannot be set when adding a port.
  - **Transceiver PEC** Optionally, specify the transceiver PEC.
  - **Tx Trace Id** Optionally, specify the transmit trace ID (only available on certain modules).
  - **Expected Trace Id** Optionally, specify the expected trace ID (only available on certain modules).
  - **Rx Trace Id** This attribute is read only.
  - **Auto-In Service Timer** Optionally, specify the AINS timer. This attribute is only applicable if the **Admin State** is **AINS**.
  - **Admin State** Specify the initial state of the module.
6. Optionally, click the **Custom Info** tab to see the **Custom Info** panel.
    - a. Specify the port identifiers **ID 1** and **ID 2**.
    - b. Specify the **Fiber Type**.
    - c. Specify the **Custom 1**, **Custom 2**, and **Custom 3** settings as desired.
    - d. Specify the **Remote Id**. For information on how to use this field, see [“Deriving Topology Using Remote IDs” on page 74](#).
  7. Click **OK**.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View > Server > Tasks** window. The new provisioning appears in the Network tree view a short while after the task completes successfully.

### ***Editing a Transponder Port***

Use this procedure to edit a port on a BT17000 Series transponder.

1. Expand the network element in the Network tree to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.
3. Expand a transponder to show the ports for that transponder.
4. Right click a provisioned port and select **Transceiver > Edit**.

The **Provision/Edit Transceiver** dialog appears.

5. Change one or more port settings as follows:

- **Protocol** Select the protocol from the list of available protocols in the drop-down menu.
- **Phy PM Thld Mon** Enable or disable monitoring of PM thresholds.
- **SD Bit Error Rate** Select the signal degrade bit error rate.
- **Vendor Part Number 1 to 3** Specify the vendor part numbers.
- **Laser Control** Select **Auto** to let software control the laser. Select **Manual On** to turn on the laser. Select **Manual Off** to turn off the laser.
- **Wavelength** Specify the wavelength to use. Set to **NONE** for copper.
- **Fault Propagation Shutdown** Enable or disable FPSD. If you enable FPSD, you must also set **Laser Control** to **Auto** and **Wavelength** to a value other than **NONE**.
- **Loopback Status** This field is read only, and indicates what kind of loopback, if any, is in effect.
- **Loopback Action** This is an action command. It will always default to **<no operation>**, meaning that no command is issued. Set to **Terminal** or **Facility** to set the port to terminal or facility loopback respectively.
- **Transceiver PEC** Specify the transceiver PEC.
- **Tx Trace Id** Specify the transmit trace ID (only available on certain modules).
- **Expected Trace Id** Specify the expected trace ID (only available on certain modules).
- **Rx Trace Id** This attribute is read only.
- **Auto-In Service Timer** Specify the AINS timer. This attribute is only applicable if the **Admin State** is **AINS**.
- **Active Auto-In Service Timer** This attribute is read only.
- **Admin State** Set the admin state of the module.
- **Operational State** This attribute is read only.
- **Secondary State** This attribute is read only.
- **Laser Status** This attribute is read only.

6. To change the **Custom Info** settings , click the **Custom Info** tab.

- a. Specify the port identifiers **ID 1** and **ID 2**.
- b. Specify the **Fiber Type**.
- c. Specify the **Custom 1**, **Custom 2**, and **Custom 3** settings as desired.
- d. Specify the **Remote Id**. For information on how to use this field, see [“Deriving Topology Using Remote IDs” on page 74](#).

7. Click **Apply**.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View >Server >Tasks** window. The new provisioning appears in the Network tree view a short while after the task completes successfully.

### ***Deleting a Transponder Port***

Use this procedure to delete a port on a BTI7000 Series transponder.

Before a port can be deleted, it must be removed from any protection groups and cross-connects.

1. Expand the network element in the Network tree view to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.
3. Expand a transponder to show the ports for that transponder.
4. Right click a provisioned port and select **Transceiver >Delete**.
5. Click **OK** in the **Delete Transceiver** confirmation dialog.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View >Server >Tasks** window. The new provisioning appears in the Network tree view a short while after the task completes successfully.

### ***Provisioning Cross-connects on a BTI7000 Series Transponder***

---

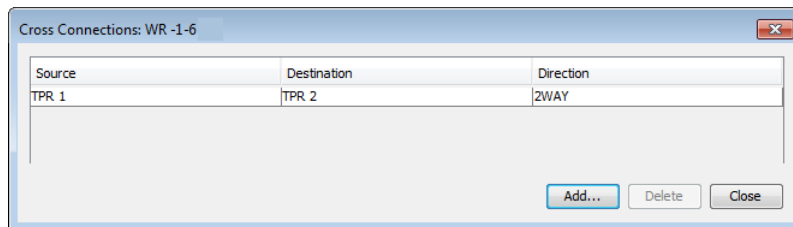
There are various rules that govern what ports and protocols can be cross-connected. See the *BTI7000 Series Transponder Solutions Guide* for information.

### ***Adding a Transponder Cross-connect***

Use this procedure to add a cross-connect on a BTI7000 Series transponder.

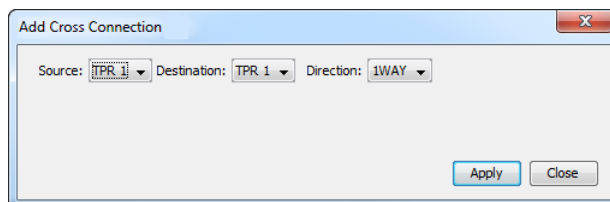
1. Expand the network element in the Network tree view to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.
3. Right click a transponder and select **Cross Connects >Edit**.

The **Cross Connections** dialog appears, displaying the existing cross-connects.



- Click **Add...** to add a cross-connect.

The **Add Cross Connection** dialog appears.



- Specify the **Source** port, the **Destination** port, and the **Direction**.
- Click **Apply**.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View > Server > Tasks** window. The new provisioning appears in the Network tree view a short while after the task completes successfully.

### ***Deleting a Transponder Cross-connect***

Use this procedure to delete a cross-connect on a BT17000 Series transponder.

- Expand the network element in the Network tree view to show the shelves in that NE.
- Expand a shelf to show the slots in that shelf.
- Right click a transponder and select **Cross Connects > Edit**.  
The **Cross Connections** dialog appears.
- Select the cross-connect you want to delete and click **Delete**.  
The **Deleting Cross Connection** confirmation dialog appears.
- Click **OK** to confirm the deletion.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View > Server > Tasks** window. The new

provisioning appears in the Network tree view a short while after the task completes successfully.

### Provisioning Line Protection Groups on a BTI7000 Series Transponder

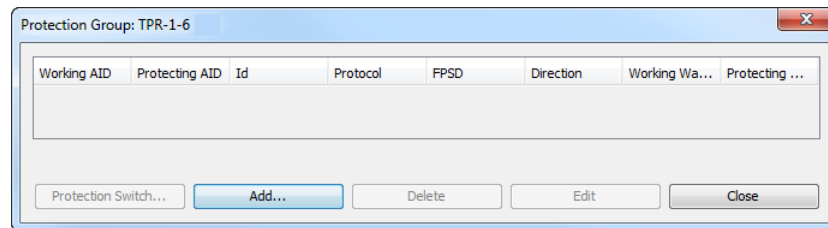
A line protection group is a pairing of a working line port and a protecting line port. There are various rules that govern the configuration of line port protection. See the *BTI7000 Series Transponder Solutions Guide* for information.

#### Adding a Transponder Protection Group

Use this procedure to add a line protection group on a BTI7000 Series transponder.

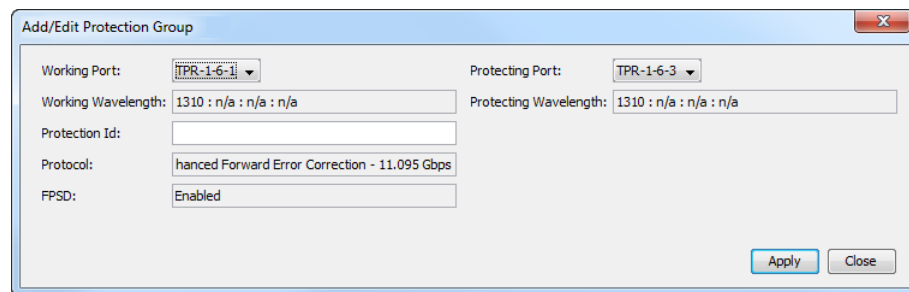
1. Expand the network element in the Network tree view to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.
3. Right click a transponder and select **Protection Groups >Edit**.

The **Protection Group** dialog appears.



4. Click **Add...** to add a protection group.

The **Add/Edit Protection Group** dialog appears.



5. Specify the **Working Port**, the **Protecting Port**, and optionally, the **Protection Id**.
6. Click **Apply**.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View >Server >Tasks** window. The new provisioning appears in the Network tree view a short while after the task completes successfully.

### ***Editing a Transponder Protection Group***

Use this procedure to edit a line protection group on a BTI7000 Series transponder.

1. Expand the network element in the Network tree view to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.
3. Right click a transponder and select **Protection Groups >Edit**.

The **Protection Group** dialog appears, displaying the existing protection group.

4. Select a protection group and click **Edit**.

The **Add/Edit Protection Group** dialog appears.

5. Edit the **Protection Id**.

6. Click **Apply**.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View >Server >Tasks** window. The new provisioning appears in the Network tree view a short while after the task completes successfully.

### ***Deleting a Transponder Protection Group***

Use this procedure to delete a protection group on a BTI7000 Series transponder.

1. Expand the network element in the Network tree view to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.
3. Right click a transponder and select **Protection Groups >Edit**.

The **Protection Group** dialog appears, displaying the existing protection group.

4. Select the protection group you want to delete and click **Delete**.

The **Deleting Protection Group** confirmation dialog appears.

5. Click **OK** to confirm the deletion.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View >Server >Tasks** window. The new provisioning appears in the Network tree a short while after the task completes successfully.

### Executing a Protection Switch Command

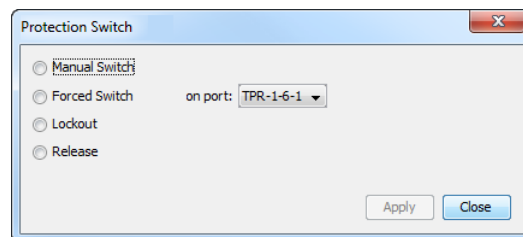
Use this procedure to execute a protection switch command on a BTI7000 Series transponder port.

1. Expand the network element in the Network tree view to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.
3. Right click a transponder and select **Protection Groups >Edit**.

The **Protection Group** dialog appears, displaying the existing protection group.

4. Select a protection group and click **Protection Switch....**

The **Protection Switch** dialog appears.



5. Select the port on which you want to apply the command.
6. Select from the following actions:
  - **Manual Switch** Switch the working and protecting ports. This is only allowed when the protecting port is free of faults.
  - **Forced Switch** Switch the working and protecting ports even if the protecting port has a Signal Degrade condition.
  - **Lockout** Make the specified port unavailable. If the specified port is the working port, a protection switch occurs. If the specified port is the protecting port, the port is no longer available for protecting.
  - **Release** Release the lockout.
7. Click **Apply**.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View >Server >Tasks** window. The new provisioning appears in the Network tree a short while after the task completes successfully.

### Provisioning Client Protection Groups on a BTI7000 Series Transponder

A client protection group is a pairing of a working client port and a protecting client port. There are various rules that govern the configuration of client port protection. See the *BTI7000 Series Transponder Solutions Guide* for information.



**NOTE:** Not all transponders support client protection.

#### Adding a Client Protection Group

Use this procedure to add a client protection group on a BTI7000 Series transponder.

1. Expand the network element in the Network tree view to show the shelves in that NE.
2. To add a group across shelves, right click a network element and select **Client Protection Groups >Edit**. To add a group within a shelf, right click a shelf and select **Client Protection Groups >Edit**.

The **Protection Group** dialog appears.

The dialog box shows a table with columns: Working AID, Protecting AID, Id, Protocol, FPSD, Direction, Working Wa..., and Protecting ... Below the table are buttons: Protection Switch..., Add..., Delete, Edit, and Close.

3. Click **Add...** to add a client protection group.

The **Add/Edit Protection Group** dialog appears.

The dialog box contains fields for: Working Port (dropdown: TPR-11-1-2), Protecting Port (dropdown: TPR-11-5-2), Working Wavelength (text: 1310 : n/a : n/a : n/a), Protecting Wavelength (text: 1310 : n/a : n/a : n/a), Protection Id (text), Protocol (text: 10 Gigabit Ethernet LAN - 10.313 Gbps), FPSD (text: Enabled), and buttons for Apply and Close.

4. Specify the **Working Port**, the **Protecting Port**, and optionally, the **Protection Id**.

5. Click **Apply**.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View >Server >Tasks** window. The new provisioning appears in the Network tree view a short while after the task completes successfully.



### ***Editing a Client Protection Group***

Use this procedure to edit a client protection group on a BTI7000 Series transponder.

1. Expand the network element in the Network tree view to show the shelves in that NE.
2. Right click the network element or a shelf and select **Client Protection Groups >Edit**.  
The **Protection Group** dialog appears, displaying the existing protection groups.
3. Select a protection group and click **Edit**.  
The **Add/Edit Protection Group** dialog appears.
4. Edit the **Protection Id**.
5. Click **Apply**.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View >Server >Tasks** window. The new provisioning appears in the Network tree a short while after the task completes successfully.

### ***Deleting a Client Protection Group***

Use this procedure to delete a client protection group on a BTI7000 Series transponder.

1. Expand the network element in the Network tree view to show the shelves in that NE.
2. Right click the network element or shelf and select **Client Protection Groups >Edit**.  
The **Protection Group** dialog appears, displaying the existing protection groups.
3. Select the protection group you want to delete and click **Delete**.  
The **Deleting Protection Group** confirmation dialog appears.
4. Click **OK** to confirm the deletion.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View >Server >Tasks** window. The new provisioning appears in the Network tree a short while after the task completes successfully.

### ***Executing a Client Protection Switch Command***

Use this procedure to execute a client protection switch command on a BTI7000 Series transponder port.

1. Expand the network element in the Network tree view to show the shelves in that NE.
2. Right click the network element or a shelf and select **Client Protection Groups >Edit**.  
The **Protection Group** dialog appears, displaying the existing protection group.
3. Select a protection group and click **Protection Switch....**  
The **Protection Switch** dialog appears.



4. Select the port on which you want to apply the command.
5. Select from the following actions:
  - **Manual Switch** Switch the working and protecting ports. This is only allowed when the protecting port is free of faults.
  - **Forced Switch** Switch the working and protecting ports even if the protecting port has a Signal Degrade condition.
  - **Lockout** Make the specified port unavailable. If the specified port is the working port, a protection switch occurs. If the specified port is the protecting port, the port is no longer available for protecting.
  - **Release** Release the lockout.
6. Click **Apply**.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View >Server >Tasks** window. The new provisioning appears in the Network tree a short while after the task completes successfully.

## Provisioning a Muxponder on a BTI7000 Series Shelf

PSM supports provisioning of the 2-port, 8-port, and 10-port muxponders.

This section contains the following topics:

- [Provisioning Ports on a BTI7000 Series Muxponder on page 151](#)
- [Provisioning Virtual Concatenation Groups on a BTI7000 Series Muxponder on page 155](#)
- [Provisioning Cross-connects on a BTI7000 Series Muxponder on page 158](#)
- [Provisioning Protection Groups on a BTI7000 Series Muxponder on page 160](#)
- [Provisioning Synchronization on a BTI7000 Series Muxponder on page 162](#)

To add a muxponder, follow the steps in [“Adding a Module” on page 137](#) and select the desired muxponder from the PEC drop-down list.

### Provisioning Ports on a BT17000 Series Muxponder

BT17000 Series muxponders consist of a set of client ports and 2 line ports.

#### Adding a Muxponder Port

Use this procedure to add a new port on a BT17000 Series muxponder.

1. Expand the network element in the Network tree view to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.
3. Expand a muxponder to show the ports in that muxponder.
4. Right click an unprovisioned port and select **Port >Provision** to add a port on that muxponder.

The **Provision Port** dialog appears:

**Figure 36: BT17000 Series Provision Port**

Provision Port: MXP-1-7-C1

Settings Custom Info

**Settings**

Protocol: Gigabit Ethernet - 1.25 Gbps

Wavelength: <not specified> (nm:THz:Ch:DOL)

Protocol Options

Phy PM Thld Mon:	Disabled	Transceiver PEC:	
Fault Propagation Shutdown:	Enabled	FPSD Recover Timer:	3500
Media Rate:	1000FD	Vendor Part Number 1:	
Loopback:	Disabled	Vendor Part Number 2:	
Flow Control:	Transparent	Vendor Part Number 3:	
Laser Control:	Auto	GFP Mode:	Framed

**State Management**

Admin State: AINS

**Timers**

AINS Timer

Config

Timer: 0 days 8 hours 0 minutes

Cancel OK

## 5. Configure the port as follows:



**NOTE:** Some fields appear only for certain protocols, ports, and cards. See the *BT17000 Series Muxponder Solutions Guide* for details.

- **Protocol** Select the protocol from the list of available protocols in the drop-down menu.
- **Wavelength** Specify the wavelength to use. Set to **NONE** for copper.
- **Phy PM Thld Mon** Enable or disable monitoring of PM thresholds.
- **Fault Propagation Shutdown** Enable or disable FPSD. If you enable FPSD, you must also set **Laser Control** to **Auto** and **Wavelength** to a value other than **NONE**.
- **SD Bit Error Rate** Select the signal degrade bit error rate.
- **TOH Transparency** Choose whether you want to have Transport Overhead transparency in the signal or not.
- **DCC Transparency** Choose whether you want to have Data Communications Channel transparency in the signal or not. If selected, you must specify the channel to transport the DCC bytes. This option is automatically selected if **TOH Transparency** is selected.
- **Laser Control** Select **Auto** to let software control the laser. Select **Manual On** to turn on the laser. Select **Manual Off** to turn off the laser.
- **Line Mapping** Specify the line mapping for line ports.
- **Transceiver PEC** Optionally, specify the transceiver PEC.
- **FPSD Recover Timer** If **Fault Propagation Shutdown** is set to **Enabled** and **GFP Mode** is set to **Framed**, specify the time that the client port takes to turn the laser back on after the link has recovered. If a link failure occurs on a client port at the near end, FPSD behavior causes the client port at the near end and the client port at the far end to turn off their lasers. After the link recovers, the client port at the near end waits for the time specified in this field before turning its laser back on and before notifying the far end that the link has recovered. A shorter time period enables the port to detect that the link is back up more quickly. A longer time period allows the port to ignore link flapping situations. This timer is supported on client ports on the BT7A48AA-I02 and BT7A48BA-I02 cards only.
- **Vendor Part Number 1 to 3** Optionally, specify the vendor part numbers.
- **Loopback** This attribute cannot be set when adding a port.
- **GFP Mode** Set the Generic Framing Procedure mapping mode.
- **Media Rate** Set the media rate.
- **Flow Control** Set the flow control mode.

- **Admin State** Specify the initial state of the port.
  - **Auto-In Service Timer** Specify the AINS timer. This attribute is only applicable if the **Admin State** is **AINS**.
6. Optionally, click the **Custom Info** tab to see the **Custom Info** panel.
    - a. Specify the port identifier **ID 1**.
    - b. Specify the **Fiber Type**.
    - c. Specify the **Custom 1** field as desired.
    - d. Specify the **Remote Id**. For information on how to use this field, see [“Deriving Topology Using Remote IDs” on page 74](#).
  7. Click **OK**.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View > Server > Tasks** window. The new provisioning appears in the Network tree view a short while after the task completes successfully.

#### ***Editing a Muxponder Port***

Use this procedure to edit a port on a BT17000 Series muxponder.

1. Expand the network element in the Network tree view to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.
3. Expand a muxponder to show the ports for that muxponder.
4. Right click a provisioned port and select **Port > Provision**.  
The **Provision Port** dialog appears.
5. Change one or more port settings as follows:



**NOTE:** Some fields appear only for certain protocols, ports, and cards. See the *BT17000 Series Muxponder Solutions Guide* for details.

- **Protocol** This attribute cannot be changed.
- **Wavelength** Specify the wavelength to use. Set to **NONE** for copper.
- **Phy PM Thld Mon** Enable or disable monitoring of PM thresholds.
- **Fault Propagation Shutdown** Enable or disable FPSD. If you enable FPSD, you must also set **Laser Control** to **Auto** and **Wavelength** to a value other than **NONE**.
- **SD Bit Error Rate** Select the signal degrade bit error rate.

- **TOH Transparency** Choose whether you want to have Transport Overhead transparency in the signal or not.
  - **DCC Transparency** Choose whether you want to have Data Communications Channel transparency in the signal or not. If selected, you must specify the channel to transport the DCC bytes. This option is automatically selected if **TOH Transparency** is selected.
  - **Laser Control** Select **Auto** to let software control the laser. Select **Manual On** to turn on the laser. Select **Manual Off** to turn off the laser.
  - **Line Mapping** Specify the line mapping for line ports.
  - **Transceiver PEC** Optionally, specify the transceiver PEC.
  - **FPSD Recover Timer** If **Fault Propagation Shutdown** is set to **Enabled** and **GFP Mode** is set to **Framed**, specify the time that the client port takes to turn the laser back on after the link has recovered. If a link failure occurs on a client port at the near end, FPSD behavior causes the client port at the near end and the client port at the far end to turn off their lasers. After the link recovers, the client port at the near end waits for the time specified in this field before turning its laser back on and before notifying the far end that the link has recovered. A shorter time period enables the port to detect that the link is back up more quickly. A longer time period allows the port to ignore link flapping situations. This timer is supported on client ports on the BT7A48AA-I02 and BT7A48BA-I02 cards only.
  - **Vendor Part Number 1 to 3** Optionally, specify the vendor part numbers.
  - **Loopback** Set to **Terminal** for terminal loopback, **Facility** for facility loopback, or **Disabled**. The port must be out of service before you can set this option.
  - **GFP Mode** Set the Generic Framing Procedure mapping mode.
  - **Media Rate** Set the media rate.
  - **Flow Control** Set the flow control mode.
  - **Admin State** Set the admin state of the port.
  - **Operational State** This attribute is read only.
  - **Secondary State** This attribute is read only.
  - **Laser Status** This attribute is read only.
  - **Auto-In Service Timer** Specify the AINS timer. This attribute is only applicable if the **Admin State** is **AINS**.
6. To change the **Custom Info** settings , click the **Custom Info** tab.
- a. Specify the port identifiers **ID 1** and **ID 2**.
  - b. Specify the **Fiber Type**.

- c. Specify the **Custom 1**, **Custom 2**, and **Custom 3** settings as desired.
  - d. Specify the **Remote Id**. For information on how to use this field, see [“Deriving Topology Using Remote IDs” on page 74](#).
7. Click **Apply**.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View > Server > Tasks** window. The new provisioning appears in the Network tree view a short while after the task completes successfully.

### ***Deleting a Muxponder Port***

Use this procedure to delete a port on a BTI7000 Series muxponder.

Before a port can be deleted, it must be removed from any protection groups and cross-connects.

1. Expand the network element in the Network tree view to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.
3. Expand a muxponder to show the ports for that muxponder.
4. Right click a provisioned port and select **Port > Delete**.
5. Click **OK** in the **Delete Port** confirmation dialog.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View > Server > Tasks** window. The new provisioning appears in the Network tree view a short while after the task completes successfully.

### ***Provisioning Virtual Concatenation Groups on a BTI7000 Series Muxponder***

---

A virtual concatenation group (VCG) is a collection of virtual tributaries that are concatenated to create a higher bit rate stream. The tributaries in a VCG do not need to be contiguous.

#### ***Adding a Muxponder Virtual Concatenation Group***

Use this procedure to add a virtual concatenation group (VCG) on a BTI7000 Series muxponder.

1. Expand the network element in the Network tree view to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.
3. Right click a muxponder and select **Virtual Concatenation Groups > Edit**.

The **Virtual Concatenation Groups** dialog appears, displaying the existing virtual concatenation groups.

Port	VCG Number	Format	Time Slots
1	1	STS1C22V	1-22
1	2	STS1C22V	23-44
1	3	STS1C22V	45-66
1	4	STS1C22V	67-88
1	5	STS1C22V	89-110
1	6	STS1C22V	111-132
1	7	STS1C22V	133-154
1	8	STS1C22V	155-176
2	1	STS1C22V	1-22
2	2	STS1C22V	23-44
2	3	STS1C22V	45-66
2	4	STS1C22V	67-88

Add Edit Delete

Close

The BTI7000 Series muxponder has number of default VCGs automatically created.

- Click **Add** to add a virtual concatenation group.

The **Provision VCG** dialog appears.

Port:  Index:

Format:  ☐ Ascending STS Selection

Time Slots

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64
65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96
97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112
113	114	115	116	117	118	119	120	121	122	123	124	125	126	127	128
129	130	131	132	133	134	135	136	137	138	139	140	141	142	143	144
145	146	147	148	149	150	151	152	153	154	155	156	157	158	159	160
161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176
177	178	179	180	181	182	183	184	185	186	187	188	189	190	191	192

Remaining Slots: 19

Apply Close

- Specify the **Port** and **Index** from the available ports and indices.
- Specify the **Format** of the concatenated signal.  
Based on your selection, the number of time slots shown might change.
- Set **Ascending STS Selection** if you want to auto-select the contiguous number of time slots required.  
With this option, all you have to do is to select the first time slot.
- Select the time slots that make up this VCG.



Click a time slot to select. Click again to clear. The **Remaining Slots** counter at the bottom shows the number of time slots that are available for selection based on the specified concatenation format.

9. Click **Apply**.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View >Server >Tasks** window. The new provisioning appears in the Network tree view a short while after the task completes successfully.

### ***Editing a Muxponder Virtual Concatenation Group***

Use this procedure to edit a virtual concatenation group on a BT17000 Series muxponder.

1. Expand the network element in the Network tree view to show the shelves in that NE.

2. Expand a shelf to show the slots in that shelf.

3. Right click a muxponder and select **Virtual Concatenation Groups >Edit**.

The **Virtual Concatenation Groups** dialog appears, displaying the existing virtual concatenation groups.

4. Select a virtual concatenation group and click **Edit**.

The **Provision VCG** dialog appears.

5. Specify the **Format** of the concatenated signal.

Based on your selection, the number of time slots shown might change.

6. Set **Ascending STS Selection** if you want to auto-select the contiguous number of time slots required.

With this option, all you have to do is to select the first time slot.

7. Select the time slots that make up this VCG.

Click a time slot to select. Click again to clear. The **Remaining Slots** counter at the bottom shows the number of time slots that are available for selection based on the specified concatenation format.

8. Click **Apply**.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View >Server >Tasks** window. The new provisioning appears in the Network tree view a short while after the task completes successfully.

### ***Deleting a Muxponder Virtual Concatenation Group***

Use this procedure to delete a virtual concatenation group on a BTI7000 Series muxponder.

1. Expand the network element in the Network tree view to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.
3. Right click a muxponder and select **Virtual Concatenation Groups >Edit**.  
The **Virtual Concatenation Groups** dialog appears, displaying the existing groups.

4. Select the virtual concatenation group you want to delete and click **Delete**.  
The **Delete VCG** confirmation dialog appears.

5. Click **OK** to confirm the deletion.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View >Server >Tasks** window. The new provisioning appears in the Network tree view a short while after the task completes successfully.

---

### ***Provisioning Cross-connects on a BTI7000 Series Muxponder***

There are various rules that govern what ports and protocols can be cross-connected. See the *BTI7000 Series Muxponder Solutions Guide* for information.

### ***Adding a Muxponder Cross-connect***

Use this procedure to add a cross-connect on a BTI7000 Series muxponder.

1. Expand the network element in the Network tree view to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.
3. Right click a muxponder and select **Cross Connects >Edit**.  
The **Manage Cross Connects** dialog appears, displaying the existing cross-connects.

Source	Destination	Format	Type	Switch Mate
Line 1 STS 73	Client 2 Channel 1	STS21C	TWO WAY	

4. Click **Add** to add a cross-connect.

The **Provision Cross Connect** dialog appears.

Type: CCAT

Source: Line 1 (SONET OC-192 - 9.953 Gbps)

Time Slot:

Destination: Client 1 (Gigabit Ethernet - 1.25 Gbps)

Direction: Two Way CRS Type: STS21C

5. Specify the concatenation **Type**.

If you specify contiguous concatenation (**CCAT**), then you will select the timeslot using **Set Time Slot** and the CCAT type using the **CRS Type** pulldown menu. If you specify virtual concatenation (**VCAT**), then you will select the virtual concatenation group through the **Source** pulldown menu. The timeslots and VCAT type for the virtual concatenation group are set when you create the virtual concatenation group. See [“Provisioning Virtual Concatenation Groups on a BT17000 Series Muxponder” on page 155](#).

6. Specify the **Source**, the **Destination**, and the **Direction**.

7. Click **Apply**.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View > Server > Tasks** window. The new provisioning appears in the Network tree view a short while after the task completes successfully.

### ***Deleting a Muxponder Cross-connect***

Use this procedure to delete a cross-connect on a BT17000 Series muxponder.

1. Expand the network element in the Network tree view to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.
3. Right click a muxponder and select **Cross Connects >Edit**.  
The **Manage Cross Connects** dialog appears.
4. Select the cross-connect you want to delete and click **Delete**.  
The **Delete Cross Connect** confirmation dialog appears.
5. Click **OK** to confirm the deletion.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View >Server >Tasks** window. The new provisioning appears in the Network tree view a short while after the task completes successfully.

### Provisioning Protection Groups on a BTI7000 Series Muxponder

---

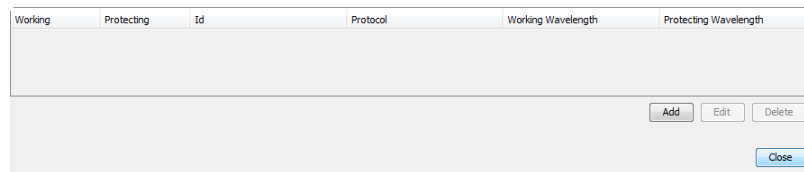
A protection group is a pairing of a working line port and a protecting line port. There are various rules that govern the configuration of line port protection. See the *BTI7000 Series Muxponder Solutions Guide* for information.

#### **Adding a Muxponder Protection Group**

Use this procedure to add a line protection group on a BTI7000 Series muxponder.

1. Expand the network element in the Network tree view to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.
3. Right click a muxponder and select **Protection Groups >Edit**.

The **Manage Protection Groups** dialog appears.



Working	Protecting	Id	Protocol	Working Wavelength	Protecting Wavelength
---------	------------	----	----------	--------------------	-----------------------

Buttons: Add, Edit, Delete, Close

4. Click **Add** to add a protection group.

The **Provision 1+1 Protection Group** dialog appears.

Working:	Line 1 (SONET OC-192 - 9.953 Gbps)	Protecting:	Line 2 (SONET OC-192 - 9.953 Gbps)
Wavelength:	850 : n/a : n/a : n/a	Wavelength:	1271 : n/a : C16 : n/a
Id:	<input type="text"/>		
<input type="button" value="Apply"/> <input type="button" value="Close"/>			

The **Working** port, the **Protecting** port, and the wavelengths are automatically set.

5. Optionally, specify the protection group **Id**.
6. Click **Apply**.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View > Server > Tasks** window. The new provisioning appears in the Network tree view a short while after the task completes successfully.

#### ***Editing a Muxponder Protection Group***

Use this procedure to edit a line protection group on a BTI7000 Series muxponder.

1. Expand the network element in the Network tree view to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.
3. Right click a muxponder and select **Protection Groups > Edit**.

The **Manage Protection Groups** dialog appears, displaying the existing protection group.

4. Select a protection group and click **Edit**.

The **Provision 1+1 Protection Group** dialog appears.

5. Edit the protection **Id**.
6. Click **Apply**.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View > Server > Tasks** window. The new provisioning appears in the Network tree view a short while after the task completes successfully.

#### ***Deleting a Muxponder Protection Group***

Use this procedure to delete a protection group on a BTI7000 Series muxponder.

1. Expand the network element in the Network tree view to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.

3. Right click a muxponder and select **Protection Groups >Edit**.

The **Manage Protection Groups** dialog appears, displaying the existing protection group.

4. Select the protection group you want to delete and click **Delete**.

The **Delete Line Protection** confirmation dialog appears.

5. Click **OK** to confirm the deletion.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View >Server >Tasks** window. The new provisioning appears in the Network tree view a short while after the task completes successfully.

### Provisioning Synchronization on a BT17000 Series Muxponder

Client traffic must be properly synchronized when multiplexing into a SONET/SDH network. This procedure shows how synchronization can be configured.

1. Expand the network element in the Network tree view to show the shelves in that NE.

2. Expand a shelf to show the slots in that shelf.

3. Right click a muxponder and select **Synchronization >Edit**.

The **Manage Synchronization** dialog appears.

The screenshot shows the 'Manage Synchronization' dialog box. It has a 'Timing Mode' dropdown menu set to 'Internal'. Below it are two rows for 'Primary Reference' and 'Secondary Reference', both set to 'None'. To the right of these are 'SSM' dropdown menus set to 'Yes' and 'Status' text boxes set to 'N/A'. At the bottom right are 'Close' and 'Apply' buttons.

4. Configure synchronization as follows:

- **Timing Mode** Set to **Internal** for internal timing, or set to **Line** for line timing. Internal timing can only be used for limited configurations.
- **Primary Reference** When using line timing, set the primary reference to the desired timing source.
- **Secondary Reference** When using line timing, set the secondary reference to the desired timing source.
- **SSM** When using line timing, specify whether synchronization status messaging is enabled. SSM prevents timing loops from occurring as a result of failures or

misconfiguration. There is a separate SSM setting for the primary and secondary references.

- **Status** When using line timing, the status' of the primary and secondary references are shown.

5. Click **Apply**.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View > Server > Tasks** window. The new provisioning appears in the Network tree view a short while after the task completes successfully.

## Provisioning a multiplexer/demultiplexer on a BTI7000 Series Shelf

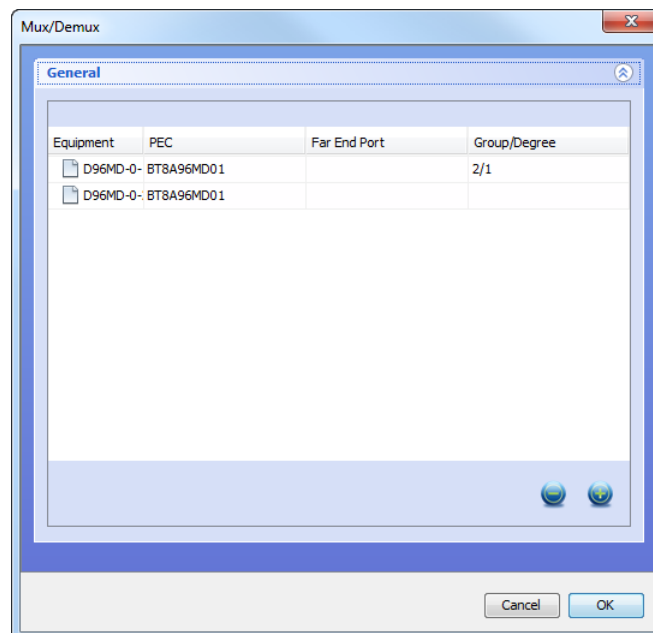
A multiplexer/demultiplexer is a passive module that provides access to add/drop wavelengths in a DOL nodal configuration.

### Adding or Viewing a multiplexer/demultiplexer

Use this procedure to view existing multiplexer/demultiplexers or to add a new one on a BTI7000 Series network element.

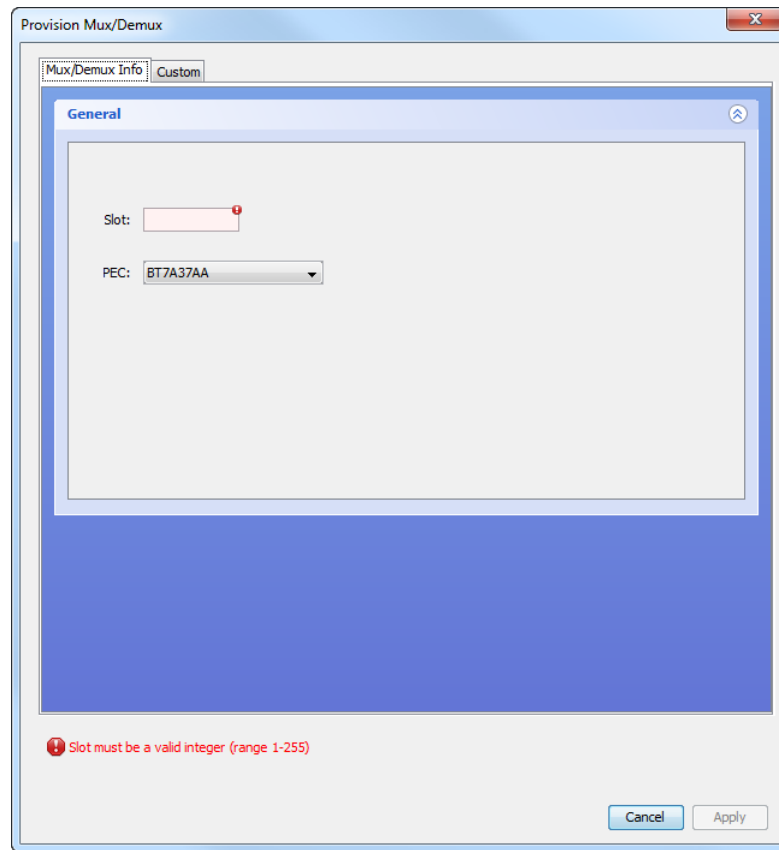
1. Right click a network element in the Network tree and select **Node > Passive > Mux/Demux > Edit**

The **Mux/Demux** window appears. This window shows a listing of the existing multiplexer/demultiplexers on the shelf, and the group/degree to which each multiplexer/demultiplexer is assigned (if any).



2. Click on the plus icon to add a new multiplexer/demultiplexer.

The **Provision Mux/Demux** window appears.



3. Specify the **Slot** for the multiplexer/demultiplexer.
4. Select a PEC from the list of available PECs.
5. Optionally, specify the **Custom** fields. These fields are for operator use and are opaque to the system.
  - a. Click the **Custom** tab.
  - b. In the **Custom** panel, specify the **Id**, **Custom 1**, **Custom 2**, and **Custom 3** settings as desired.
6. When you are finished, click **Apply**.

The newly added multiplexer/demultiplexer appears in the **Mux/Demux** window. To assign the multiplexer/demultiplexer to an optical group and degree, see [“Assigning or Unassigning Equipment” on page 170](#).

7. Click **OK**.



The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View > Server > Tasks** window. The new provisioning appears in PSM a short while after the task completes successfully.

### Deleting a multiplexer/demultiplexer

Use this procedure to delete a multiplexer/demultiplexer from a BTI7000 Series network element.

1. Right click a network element in the Network tree and select **Node > Passive > Mux/Demux > Edit**

The **Mux/Demux** window appears.

2. Select a multiplexer/demultiplexer and click on the minus icon to delete it.

The selected multiplexer/demultiplexer disappears from the window.

3. Click **OK**.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View > Server > Tasks** window. The new provisioning takes effect a short while after the task completes successfully.

## Provisioning GCC on a BTI7000 Series Network Element

### Provisioning GCC

Use this procedure to provision GCC on a transponder, muxponder, or PVX port on a BTI7000 Series network element. GCC is used to carry management traffic inband.

1. Expand the network element in the Network tree to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.
3. Expand a transponder, muxponder, or PVX to see the ports on that module.
4. Right click a provisioned port and select **GCC > Provision**.



**NOTE:** GCC is only available for selection when the transceiver is configured for certain protocols.

The **Manage GCC** dialog appears.

5. Configure GCC as follows:
  - **Mode:** The mode is set at Full Rate and cannot be changed.
  - **Admin State:** Select **Enabled** or **Disabled**.

- **Operational State:** The operational state is read-only.
- **Secondary State:** The secondary state is read-only.

6. When you are finished, click **Apply**.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View > Server > Tasks** window. The new provisioning appears in PSM a short while after the task completes successfully.

---

### Deleting GCC

Use this procedure to delete GCC from a transponder, muxponder, or PVX port on a BTI7000 Series network element.

1. Expand the network element in the Network tree to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.
3. Expand a transponder, muxponder, or PVX to see the ports on that module.
4. Right click a provisioned port and select **GCC > Delete**.
5. Click **OK** in the confirmation dialog.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View > Server > Tasks** window. The new provisioning appears in PSM a short while after the task completes successfully.

### Viewing Port PMs on a BTI7000 Series Network Element

Use this procedure to view current port PMs on transponder, muxponder, and packetVX modules on a BTI7000 Series network element.

1. Expand the network element in the Network tree to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.
3. Right-click a transponder, muxponder, or packetVX module and select **Port PM > View**

The **Port PM** window appears. By default, the current 15-minute bin is displayed. Here is an example of the window for a transponder module:

Port PM Thu 25 Jun 2015 16:25:37 EDT - 3 Ports (15 Minute)

Port	Protocol	Wavelength...	OPR (dBm)	OPR-AVG (...)	OPT (dBm)	CV	ES	SES	UAS	INBLK	TFCRX	FRDR
TPR-1-2-1	10GBELAN E...	1559.79 : n/a	-14.4	-14.5	1.5	n/a	n/a	n/a	n/a	n/a	5580751151	0
TPR-1-2-2	10GBELAN	1550.0 : n/a	-2.0	-2.0	1.2	n/a	0	0	0	0	n/a	n/a
TPR-1-2-3	10GBELAN E...	1559.79 : n/a	-11.9	-12.3	1.5	n/a	n/a	n/a	n/a	n/a	n/a	n/a

Bin: 15 Minute

Valid Partial Invalid

Refresh Export


The counts are color-coded to show valid, partial, and invalid counts. In most situations, the running counters will be partial counts because you are retrieving the counts in the middle of a bin period. An invalid count indicates that the count cannot be retrieved and therefore cannot be trusted. An n/a designation indicates that the particular count is not applicable to this port and protocol.



**NOTE:** This window shows a snapshot of the PM counts. The counts do not update automatically in this window. To see the latest counts, click the **Refresh** button.

- To see the 1-day bin or the untimed bin, select the desired bin from the **Bin** drop-down menu in the lower left corner, and click the **Refresh** button.

The PM counts for the selected bin appears shortly.

- To select what columns to display, click the  icon in the upper right corner to bring up the **Change Visible Columns** window. Alternatively, if you are only making a single change, right-click anywhere in the headings row to bring up a column selection window that disappears after you make a single change.

Check or uncheck column headings as desired.

- To sort the PMs based on column values, click on the column heading that you want to sort.
- To export the PM data to a CSV file, click **Export** and save the file.

## Provisioning the BTI7000 Series Dynamic Optical Layer (DOL)

The BTI7000 Series Dynamic Optical Layer provides reconfigurable optical add/drop multiplexing, reach extension, and end-to-end service management for the BTI7000 Series optical network. The Dynamic Optical Layer consists of ROADM modules that provide wavelength routing, line amplifier modules that provide reach extension, and passive multiplexer/demultiplexer modules that provide wavelength access. A DOL node can be configured to be a channel equalizing terminal, a channel equalizing line node, a line amplifier node, or a ROADM node.

Before you can provision DOL, you must first add optical modules to the shelf. To add a module, follow the steps in [“Adding a Module” on page 137](#) and select the desired module from the PEC drop-down list. Once all the modules are added, use the procedures in this section to create the desired optical nodal function.

Once the nodal function is created, you can activate DOL services using the procedures described in [“Optical Services” on page 301](#).

---

### Provisioning Optical Groups

An optical group is a representation of an optical node (i.e. a collection of modules that together provide a specific nodal function in the optical network). An optical node can be a DOL or a non-DOL node.

The following optical group types are supported:

- **NON\_EQUALIZING\_TERM** - This is a non-channel equalizing terminal that consists of non-equalizing amplifiers that do not support DOL.
- **CHANNEL\_EQUALIZING\_TERMINAL** - This is a channel equalizing terminal that consists of DOL equipment.
- **LINE\_AMPLIFIER\_NODE** - This is a non-channel equalizing line node that consists of DOL equipment.
- **CHANNEL\_EQUALIZING\_LINE\_NODE** - This is a channel equalizing terminal that consists of DOL equipment.
- **ROADM** - This is a ROADM node that consists of DOL equipment.

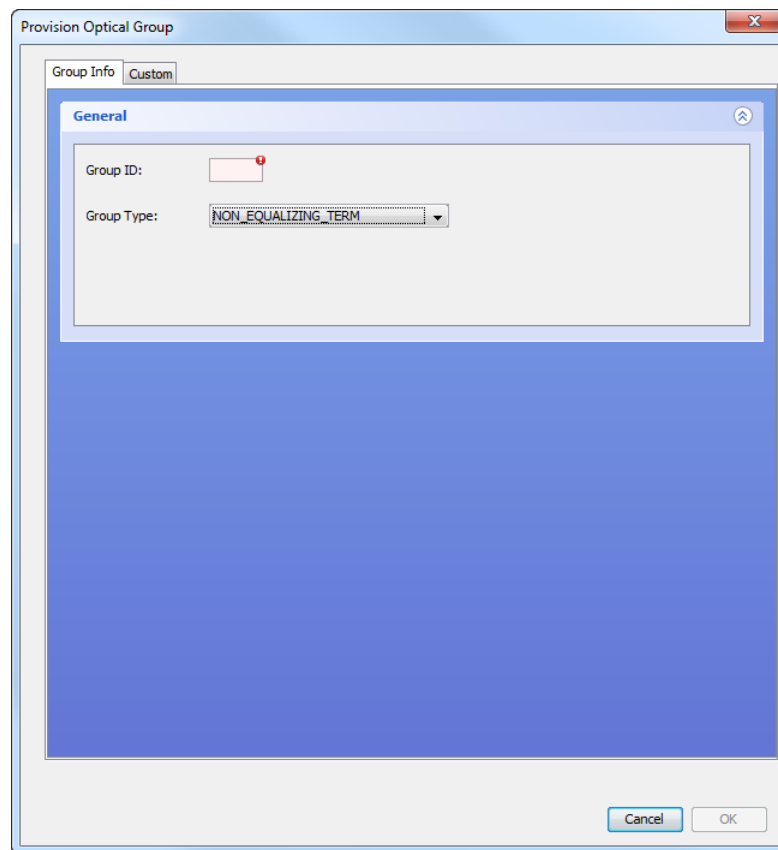
### *Creating an Optical Group*

Use this procedure to create an optical group on a BTI7000 Series network element.

1. Expand the network element in the Network tree to show the shelves in that NE.
2. Right-click on **Optical Groups** and select **Group/Degree >Provision**.

The **Provision Optical Group** dialog appears:

Figure 37: Provision Optical Group



3. Configure the group as follows:
  - **Group ID** Specify the Group ID to distinguish the new group from the other optical groups on the node.
  - **Group Type** Specify the function for the group from the drop-down menu.
4. Optionally, specify the **Custom** fields. These fields are for operator use and are opaque to the system.
  - a. Click the **Custom Settings** tab.
  - b. In the **Custom Settings** panel, specify the **Id**, **Custom 1**, **Custom 2**, and **Custom 3** settings as desired.
5. When you are finished, click **OK**.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View > Server > Tasks** window. The new optical group appears in the Network tree a short while after the task completes successfully.

### Assigning or Unassigning Equipment

Use this procedure to assign or unassign equipment to or from an optical group on a BT17000 Series network element. An optical group is a collection of modules that together provide a specific nodal function in the optical network. Modules must belong to an optical group in order to provide the nodal function.

1. Expand the network element in the Network tree.
2. Expand the **Optical Groups** to see the optical groups on that NE.
3. Right-click the optical group in which you want to assign equipment, and select **Group/Degree >Edit**.

The **Update Optical Group** dialog appears.

Equipment	Shelf	Slot	Degree
ROB-11-1	11	1	1
D96MD-0-10	0	10	1

At the bottom of the dialog are 'Cancel' and 'Apply' buttons.

The **Group ID** is set during optical group creation, and cannot be edited.

4. Assign or unassign equipment from the group.
  - To assign equipment to the group, click on the plus icon. This brings you to the **Assign Optical Equipment** window where you can assign equipment by selecting the degree

and the equipment. Click **Apply** when you are done. The newly assigned equipment appears in the Equipment list.



**NOTE:** If the degree that you select does not yet exist, the degree is created and will appear in the Network tree.

- To unassign equipment, select the equipment from the list and then click on the minus icon. The unassigned equipment is removed from the Equipment list.
5. Configure the **Custom** fields. These fields are for operator use and are opaque to the system.
    - a. Click the **Custom Settings** tab.
    - b. In the **Custom Settings** panel, edit the **Id**, **Custom 1**, **Custom 2**, and **Custom 3** settings as desired.
  6. When you are finished, click **Apply**.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View > Server > Tasks** window. The changes appear in PSM a short while after the task completes successfully.

#### ***Deleting an Optical Group***

Use this procedure to delete an optical group on a BT17000 Series network element.

1. Expand the network element in the Network tree to show the shelves in that NE.
2. Expand **Optical Groups** to show the optical groups in that NE.
3. Right-click an optical group and select **Group/Degree > Delete**.
4. Click **OK** in the confirmation dialog.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View > Server > Tasks** window. The deleted group disappears from the Network tree a short while after the task completes successfully.

#### ***Editing WDM Parameters in an Optical Group***

Use this procedure to edit WDM parameters on a BT17000 Series network element. WDM parameters apply to the respective line span for equipment in optical groups.

1. Expand the network element in the Network tree.
2. Expand **Optical Groups** to see the optical groups on that NE.
3. Expand an optical group to see the degrees in that group.

4. Expand a degree to see the equipment in that degree.
5. Right-click on the module you want to edit and select **WDM >Edit**.

The **Edit WDM** dialog appears.

*Figure 38: Edit WDM Dialog for a BT17000 Series ROADM Module*

The dialog (and/or tabs) might differ depending on the module selected.

6. Configure the WDM parameters as follows:



**NOTE:** Not all of the parameters below appear in all dialogs.

- **Administrative State** Select the state from the list of available states in the drop-down menu.
- **State** This is the operational state. It is read-only.
- **Secondary State** This is the secondary operational state. It is read-only.
- **Fiber Type** Specify the fiber type from the list of available fiber types in the drop-down menu.



- **Measured Span Length** The span length is measured automatically. This is read-only.
  - **Measured Span Loss** The span loss is measured automatically. This is read-only.
  - **Max. Supported Span Loss** The maximum supported span loss is calculated automatically. This is read-only.
  - **Max. Span Loss Alarm Threshold** Specify the span loss threshold beyond which an alarm is raised. This field can only be edited if **Enable Alarm** is selected.
  - **Loss Rx High Threshold**- Similar to **Max. Span Loss Alarm Threshold**. Specify the span loss threshold beyond which an alarm is raised. Set to 0 to disable.
  - **Enable Alarm** Select to enable the span loss threshold alarm.
  - **Provisioned Channels** This is the number of channels that can be carried. This is read-only.
  - **Amp Tilt Trim** Set to fine tune the system gain tilt.
  - **Post Amp Gain** Set the system gain.
  - **Auto-In Service Timer** Optionally, specify the AINS timer. This attribute is only applicable if the **Administrative State** is **Auto-In-Service**.
  - **Active Countdown** This is the countdown for the AINS timer. It is read-only.
7. Configure the **Custom** fields. These fields are for operator use and are opaque to the system.
    - a. Click the **Custom Settings** tab.
    - b. In the **Custom Settings** panel, edit the **Id**, **Custom 1**, **Custom 2**, and **Custom 3** settings as desired.
  8. When you are finished, click **Apply**.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View > Server > Tasks** window. The changes appear in PSM a short while after the task completes successfully.

### Adding and Deleting the C2 Port

In some BT17000 Series nodal configurations, the C2 port of a ROADM module is optional. In these situations, PSM does not automatically create the C2 port, but leaves it up to the user to create it manually.

Use this procedure to create and/or delete the optional C2 port on a BT17000 Series ROADM module for the optical group type **CHANNEL\_EQUALIZING\_TERMINAL**. In this configuration, the C2 port can be used to connect to alien wavelengths. See the *BT17000 Series Dynamic Optical Layer Engineering Guideline* for details.

1. Expand the network element in the Network tree.
2. Expand the **Optical Groups** to see the optical groups on that NE.

3. Expand an optical group to see the degrees in that group.

4. Expand a degree to see the equipment in that degree.

5. To add the C2 port, right-click on the ROADM module and select **C2 >Provision**.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View >Server >Tasks** window. The C2 port is added to the ROADM in that degree a short while after the task completes successfully.

6. To delete a previously-added optional C2 port, right-click on the ROADM module and select **C2 >Delete**.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View >Server >Tasks** window. The C2 port is deleted from the ROADM in that degree a short while after the task completes successfully.

---

### Editing Optical Port Parameters

Use this procedure to edit optical port parameters on a BT17000 Series network element. An optical port can be a line port, a client port, or a DCM port.

1. Expand the network element in the Network tree.

2. Expand the **Optical Groups** to see the optical groups on that NE.

3. Expand an optical group to see the degrees in that group.

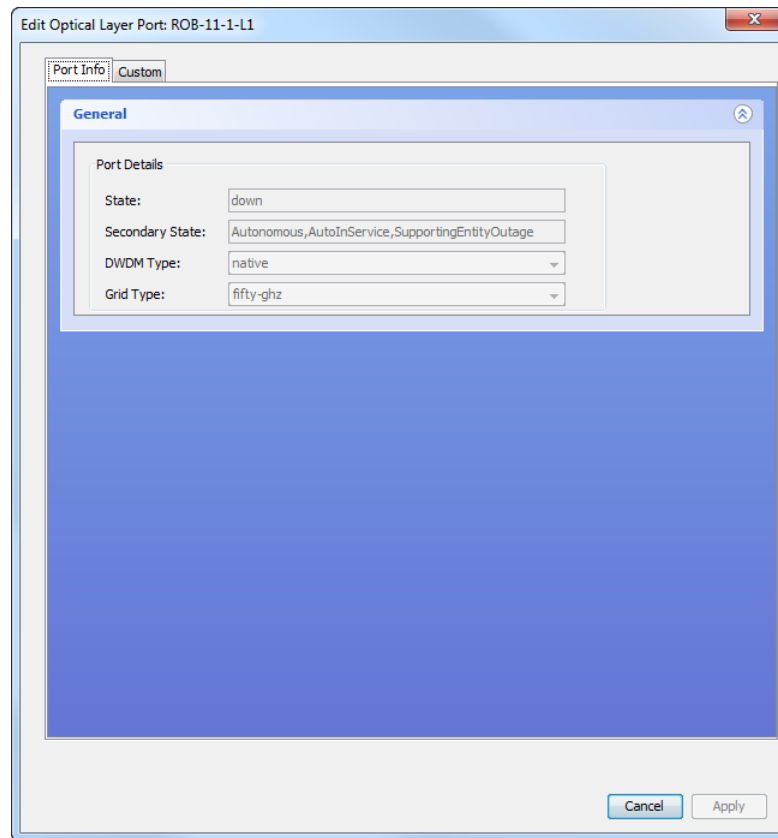
4. Expand a degree to see the equipment in that degree.

5. Expand a module to see the ports on that module.

6. Right-click on an optical port you want to edit and select **Optical Port >Edit**.

The **Edit Optical Layer Port** dialog appears.

Figure 39: Edit Optical Layer Port Dialog for a BTI7000 Series ROADM Line Port



The dialog (and/or tabs) might differ depending on the module and port selected.

7. Configure the optical port parameters as follows:



**NOTE:** Not all of the parameters below appear in all dialogs.

- **State** This is the operational state. It is read-only.
- **Secondary State** This is the secondary operational state. It is read-only.
- **DWDM Type** This is the type of DWDM composite signal expected on the port. It is set to **native** when connected to DOL equipment. It is set to **alien** when connected to other equipment. This is read-only.
- **Grid Type** This is the DWDM grid spacing for the port. If the equipment only supports a specific grid spacing, then this field is read-only.
- **Fiber Connection** This shows the equipment at the other end of the fiber connection. This is read-only.
- **Wavelength** The wavelength for the port. This is read-only.
- **Frequency** The frequency for the port. This is read-only.

- **Tx Loss** Specify the optical loss in the transmit direction. Set to 0 for no loss.
  - **Auto-In Service Timer** Optionally, specify the AINS timer.
  - **Active Countdown** This is the countdown for the AINS timer. It is read-only.
- Optionally, configure the **Custom** fields. These fields are for operator use and are opaque to the system (with the exception of the Remote ID).
    - Click the **Custom Settings** tab.
    - In the **Custom Settings** panel, edit the **Id**, **Custom 1**, **Custom 2**, and **Custom 3** settings as desired.
    - Set the **Remote Id** to describe the equipment at the other end of the fiber. PSM uses the **Remote Id** when determining topology.
  - When you are finished, click **Apply**.

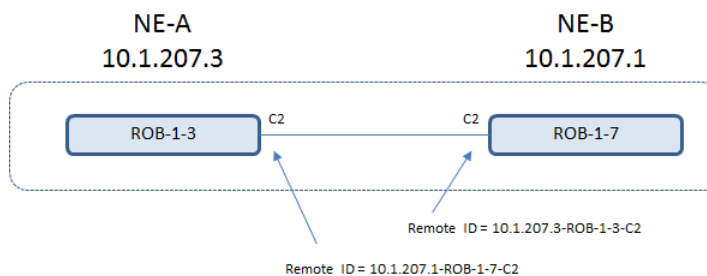
The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View > Server > Tasks** window. The changes appear in PSM a short while after the task completes successfully.

### Configuring a Split ROADM Node

Use this procedure to configure a split ROADM node on a BTI7000 Series system.

A split ROADM node is a highly survivable configuration where each ROADM module in a BTI7000 Series ROADM node is located in a separate network element, managed by a separate management module. While these network elements are distinct in every other aspect, PSM treats this combination as a single ROADM node during optical service activation.

Creating a split ROADM node is essentially a hardware installation function where the ROADM modules are installed on separate network elements and connected together by fiber over their C2 ports. There is no provisioning required except to enable PSM to recognize the split ROADM node. In order for PSM to recognize the split ROADM node as a single ROADM node, the Remote ID configuration on the C2 ports of the ROADM modules must point to each other. This is shown in the following figure. By configuring the Remote IDs on the C2 ports in this manner, PSM is able to recognize this as a split ROADM node configuration.



A split ROADM node can be configured for the **CHANNEL\_EQUALIZING\_LINE\_NODE** and **ROADM** optical group types.

1. Follow the procedure in “[Setting the Remote ID on a ROADM C2 Port](#)” on page 82 to set the Remote ID on a ROADM C2 port.

Configure the Remote ID to point to the C2 port of the second ROADM module. For example:

The screenshot shows a configuration window titled "Local Port ID". It has two main sections: "Local Port ID" and "Far End".

- Local Port ID:** A text field containing "10.1.207.3-ROB-1-3-C2".
- Far End:**
  - Remote Id:** A text field containing "10.1.207.1-ROB-1-7-C2". Below it are "Clear" and "Reset" buttons.
  - Edit:** A sub-section containing several fields:
    - Hostname/IP Address:** "10.1.207.1"
    - CP Type:** A dropdown menu showing "ROB".
    - Shelf:** A dropdown menu showing "1".
    - Slot:** A dropdown menu showing "7".
    - Port:** A text field showing "C2".
    - Alien:** An unchecked checkbox.
    - Bidirectional:** A checked checkbox.

At the bottom of the window are "Cancel" and "OK" buttons.

By selecting the **Bidirectional** option, PSM automatically configures the C2 port at the other end to point back to this C2 port.

### Editing OSC Parameters in an Optical Group

Use this procedure to edit OSC parameters on a BTI7000 Series network element. The optical service channel (OSC) is used as a communications medium for control information between optical equipment at both ends of a line span. Through the OSC, optical elements share information and automatically measure span loss, adjust the system gain, and leverage a multi-span feedback loop that enables per-channel pre-emphasis to address wavelength tilt and ripple.

1. Expand the network element in the Network tree.
2. Expand the **Optical Groups** to see the optical groups on that NE.
3. Expand an optical group to see the equipment in that group.
4. Right-click on the module you want to edit and select **OSC >Edit**.

The **Edit OSC** dialog appears.

Figure 40: Edit OSC Dialog for a BTI7000 Series ROADM Module

The screenshot shows a window titled 'Edit OSC Dialog for a BTI7000 Series ROADM Module'. It has four tabs: 'General', 'FarEnd', 'ODCC', and 'Custom'. The 'General' tab is selected and contains two main sections: 'Administration Info' and 'AINS Timer'. Under 'Administration Info', there is a dropdown for 'Administrative State' set to 'Auto-In-Service', a text field for 'State' set to 'down', and a text field for 'Secondary State' set to 'AU, AINS, SGEO'. Under 'AINS Timer', there is a 'Config' section with a 'Timer' field showing '0 days 8 hours 0 minutes' and an 'Active Countdown' field set to '<None>'. At the bottom right are 'Cancel' and 'Apply' buttons.

The dialog (and/or tabs) might differ depending on the module selected.

5. In the **General** tab, configure the OSC parameters as follows:



**NOTE:** Not all of the parameters below appear in all dialogs.

- **Administrative State** or **Admin Status** Select the state from the list of available states in the drop-down menu.
- **State** or **Oper Status** This is the operational state. It is read-only.
- **Secondary State** This is the secondary operational state. It is read-only.
- **AINS Timer** Optionally, specify the AINS timer. This attribute is only applicable if the **Administrative State** is **Auto-In-Service**.
- **Active Countdown** This is the countdown for the AINS timer. It is read-only.

6. In the **OSC Info** tab, configure the OSC parameters as follows:



**NOTE:** Not all of the parameters below appear in all dialogs.

- **Admin Status** Select the state from the list of available states in the drop-down menu.
  - **Oper Status** This is the operational state. It is read-only.
  - **FE IM Mon** Select if you want the near end to validate the identity of the far end with the expected far end parameters. If the identity does not match, the system will raise an alarm or condition.
  - **System Name (actual)** This is the actual system name of the far end. It is read-only.
  - **IP Address (actual)** This is the actual NMS IP address of the far end. It is read-only.
  - **Group (actual)** This is the actual optical group identifier of the far end. It is read-only.
  - **Degree (actual)** This is the actual optical degree of the far end. It is read-only.
  - **Group Type (actual)**- This is the actual group type of the far end. It is read-only.
  - **System Name (expected)** Set to the expected system name of the far end.
  - **IP Address (expected)** Set to the expected NMS IP address of the far end.
  - **Group (expected)** Set to the expected optical group identifier of the far end.
  - **Degree (expected)** Set to the expected optical degree of the far end.
7. In the **FarEnd** tab, configure the OSC parameters as follows:



**NOTE:** Not all of the parameters below appear in all dialogs.

- **Far-End Monitoring** Select if you want the near end to validate the identity of the far end with the expected far end parameters. If the identity does not match, the system will raise an alarm or condition.
  - **System Name (actual)** This is the actual system name of the far end. It is read-only.
  - **NMS IP Address (actual)** This is the actual NMS IP address of the far end. It is read-only.
  - **Optical Group (actual)** This is the actual optical group identifier of the far end. It is read-only.
  - **Optical Degree (actual)** This is the actual optical degree of the far end. It is read-only.
  - **Group Type (actual)**- This is the actual group type of the far end. It is read-only.
  - **System Name (expected)** Set to the expected system name of the far end.
  - **NMS IP Address (expected)** Set to the expected NMS IP address of the far end.
  - **Optical Group (expected)** Set to the expected optical group identifier of the far end.
  - **Optical Degree (expected)** Set to the expected optical degree of the far end.
8. In the **ODCC** tab, configure the ODCC parameters as follows:



**NOTE:** Not all of the parameters below appear in all dialogs.

The optical data communications channel (ODCC) is used to carry inband management traffic between Juniper Networks network elements.

- **Enable** Select to enable ODCC within the OSC.
  - **Admin Status** Select the state from the list of available states in the drop-down menu.
  - **Oper Status** This is the operational state of the ODCC. It is read-only.
9. Optionally, configure the **Custom** fields. These fields are for operator use and are opaque to the system.
    - a. Click the **Custom Settings** tab.
    - b. In the **Custom Settings** panel, edit the **Id**, **Custom 1**, **Custom 2**, and **Custom 3** settings as desired.
  10. When you are finished, click **Apply**.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View > Server > Tasks** window. The changes appear in the Network tree (if applicable) a short while after the task completes successfully.

## Enabling or Disabling a Port

Use this procedure to administratively enable or disable a port on a BT17000 Series network element.

1. Expand the network element in the Network tree to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.
3. Expand a module to show the ports on that module.
4. Enable or disable a port as follows.
  - a. To enable a provisioned port, right click the port and select **Admin State > Enable**.  
For PVX ports, you have the option of enabling the port at layer 1 or at layer 2.
  - b. To disable a provisioned port, right click the port and select **Admin State > Disable**.  
For PVX ports, you have the option of disabling the port at layer 1 or at layer 2.



## Nodal Management for BTI7800 Series Network Elements

---



**NOTE:** The BTI7800 typically provisions equipment automatically when the modules are physically installed. This is called auto-provisioning. See the *BTI7800 Series Software Configuration Guide* for details.

---

- [Provisioning a BTI7800 Chassis on page 181](#)
- [Provisioning a Universal Forwarding Module on a BTI7800 on page 184](#)
- [Provisioning a ROADM Node on a BTI7800 on page 216](#)
- [Provisioning a 96-Channel Amplifier on a BTI7800 on page 241](#)
- [Provisioning a Wavelength Protection Switch Module on a BTI7800 on page 251](#)
- [Enabling or Disabling a Port on page 257](#)

### Provisioning a BTI7800 Chassis

#### Adding a Shelf

---

Use this procedure to add a new chassis on a BTI7800 Series network element.

1. Right-click a network element in the Network tree or in the Topology Map view and select **Node > Shelf > Provision**.

The **Provision Shelf** dialog appears:

*Figure 41: BT17800 Series Provision Shelf*

Provision Shelf

Settings Custom Settings

**General**

PEC: 14-slot (BT8A78CH14) Alias:

Shelf Number: 2

**Chassis Information**

Location: Chassis Type: 14-Slot

**State Management**

Admin Status: Up

Cancel OK

2. Configure the shelf as follows:
  - **PEC** Select the PEC from the list of available PECs in the drop-down menu.
  - **Shelf Number** Select the shelf number from the drop-down menu. The drop-down menu only displays the shelf numbers that are available and not already in use.
  - **Alias** Optionally, enter a string identifying the shelf.
  - **Location** Optionally, enter a string describing the location of the NE.
  - **Chassis Type** The chassis type is automatically populated based on the PEC.
  - **Admin Status** Specify whether the initial state of the shelf is **Up** or **Down** or **Testing**.
3. Optionally, specify the **Custom** fields. These fields are for operator use and are opaque to the system.
  - a. Click the **Custom Settings** tab.

- b. In the **Custom Settings** panel, specify the **Custom 1**, **Custom 2**, and **Custom 3** settings as desired.
4. When you are finished, click **OK**.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View > Server > Tasks** window. The new provisioning appears in the Network tree view a short while after the task completes successfully.

### Editing a Shelf

Use this procedure to edit a chassis on a BT17800 Series network element.

1. Expand a network element in the Network tree view to show the shelves on that network element.
2. Right-click a shelf and select **Shelf > Edit**.

The **Edit Shelf** dialog appears:

*Figure 42: BT17800 Series Provision Shelf*

The screenshot shows the 'Edit Shelf' dialog box with the following details:

- Tabs:** Settings, Custom Settings, General (selected).
- General Section:**
  - PEC: 14-slot (BT8A78CH14)
  - Alias: (empty field)
  - Shelf Number: 1
- Chassis Information Section:**
  - Location: (empty field)
  - Chassis Type: 14-Slot
- State Management Section:**
  - Admin Status: Up
- Buttons:** Cancel, Apply

3. Edit the shelf as follows:

- **PEC** This field is read-only.
  - **Shelf Number** This field is read-only.
  - **Alias** Enter a string identifying the shelf.
  - **Location** Enter a string describing the location of the NE.
  - **Chassis Type** This field is read-only.
  - **Admin Status** Specify whether the state of the shelf is **Up** or **Down** or **Testing**.
4. Optionally, specify the **Custom** fields. These fields are for operator use and are opaque to the system.
    - a. Click the **Custom Settings** tab.
    - b. In the **Custom Settings** panel, specify the **Custom 1**, **Custom 2**, and **Custom 3** settings as desired.
  5. When you are finished, click **Apply**.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View > Server > Tasks** window. The new provisioning appears in the Network tree view a short while after the task completes successfully.

---

### Deleting a Shelf

Use this procedure to delete a chassis on a BTI7800 Series network element.

#### Prerequisites:

All components on the shelf must be deleted before you can delete the shelf.

1. Expand the network element in the Network tree view to show the shelves in that NE.
2. Right-click a shelf and select **Shelf > Delete**.
3. Click **OK** in the **Delete Shelf** confirmation dialog.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View > Server > Tasks** window. The new provisioning appears in the Network tree view a short while after the task completes successfully.

### Provisioning a Universal Forwarding Module on a BTI7800

- [Adding a UFM on page 185](#)
- [Editing a UFM on page 187](#)
- [Deleting a UFM on page 188](#)
- [Adding a BIC on page 188](#)
- [Editing a BIC on page 190](#)

- [Cloning a BIC on page 191](#)
- [Deleting a BIC on page 192](#)
- [Adding a Transceiver on page 193](#)
- [Editing a Transceiver on page 195](#)
- [Cloning a Transceiver on page 196](#)
- [Deleting a Transceiver on page 197](#)
- [Adding an Interface on page 198](#)
- [Editing an Interface on page 205](#)
- [Configuring a Multiplexed Interface on page 211](#)
- [Cloning an Interface on page 213](#)
- [Deleting an Interface on page 214](#)
- [Viewing Interface PMs on a UFM on page 215](#)

---

### **Adding a UFM**

Use this procedure to add a new UFM on a BT17800 Series network element.

1. Expand the network element in the Network tree to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.
3. Right-click an unprovisioned slot and select **Slot >Provision** to add a module in that slot.

The **Provision Slot** dialog appears:

Figure 43: BT17800 Series Provision Slot

The screenshot shows the 'Provision Slot' configuration window. It has a title bar with a close button. Below the title bar are two tabs: 'Settings' and 'Custom Settings'. The 'Settings' tab is selected. Inside the 'Settings' tab, there are two main sections: 'General' and 'State Management'. The 'General' section contains two dropdown menus: 'PEC' (set to 'UFM1 - 100G XCVR (BT8A78UFM1)') and 'UFM Type' (set to 'MSA\_SWITCHING'). The 'State Management' section contains one dropdown menu: 'Admin Status' (set to 'Up'). At the bottom right of the window are 'Cancel' and 'OK' buttons.

4. Configure the slot as follows:
  - **PEC** Select a UFM PEC from the list of available PECs in the drop-down menu.
  - **UFM Type** This read-only field is automatically populated, and shows the BIC configuration supported for the UFM selected.
  - **Admin Status** Specify whether the initial state of the module is **Up** or **Down** or **Testing**.
5. Optionally, specify the **Custom** fields. These fields are for operator use and are opaque to the system.
  - a. Click the **Custom Settings** tab.
  - b. In the **Custom Settings** panel, specify the **Id**, **Custom 1**, **Custom 2**, and **Custom 3** settings as desired.
6. When you are finished, click **OK**.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View > Server > Tasks** window. The new provisioning appears in the Network tree view a short while after the task completes successfully.

### Editing a UFM

Use this procedure to edit an existing UFM on a BT17800 Series network element.

1. Expand the network element in the Network tree view to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.
3. Right-click a UFM and select **Slot >Edit** to edit the module in that slot.

The **Edit Slot** dialog appears.

*Figure 44: BT17800 Series Edit Slot (UFM)*

The screenshot shows a window titled "Edit Slot 10.1.220.104 ufm:1/2". Inside, there are two tabs: "Settings" and "Custom". The "Settings" tab is selected and contains two expandable sections. The "General" section is expanded, showing "PEC" as "UFM3 lite (BT8A78UFM3)" and "UFM Type" as "DUAL\_BIC\_NO\_SWITCHING". The "State Management" section is also expanded, showing "Admin Status" as "Up". At the bottom right of the dialog are "Cancel" and "Apply" buttons.

4. Edit the slot as follows:
  - **PEC** This field is read-only.
  - **UFM Type** This field is read-only.
  - **Admin Status** Change the state of the module to **Up** or **Down** or **Testing**.
5. Optionally, edit the **Custom** fields. These fields are for operator use and are opaque to the system.

- a. Click the **Custom Settings** tab.
  - b. In the **Custom Settings** panel, specify the **Id**, **Custom 1**, **Custom 2**, and **Custom 3** settings as desired.
6. When you are finished, click **Apply**.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View > Server > Tasks** window. The new provisioning appears in the Network tree view a short while after the task completes successfully.

---

### Deleting a UFM

Use this procedure to delete a UFM on a BTI7800 Series network element.

#### Prerequisites:

All components in the UFM must be deleted before you can delete the UFM.

1. Expand the network element in the Network tree view to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.
3. Right-click a UFM and select **Slot > Delete**.
4. Click **OK** in the **Delete Slot** confirmation dialog.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View > Server > Tasks** window. The new provisioning appears in the Network tree view a short while after the task completes successfully.

---

### Adding a BIC

Use this procedure to add a BTI Interface Card (BIC) to a UFM on a BTI7800 Series network element.



**NOTE:** Not all UFM's support BICs.

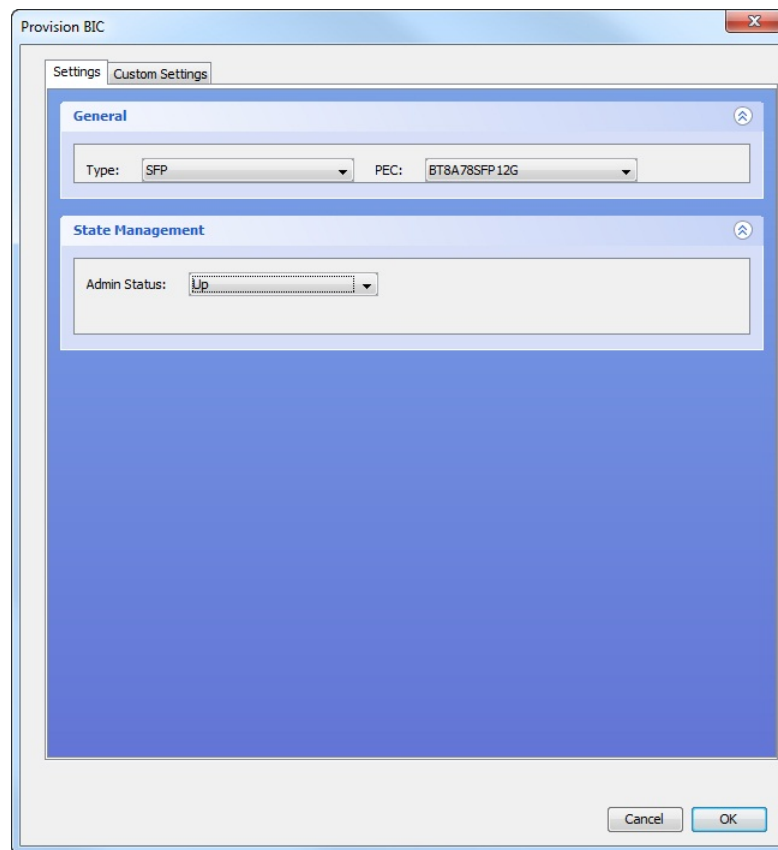
---

1. Expand the network element in the Network tree view to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.
3. Expand a UFM to show the BICs in that UFM.
4. Right-click an unprovisioned BIC and select **BIC > Provision**.

The **Provision BIC** dialog appears:



Figure 45: BT17800 Series Provision BIC



5. Configure the BIC as follows:
  - **Type** Specify the type of BIC.
  - **PEC** Select the PEC from the list of available PECs in the drop-down menu. Only the list of PECs for the specified type is shown.
  - **Admin Status** Specify whether the initial state of the module is **Up** or **Down** or **Testing**.
6. Optionally, specify the **Custom** fields. These fields are for operator use and are opaque to the system.
  - a. Click the **Custom Settings** tab.
  - b. In the **Custom Settings** panel, specify the **Id**, **Custom 1**, **Custom 2**, and **Custom 3** settings as desired.
7. When you are finished, click **OK**.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View > Server > Tasks** window. The new provisioning appears in the Network tree view a short while after the task completes successfully.

## Editing a BIC

Use this procedure to edit an existing BTI Interface Card (BIC) on a UFM on a BTI7800 Series network element.

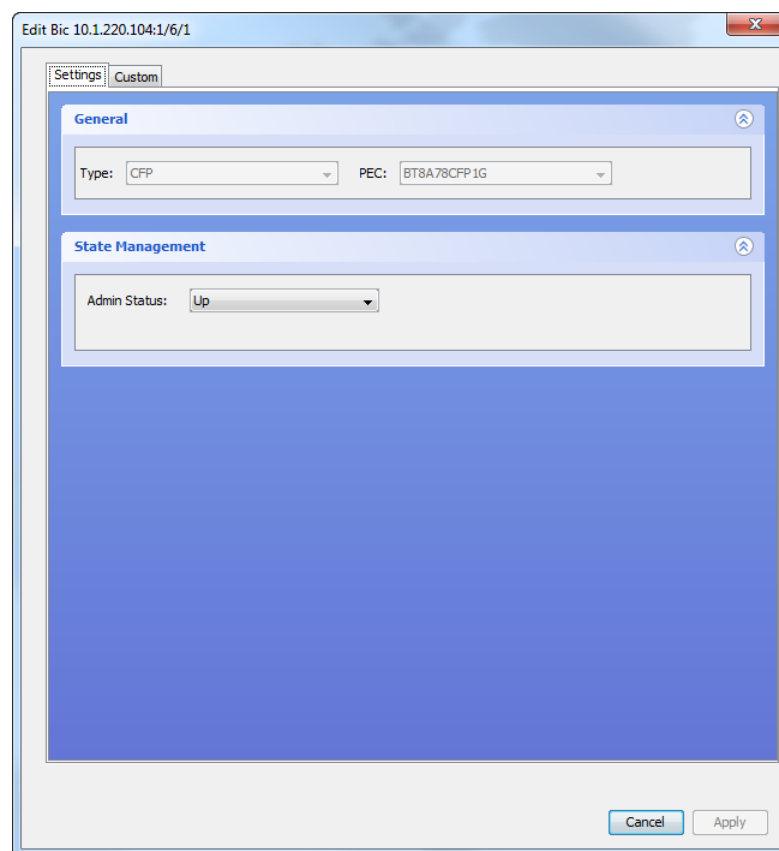


**NOTE:** Not all UFM's support BICs.

1. Expand the network element in the Network tree view to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.
3. Expand a UFM to show the BICs in that UFM.
4. Right-click an existing BIC and select **BIC >Edit**.

The **Edit BIC** dialog appears.

*Figure 46: BTI7800 Series Edit BIC*



5. Edit the BIC as follows:

- **Type** This field is read-only.
  - **PEC** This field is read-only.
  - **Admin Status** Change the state of the BIC to **Up** or **Down** or **Testing**.
6. Optionally, edit the **Custom** fields. These fields are for operator use and are opaque to the system.
    - a. Click the **Custom Settings** tab.
    - b. In the **Custom Settings** panel, edit the **Id**, **Custom 1**, **Custom 2**, and **Custom 3** settings as desired.
  7. When you are finished, click **Apply**.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View > Server > Tasks** window. The new provisioning appears in the Network tree view a short while after the task completes successfully.

### Cloning a BIC

Use this procedure to clone an existing BTI Interface Card (BIC) along with its provisioned transceivers and interfaces on a UFM on a BTI7800 Series network element.

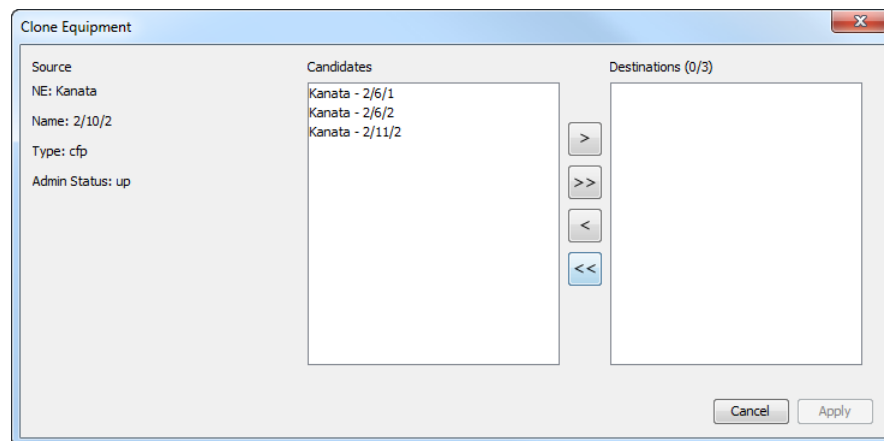


**NOTE:** Not all UFM's support BICs.

1. Expand the network element in the Network tree view to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.
3. Expand a UFM to show the BICs in that UFM.
4. Right-click a provisioned BIC and select **BIC > Clone**.

The **Clone Equipment** dialog appears.

Figure 47: BTI7800 Series Clone Equipment (BIC)



The **Candidates** pane shows the list of possible destinations to which the source BIC can be cloned. Only those destinations that are unprovisioned and compatible with the source BIC are shown. To be compatible, the target module must support the cloned BIC type.

- From the list of **Candidates**, use the arrow buttons to move one or more interfaces to the **Destinations** pane.



**NOTE:** All provisioned transceivers and interfaces that belong to the selected source BIC will be cloned as well.

- When you are finished, click **Apply**.

The PSM server sends the configuration requests to the network element. You can monitor the status of the requests through the **View > Server > Tasks** window. The new provisioning appears in the Network tree view a short while after the tasks complete successfully.

### Deleting a BIC

Use this procedure to delete a BTI Interface Card (BIC) on a UFM on a BTI7800 Series network element.

#### Prerequisites:

All transceivers and interfaces for that BIC must be deleted before you can delete the BIC.



**NOTE:** Not all UFM's support BICs.

1. Expand the network element in the Network tree view to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.
3. Expand a UFM to show the BICs in that UFM.
4. Right-click a provisioned BIC and select **BIC >Delete**.
5. Click **OK** in the **Delete BIC** confirmation dialog.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View >Server >Tasks** window. The new provisioning appears in the Network tree view a short while after the task completes successfully.

### Adding a Transceiver

Use this procedure to add a transceiver to a BIC on a UFM or to a UFM directly.



**NOTE:** Integrated transceivers on some UFM s are added automatically.

1. Expand the network element in the Network tree to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.
3. Expand a UFM to show the BICs and/or ports in that UFM.

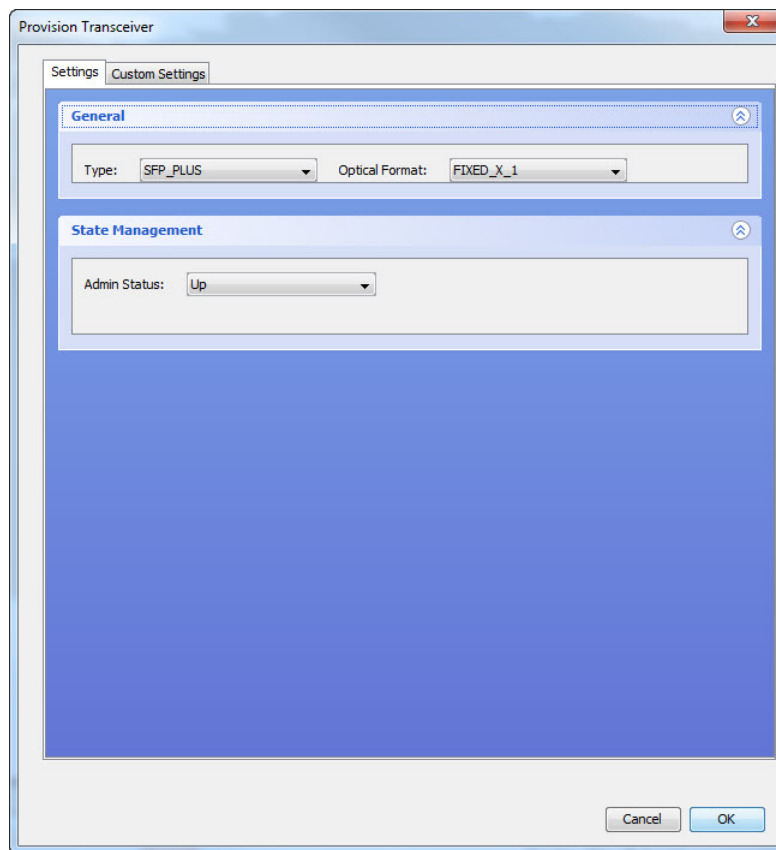


**NOTE:** Not all UFM s support BICs.

4. If you are adding a transceiver to a BIC, expand the BIC to show the ports for that BIC.
5. Right-click an unprovisioned port and select **Transceiver >Provision**.

The **Provision Transceiver** dialog appears:

Figure 48: BT17800 Series Provision Transceiver



6. Configure the transceiver as follows:
  - **Type** Specify the type of transceiver from the drop-down menu. This selection is greyed out if it has already been pre-determined by the BIC type.
  - **Optical Format** Select the optical format from the drop-down menu.
  - **Admin Status** Specify whether the initial state of the module is **Up** or **Down** or **Testing**.
7. Optionally, specify the **Custom** fields.
  - a. Click the **Custom Settings** tab. These fields are for operator use and are opaque to the system.
  - b. In the **Custom Settings** panel, specify the **Id**, **Custom 1**, **Custom 2**, and **Custom 3** settings as desired.
8. When you are finished, click **OK**.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View > Server > Tasks** window. The new provisioning appears in the Network tree view a short while after the task completes successfully.

### Editing a Transceiver

Use this procedure to edit an existing transceiver on a UFM port on a BT17800 Series network element.

1. Expand the network element in the Network tree to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.
3. Expand a UFM to show the BICs and/or ports in that UFM.

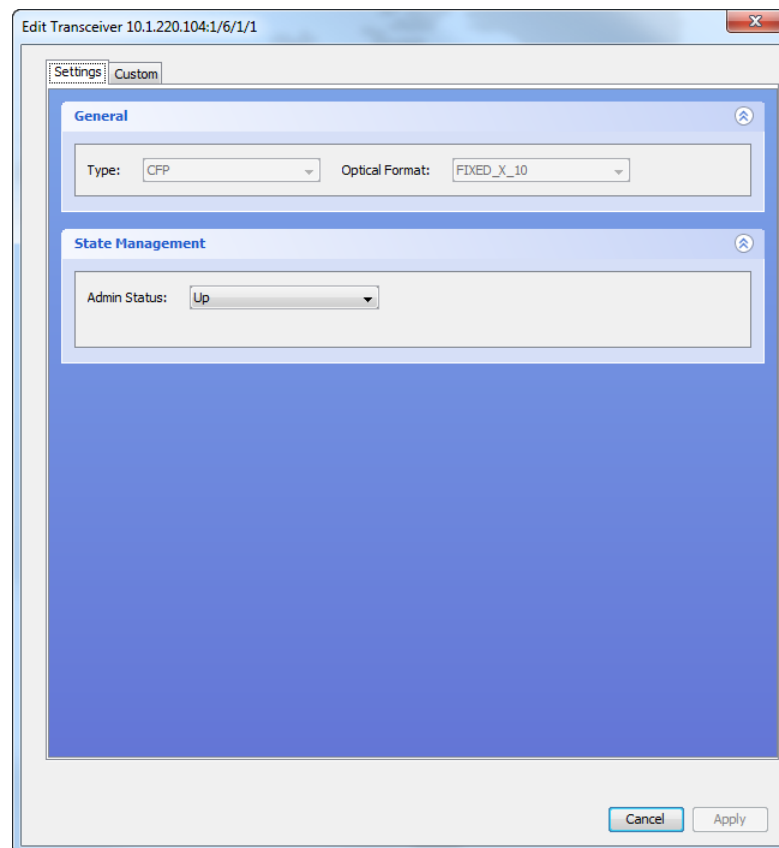


**NOTE:** Not all UFM's support BICs.

4. If you are editing a transceiver on a BIC, expand the BIC to show the ports for that BIC.
5. Right-click an existing port and select **Transceiver > Edit**.

The **Edit Transceiver** dialog appears.

*Figure 49: BT17800 Series Edit Transceiver*



6. Edit the transceiver as follows:
  - **Type** This field is read-only.
  - **Optical Format** This field is read-only.
  - **Admin Status** Change the state of the module to **Up** or **Down** or **Testing**.
7. Optionally, edit the **Custom** fields.
  - a. Click the **Custom Settings** tab. These fields are for operator use and are opaque to the system.
  - b. In the **Custom Settings** panel, edit the **Id**, **Custom 1**, **Custom 2**, and **Custom 3** settings as desired.
8. When you are finished, click **Apply**.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View > Server > Tasks** window. The new provisioning appears in the Network tree view a short while after the task completes successfully.

---

### Cloning a Transceiver

Use this procedure to clone an existing transceiver along with its provisioned interfaces on a UFM on a BT17800 Series network element.



**NOTE:** Integrated transceivers cannot be cloned.

---

1. Expand the network element in the Network tree view to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.
3. Expand a UFM to show the BICs and/or ports in that UFM.



**NOTE:** Not all UFM's support BICs.

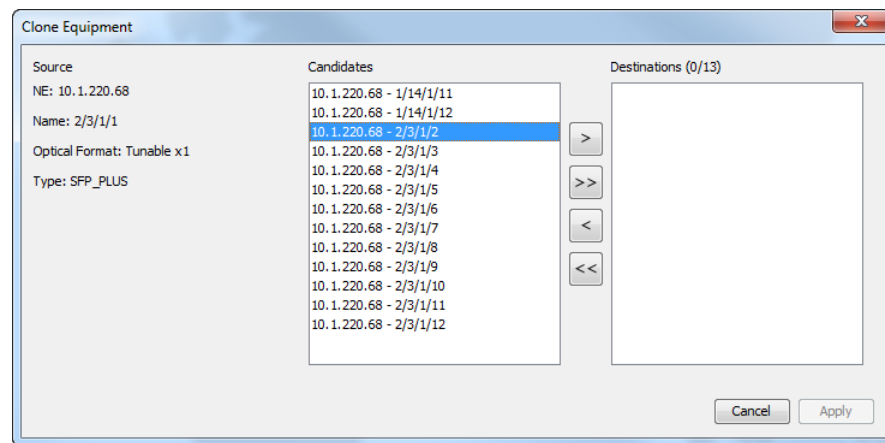
---

4. If you are cloning a transceiver on a BIC, expand the BIC to show the ports for that BIC.
5. Right-click a provisioned port and select **Transceiver > Clone**.

The **Clone Equipment** dialog appears:



Figure 50: BT17800 Series Clone Equipment (transceiver)



The **Candidates** pane shows the list of possible destinations to which the source transceiver can be cloned. Only those destinations that are unprovisioned and compatible with the source transceiver are shown. To be compatible, the source and target transceiver must have the same BIC type.

- From the list of **Candidates**, use the arrow buttons to move one or more interfaces to the **Destinations** pane.



**NOTE:** All provisioned interfaces that belong to the selected source transceiver will be cloned as well.

- When you are finished, click **Apply**.

The PSM server sends the configuration requests to the network element. You can monitor the status of the requests through the **View > Server > Tasks** window. The new provisioning appears in the Network tree view a short while after the tasks complete successfully.

### Deleting a Transceiver

Use this procedure to delete a transceiver on a UFM on a BT17800 Series network element.

#### Prerequisites:

All interfaces for that transceiver must be deleted before you can delete the transceiver.



**NOTE:** You cannot delete an integrated transceiver.

- Expand the network element in the Network tree view to show the shelves in that NE.
- Expand a shelf to show the slots in that shelf.

3. Expand a UFM to show the BICs and/or ports in that UFM.



**NOTE:** Not all UFM's support BICs.

4. If you are deleting a transceiver on a BIC, expand the BIC to show the ports for that BIC.
5. Right-click a provisioned port and select **Transceiver >Delete**.
6. Click **OK** in the **Delete Transceiver** confirmation dialog.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View >Server >Tasks** window. The new provisioning appears in the Network tree view a short while after the task completes successfully.

---

### Adding an Interface

Use this procedure to add an interface to a UFM port on a BT17800 Series network element.

Before you can add an interface, you must add the associated transceiver first.



**NOTE:** Interface parameters vary between interface types. Some parameters appear only for some interface types.

1. Expand the network element in the Network tree to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.
3. Expand a UFM to show the BICs and/or ports in that UFM.



**NOTE:** Not all UFM's support BICs.

4. If you are adding an interface to a BIC, expand the BIC to show the ports for that BIC.
5. Right-click a provisioned port and select **Interface >Provision**.

The **Provision Interface** dialog appears. For example:

Figure 51: BT17800 Series Provision Interface (OTU4)

Provision Interface 7800:1/4/1/1

Settings Custom

**General**

Type:  ☒ Enabled  
Ifindex:

**Auto In-Service**

☐ Enabled      Timer:  days  hours  minutes

**OTU**

FEC:

Degraded Threshold Per Second:

Seconds Degraded For Fault:

Expected Trace:

Tx Trace:

Cancel OK

Figure 52: BTI7800 Series Provision Interface (Optical Channel)

The screenshot shows a configuration window titled "Provision Interface 7800:1/5/2/1/2.1". It has two tabs: "Settings" and "Custom". The "General" section includes a "Type" dropdown set to "och" and an "Enabled" checkbox that is checked. Below it is an "Ifindex" text field. The "Auto In-Service" section has an "Enabled" checkbox that is unchecked, followed by a "Timer" section with spinners for "0" days, "8" hours, and "0" minutes. The "OCH" section contains several dropdown menus: "Grid" (50 GHz), "Channel Name" (C1), "Wavelength" (1566.72 nm), "Frequency" (191.35 THz), "Fiber Port" (2), "CPRWS" (64-symbols), and "Modulation" (16-qam). At the bottom right are "Cancel" and "OK" buttons.



**NOTE:** UFM6 client interfaces:

The UFM6 QSFP+ client-side transceiver supports up to four 10G client interfaces. Client interfaces are created sequentially. To create the next client interface, repeat step 5 on the same client port.

The UFM6 QSFP28 client-side transceiver supports a single 100G client interface.

There are restrictions on how client-side transceivers are installed and consequently how interfaces can be configured on the UFM6. See the *BTI7800 Series Software Configuration Guide* for details.



**NOTE:** UFM6 line interfaces:

The UFM6 400G Coherent MSA XCVR supports up to two optical channel (OCH) interfaces. Each OCH interface is associated with a physical line port on the faceplate. When you create an OCH interface, you specify the association to this line port (also known as a Fiber Port or subport). To create the other OCH interface, repeat step 5 and associate the OCH interface to the other line port. Each OCH interface (that is, each physical line port you see on the faceplate) supports up to two OTU4 tributary interfaces. To create an OTU4 tributary interface, right-click a provisioned OCH interface and select **Interface > Provision**. Repeat to create the second OTU4 tributary interface.

There are restrictions on how line interfaces can be configured on the UFM6. See the *BT17800 Series Software Configuration Guide* for details.



**NOTE:** The UFM6 OTU4 tributary interface configuration is different from the OTU4 interface configuration on the other UFM6s. Some physical layer parameters can only be configured on the containing OCH interface and not on the individual OTU4 tributary interfaces. This is because both OTU4 tributary interfaces are driven from the same set of optics.

6. Configure the general interface attributes:

- **Type** Specify the interface type from the drop-down menu.



**NOTE:** When you add an OTU interface, the BT17800 automatically creates a corresponding ODU interface. You cannot add an ODU interface directly.

- **Enabled** Select to enable the interface after provisioning.
- **Ifindex** This is read-only. It is displayed after you add the interface.

7. Configure the auto in-service attributes:

- **Enabled** Enable or disable the auto in-service timer.
- **Timer** Specify the timer value.

8. Configure the protocol attributes. Protocol attributes vary depending on the protocol.

Table 20: OTU Protocol Attributes

Attribute	Description
FEC	Specify the type of Forward Error Correction (FEC) from the drop-down menu. For UFM6 OTU interfaces within an optical channel, the FEC is set within the optical channel (OCH) interface configuration.
Delta-Q	Specify the delta Q factor difference threshold (dB) between X and Y polarization states.  This attribute represents the threshold at which the Transmitter Degrade (transmitterDegrade) alarm is raised for OTU4 interfaces.
Degraded Threshold Per Second	Set the signal degrade threshold for a 1-second interval. When the percentage of errored blocks within a 1-second interval reaches this value, the interval is considered a degraded interval. The valid range is 1 to 100 (percent) inclusive.
Seconds Degraded For Fault	Set the signal degrade fault threshold. When the number of consecutive degraded 1-second intervals reaches this value, a signal degrade fault is raised. Valid values are 0 (no fault is raised) and 2 through 10 (seconds) inclusive.
Expected Trace	Specify the trace message that is expected to be received.
Tx Trace	This is the trace message that is to be transmitted. It cannot be changed.
Rx Trace	This is the trace message that has been received. It cannot be changed. This attribute is only available on some transceivers.

Table 21: ODU Protocol Attributes

Attribute	Description
Multiplex	Specify <b>GMP_CAPABLE</b> if you want the interface to be multiplexed, or specify <b>NO_MULTIPLEX</b> if you do not want multiplexing. For more information, see <a href="#">“Configuring a Multiplexed Interface” on page 211</a> .  This attribute can only be changed for ODU4 interfaces. For other ODU interfaces, this attribute is set to <b>NO_MULTIPLEX</b> and cannot be changed.

Table 22: SONET/SDH Protocol Attributes

Attribute	Description
Expected Trace	Specify the trace message that is expected to be received.
SD-THR	Set the signal degrade fault threshold. When the threshold is set to x, a signal degrade fault is raised when the bit error rate exceeds $10 \times 10^{-x}$ . Valid values are 0 (no fault is raised) and 3 through 11 inclusive.
Mapping	Specify either <b>ASYNCHRONOUS</b> or <b>BIT_SYNCHRONOUS</b> to indicate how the SONET/SDH signal maps into the ODU payload.

*Table 23: Ethernet Protocol Attributes*

Attribute	Description
-----------	-------------

There are no protocol attributes specific to Ethernet.

*Table 24: Fibre Channel Protocol Attributes*

Attribute	Description
-----------	-------------

There are no protocol attributes specific to fibre channel.

9. Configure the physical or OCH attributes.

Some of these attributes can only be configured if the **Enabled** check box is unchecked in the **General** attributes section.

*Table 25: Physical Attributes*

Attribute	Description
<b>Grid</b>	<p>Specify the grid spacing from the drop-down menu. The grid spacing can only be specified for tunable transceivers.</p> <p>If you are editing an existing interface, you must disable the interface before you can change this attribute.</p>
<b>Wavelength or Frequency</b>	<p>Specify either the desired wavelength or the desired frequency. The wavelength or frequency can only be specified for tunable transceivers.</p> <p>If you are editing an existing interface, you must disable the interface before you can change this attribute.</p>
<b>Loopback</b>	<p>Select the type of loopback, if any, from the drop-down menu. This attribute can only be set if the <b>Enabled</b> check box is unchecked in the <b>General</b> attributes section. If the <b>Enabled</b> check box is selected, this value automatically changes to <b>NO_LOOPBACK</b>.</p>
<b>CPRWS</b>	<p>Select the carrier phase recovery window size from the drop-down menu. This attribute is not applicable to all transceiver types.</p> <p>If you are editing an existing interface, you must disable the interface before you can change this attribute.</p>
<b>Laser Enabled</b>	<p>Select to enable the transmit laser after provisioning. Uncheck to disable the transmit laser.</p>
<b>FPSD</b>	<p>Select to enable Fault Propagation Shutdown (FPSD). When a failure occurs and FPSD is enabled, the interface shuts down its laser instead of transmitting a maintenance signal.</p> <p>This attribute is only available for selection for Ethernet interfaces.</p>

Table 26: UFM6 Optical Channel (OCH) Attributes

Attribute	Description
<b>Grid</b>	Specify the grid spacing from the drop-down menu.  If you are editing an existing interface, you must disable the interface before you can change this attribute.
<b>Channel Name or Wavelength or Frequency</b>	Specify the channel, the desired wavelength, or the desired frequency. The channel number automatically determines the wavelength and frequency.  If you are editing an existing interface, you must disable the interface before you can change this attribute.
<b>Fiber Port</b>	Select the fiber port (also known as the subport).  This attribute can only be selected when adding an interface. You cannot change this attribute for an existing interface.
<b>CPRWS</b>	Select the carrier phase recovery window size from the drop-down menu.  If you are editing an existing interface, you must disable the interface before you can change this attribute.
<b>Modulation</b>	Select either <b>16-qam</b> or <b>qpsk</b> modulation. If you select <b>16-qam</b> , the optical channel contains up to two OTU4 signals. If you select <b>qpsk</b> , the optical channel contains one OTU4 signal.  This attribute can only be selected when adding an interface. You cannot change this attribute for an existing interface.  <b>NOTE:</b> In order to interwork with OTU4 signals on UFM3 and UFM4 line ports, you must configure the UFM6 optical channel for <b>qpsk</b> modulation.
<b>Tx-Power</b>	Specify the transmit power.
<b>FEC</b>	Specify the type of Forward Error Correction (FEC) from the drop-down menu.  The line coding is automatically set based on the FEC setting. If you select <b>SDFEC_25</b> , the line coding is automatically set to non-differential. If you select <b>SDFEC</b> , the line coding is automatically set to differential.
<b>Delta-Q</b>	Specify the delta Q factor difference threshold (dB) between X and Y polarization states.  This attribute represents the threshold at which the Transmitter Degrade (transmitterDegrade) alarm is raised for OCH interfaces.

10. Optionally, select **LLDP snooping**. LLDP snooping allows the BTI7800 to snoop LLDP frames on an Ethernet interface to determine the identity of the attached device.

11. Optionally, configure PRBS (pseudorandom binary sequence) generation.



Set **PRBS Mode** to **NO\_PRBS** or **EGRESS** or **INGRESS** as desired. Not all options are supported for some protocols. This attribute can only be set to **EGRESS** or **INGRESS** if the **Enabled** check box is unchecked in the **General** attributes section.

12. Optionally, specify the **Custom** fields.

- a. Click the **Custom** tab. These fields are for operator use and are opaque to the system.
- b. In the **Custom** panel, specify the **Id**, **Custom 1**, **Custom 2**, and **Custom 3** settings as desired.

13. When you are finished, click **OK**.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View > Server > Tasks** window. The new provisioning appears in PSM a short while after the task completes successfully.

### Editing an Interface

Use this procedure to edit an existing interface on a UFM on a BT17800 Series network element.



**NOTE:** Interface parameters vary between interface types. Some parameters appear only for some interface types.

1. Expand the network element in the Network tree to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.
3. Expand a UFM to show the BICs and/or ports in that UFM.



**NOTE:** Not all UFM's support BICs.

4. If you are editing an interface on a BIC, expand the BIC to show the ports for that BIC.
5. Expand a port to show the interfaces for that port.
6. If applicable, expand an interface to show the sub-interfaces for that interface.
7. Right-click a provisioned interface (or sub-interface) and select **Interface > Edit**.

The **Edit Interface** dialog appears. For example:

*Figure 53: BT17800 Series Edit Interface (OTU4)*

The screenshot displays the 'Edit Interface 7800:1/4/1/1' window. It features a 'Settings' tab and a 'Custom' sub-tab. The interface is divided into three main sections: General, Auto In-Service, and OTU.

**General**

- Type:  ☒ Enabled
- Ifindex:

**Auto In-Service**

- ☐ Enabled
- Timer:  days  hours  minutes

**OTU**

- FEC:
- Degraded Threshold Per Second:
- Seconds Degraded For Fault:
- Expected Trace:
- Tx Trace:

At the bottom right, there are 'Cancel' and 'Apply' buttons.

Figure 54: BT17800 Series Edit Interface (Optical Channel)

Edit Interface 7800:1/5/2/1/1.1

Settings Custom

**General**

Type:  ☒ Enabled

Ifindex:

**Auto In-Service**

☐ Enabled Timer:  days  hours  minutes

**OCH**

Grid:  Channel Name:

Wavelength:  nm Frequency:  THz

Fiber Port:  CPRWS:

Modulation:

Cancel Apply



**NOTE:** In order to view or edit an OTU4 tributary interface on a UFM6 line port, expand the OCH interface to show the OTU4 tributary interfaces on that OCH interface.

8. Edit the general interface attributes:

- **Type** This field can only be changed if you are changing between a multiplexed ODU2 sub-interface and a multiplexed ODU2e sub-interface on supported UFM6. Otherwise it is read-only.
- **Enabled** Select to enable the interface. Uncheck to disable the interface.
- **Ifindex** This is read-only.

9. Edit the auto in-service attributes:

- **Enabled** Enable or disable the auto in-service timer.
- **Timer** Edit the timer value.

10. Edit the protocol attributes. Protocol attributes vary depending on the protocol.

Table 27: OTU Protocol Attributes

Attribute	Description
FEC	Specify the type of Forward Error Correction (FEC) from the drop-down menu. For UFM6 OTU interfaces within an optical channel, the FEC is set within the optical channel (OCH) interface configuration.
Delta-Q	Specify the delta Q factor difference threshold (dB) between X and Y polarization states.  This attribute represents the threshold at which the Transmitter Degrade (transmitterDegrade) alarm is raised for OTU4 interfaces.
Degraded Threshold Per Second	Set the signal degrade threshold for a 1-second interval. When the percentage of errored blocks within a 1-second interval reaches this value, the interval is considered a degraded interval. The valid range is 1 to 100 (percent) inclusive.
Seconds Degraded For Fault	Set the signal degrade fault threshold. When the number of consecutive degraded 1-second intervals reaches this value, a signal degrade fault is raised. Valid values are 0 (no fault is raised) and 2 through 10 (seconds) inclusive.
Expected Trace	Specify the trace message that is expected to be received.
Tx Trace	This is the trace message that is to be transmitted. It cannot be changed.
Rx Trace	This is the trace message that has been received. It cannot be changed. This attribute is only available on some transceivers.

Table 28: ODU Protocol Attributes

Attribute	Description
Multiplex	Specify <b>GMP_CAPABLE</b> if you want the interface to be multiplexed, or specify <b>NO_MULTIPLEX</b> if you do not want multiplexing. For more information, see <a href="#">“Configuring a Multiplexed Interface” on page 211</a> .  This attribute can only be changed for ODU4 interfaces. For other ODU interfaces, this attribute is set to <b>NO_MULTIPLEX</b> and cannot be changed.

Table 29: SONET/SDH Protocol Attributes

Attribute	Description
Expected Trace	Specify the trace message that is expected to be received.
SD-THR	Set the signal degrade fault threshold. When the threshold is set to x, a signal degrade fault is raised when the bit error rate exceeds $10 \times 10^{-x}$ . Valid values are 0 (no fault is raised) and 3 through 11 inclusive.
Mapping	Specify either <b>ASYNCHRONOUS</b> or <b>BIT_SYNCHRONOUS</b> to indicate how the SONET/SDH signal maps into the ODU payload.

*Table 30: Ethernet Protocol Attributes*

Attribute	Description
-----------	-------------

There are no protocol attributes specific to Ethernet.

*Table 31: Fibre Channel Protocol Attributes*

Attribute	Description
-----------	-------------

There are no protocol attributes specific to fibre channel.

11. Edit the physical or OCH attributes.

Some of these attributes can only be configured if the interface is disabled. When changing an attribute that requires the interface to be disabled, follow these steps:

- Disable the interface by unchecking **Enabled** in the **General** attributes section.
- Change the desired attributes and click **Apply** to apply the changes to the network element.
- After the changes are reflected in PSM, edit the interface again, re-select **Enabled** in the **General** attributes section, and click **Apply**.

*Table 32: Physical Attributes*

Attribute	Description
<b>Grid</b>	Specify the grid spacing from the drop-down menu. The grid spacing can only be specified for tunable transceivers.  If you are editing an existing interface, you must disable the interface before you can change this attribute.
<b>Wavelength or Frequency</b>	Specify either the desired wavelength or the desired frequency. The wavelength or frequency can only be specified for tunable transceivers.  If you are editing an existing interface, you must disable the interface before you can change this attribute.
<b>Loopback</b>	Select the type of loopback, if any, from the drop-down menu. This attribute can only be set if the <b>Enabled</b> check box is unchecked in the <b>General</b> attributes section. If the <b>Enabled</b> check box is selected, this value automatically changes to <b>NO_LOOPBACK</b> .
<b>CPRWS</b>	Select the carrier phase recovery window size from the drop-down menu. This attribute is not applicable to all transceiver types.  If you are editing an existing interface, you must disable the interface before you can change this attribute.
<b>Laser Enabled</b>	Select to enable the transmit laser after provisioning. Uncheck to disable the transmit laser.

Table 32: Physical Attributes (continued)

Attribute	Description
<b>FPSD</b>	<p>Select to enable Fault Propagation Shutdown (FPSD). When a failure occurs and FPSD is enabled, the interface shuts down its laser instead of transmitting a maintenance signal.</p> <p>This attribute is only available for selection for Ethernet interfaces.</p>

Table 33: UFM6 Optical Channel (OCH) Attributes

Attribute	Description
<b>Grid</b>	<p>Specify the grid spacing from the drop-down menu.</p> <p>If you are editing an existing interface, you must disable the interface before you can change this attribute.</p>
<b>Channel Name or Wavelength or Frequency</b>	<p>Specify the channel, the desired wavelength, or the desired frequency. The channel number automatically determines the wavelength and frequency.</p> <p>If you are editing an existing interface, you must disable the interface before you can change this attribute.</p>
<b>Fiber Port</b>	<p>Select the fiber port (also known as the subport).</p> <p>This attribute can only be selected when adding an interface. You cannot change this attribute for an existing interface.</p>
<b>CPRWS</b>	<p>Select the carrier phase recovery window size from the drop-down menu.</p> <p>If you are editing an existing interface, you must disable the interface before you can change this attribute.</p>
<b>Modulation</b>	<p>Select either <b>16-qam</b> or <b>qpsk</b> modulation. If you select <b>16-qam</b>, the optical channel contains up to two OTU4 signals. If you select <b>qpsk</b>, the optical channel contains one OTU4 signal.</p> <p>This attribute can only be selected when adding an interface. You cannot change this attribute for an existing interface.</p> <p><b>NOTE:</b> In order to interwork with OTU4 signals on UFM3 and UFM4 line ports, you must configure the UFM6 optical channel for <b>qpsk</b> modulation.</p>
<b>Tx-Power</b>	Specify the transmit power.
<b>FEC</b>	<p>Specify the type of Forward Error Correction (FEC) from the drop-down menu.</p> <p>The line coding is automatically set based on the FEC setting. If you select <b>SDFEC_25</b>, the line coding is automatically set to non-differential. If you select <b>SDFEC</b>, the line coding is automatically set to differential.</p>

Table 33: UFM6 Optical Channel (OCH) Attributes (continued)

Attribute	Description
<b>Delta-Q</b>	<p>Specify the delta Q factor difference threshold (dB) between X and Y polarization states.</p> <p>This attribute represents the threshold at which the Transmitter Degrade (transmitterDegrade) alarm is raised for OCH interfaces.</p>

12. Optionally, select **LLDP snooping**. LLDP snooping allows the BTI7800 to snoop LLDP frames on an Ethernet interface to determine the identity of the attached device.

13. Optionally, configure PRBS (pseudorandom binary sequence) generation.

Set **PRBS Mode** to **NO\_PRBS** or **EGRESS** or **INGRESS** as desired. Not all options are supported for some protocols. This attribute can only be set to **EGRESS** or **INGRESS** if the **Enabled** check box is unchecked in the **General** attributes section.

14. Optionally, edit the **Custom** fields.

- Click the **Custom** tab. These fields are for operator use and are opaque to the system.
- In the **Custom** panel, edit the **Id**, **Custom 1**, **Custom 2**, and **Custom 3** settings as desired.

15. When you are finished, click **Apply**.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View > Server > Tasks** window. The new provisioning appears in PSM a short while after the task completes successfully.

### Configuring a Multiplexed Interface

Use this procedure to configure a multiplexed ODU interface on a UFM on a BTI7800 Series network element.

#### Prerequisites:

- The corresponding OTU interface is created.



**NOTE:** You do not need to create an ODU interface explicitly. An ODU interface is automatically created when you create the corresponding OTU interface.

Only some ODU interfaces can be configured for multiplexing.

1. Expand the network element in the Network tree to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.
3. Expand a UFM to show the BICs and/or ports in that UFM.



**NOTE:** Not all UFM's support BICs.

4. If you are adding an interface to a BIC, expand the BIC to show the ports for that BIC.
5. Expand a port to show the OTU interfaces for that port.
6. Expand an OTU interface to see the corresponding ODU interface.
7. Right-click the ODU interface and select **Interface > Edit**.

The **Edit Interface** dialog appears.

*Figure 55: BT17800 Series Edit Interface (ODU4)*

Settings

**General**

Type: odu4

Mode: transport

Ifindex: 1

**Auto In-Service**

☐ Enabled

Timer: 0 days 8 hours 0 minutes

**ODU**

Multiplex: NO\_MULTIPLEX

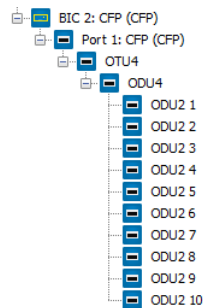
Cancel Apply



8. To specify that this ODU interface can be multiplexed into, select **GMP-CAPABLE** in the ODU **Multiplex** field.
9. When you are finished, click **Apply**.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View > Server > Tasks** window. The new provisioning appears in PSM a short while after the task completes successfully.

*Figure 56: ODU4 Interface with 10 ODU2 Sub-interfaces*



**NOTE:** If you want to change one or more of the automatically-created subinterfaces between an ODU2 and an ODU2e, then edit the subinterface and change the interface type. For more information, see [“Editing an Interface” on page 205](#)

### Cloning an Interface

Use this procedure to clone an existing interface on a UFM on a BT17800 Series network element.

1. Expand the network element in the Network tree to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.
3. Expand a UFM to show the BICs and/or ports in that UFM.

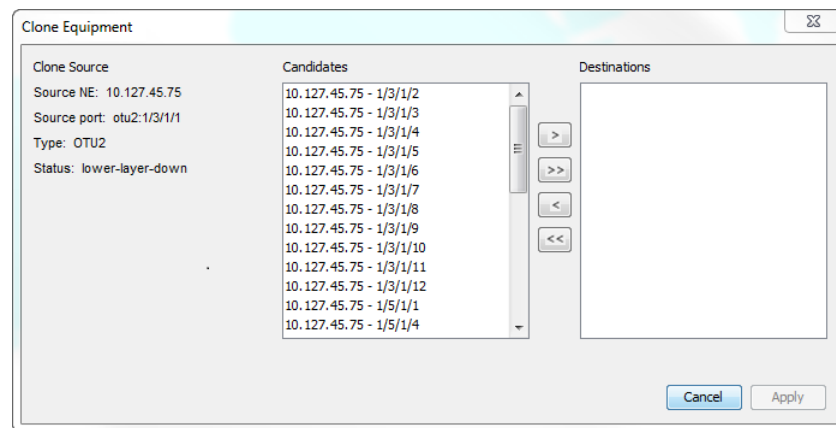


**NOTE:** Not all UFM's support BICs.

4. If you are adding an interface to a BIC, expand the BIC to show the ports for that BIC.
5. Expand a port to show the interfaces.
6. Right-click a provisioned interface and select **Interface > Clone**.

The **Clone Equipment** dialog appears:

Figure 57: BTI7800 Series Clone Equipment (interface)



The **Candidates** pane shows the list of possible destinations to which the source interface can be cloned. Only those destinations that are unprovisioned and compatible with the source interface are shown. To be compatible, the source and target interfaces must have the same BIC type and the same optical format (fixed/tunable).

7. From the list of **Candidates**, use the arrow buttons to move one or more interfaces to the **Destinations** pane.
8. When you are finished, click **Apply**.

The PSM server sends the configuration requests to the network element. You can monitor the status of the requests through the **View > Server > Tasks** window. The new provisioning appears in the Network tree view a short while after the tasks complete successfully.

### Deleting an Interface

Use this procedure to delete an interface on a UFM on a BTI7800 Series network element.

1. Expand the network element in the Network tree view to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.
3. Expand a UFM to show the BICs and/or ports in that UFM.



**NOTE:** Not all UFM's support BICs.

4. If you are deleting an interface on a BIC, expand the BIC to show the ports for that BIC.
5. Expand a port to show the interfaces for that port.



**NOTE:** In order to delete an OTU4 tributary interface on a UFM6 line port, expand the OCH interface to show the OTU4 tributary interfaces on that OCH interface.

6. Right-click a provisioned interface and select **Interface >Delete**.
7. Click **OK** in the **Delete Interface** confirmation dialog.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View >Server >Tasks** window. The new provisioning appears in the Network tree view a short while after the task completes successfully.

### Viewing Interface PMs on a UFM

Use this procedure to view current interface PMs on a UFM on a BTI7800 Series network element.

1. Expand the network element in the Network tree to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.
3. Expand a UFM to show the BICs and/or ports in that UFM.



**NOTE:** Not all UFM's support BICs.

4. If you are adding an interface to a BIC, expand the BIC to show the ports for that BIC.
5. Expand a port to show the interfaces.
6. Right-click a provisioned interface and select **Interface PMs >View**.

The **Interface Current PM** window appears:

OTU2-2/3/1/1 Tue 22 Apr 2014 17:33:02 EDT

PM Name	Value
OTU Error Blocks (OTU-EB)	0
OTU Background Block Errors (OTU-BBE)	0
OTU Error Seconds (OTU-ES)	27 seconds
OTU Severely Error Seconds (OTU-SES)	27 seconds
OTU Out of Frame Seconds (OTU-OFS)	27 seconds
OTU Bit Error Ratio (OTU-BER)	0
OTU Min. Bit Error Ratio (OTU-BER-MIN)	0
OTU Max. Bit Error Ratio (OTU-BER-MAX)	0
OTU Avg. Bit Error Ratio (OTU-BER-AVG)	0

The PMs are listed for the interface selected.



**NOTE:** This window shows a snapshot of the PM counts. The counts do not update automatically in this window. To see the latest counts, click the **Refresh** button.

7. To select what columns to display, right-click anywhere in the headings row to bring up a column selection window.  
Check or uncheck column headings as desired.
8. To sort the PMs based on column values, click on the column heading that you want to sort.
9. To export the PM data to a CSV file, click **Export** and save the file.

## Provisioning a ROADM Node on a BT17800

The following sections describe how to provision a ROADM node and how to perform other ROADM-related tasks on a BT17800.

- [General Provisioning Procedure on page 217](#)
- [Adding a ROADM or an ILA Module on page 218](#)
- [Editing a ROADM or an ILA Module on page 219](#)
- [Deleting a ROADM or an ILA Module on page 220](#)
- [Adding a PRE Module on page 220](#)
- [Editing a PRE Module on page 221](#)
- [Deleting a PRE Module on page 222](#)
- [Adding or Viewing a multiplexer/demultiplexer on page 222](#)
- [Deleting a multiplexer/demultiplexer on page 225](#)
- [Editing a Port on page 225](#)

- [Editing the OMS on page 226](#)
- [Editing the OSC on page 227](#)
- [Adding a Fiber Connection on a ROADM or an ILA Client Port on page 227](#)
- [Editing a Fiber Connection on a ROADM or an ILA Client Port on page 228](#)
- [Deleting a Fiber Connection on a ROADM or an ILA Client Port on page 229](#)
- [Adding a Fiber Connection on a ROADM or an ILA Line Port on page 230](#)
- [Editing a Fiber Connection on a ROADM or an ILA Line Port on page 231](#)
- [Deleting a Fiber Connection on a ROADM or an ILA Line Port on page 231](#)
- [Adding a Fiber Connection on a UFM Interface on page 232](#)
- [Editing a Fiber Connection on a UFM Interface on page 233](#)
- [Deleting a Fiber Connection on a UFM Interface on page 233](#)
- [Viewing Fiber Connections on page 234](#)
- [Adding an Optical Channel on page 234](#)
- [Bulk Adding Optical Channels on page 235](#)
- [Editing an Optical Channel on page 237](#)
- [Deleting an Optical Channel on page 238](#)
- [Viewing Port PMs on a ROADM Element on page 238](#)
- [Viewing OMS PMs on a ROADM Element on page 239](#)
- [Viewing OSC PMs on a ROADM Element on page 240](#)
- [Viewing Optical Channel PMs on a ROADM Element on page 240](#)

---

### General Provisioning Procedure

The procedure for provisioning a ROADM node can be summarized as follows:

1. Provision all required modules. This is covered in sections [“Adding a ROADM or an ILA Module” on page 218](#) through [“Editing the OSC” on page 227](#). It is usually not necessary for you to perform this step explicitly because the BT17800 automatically provisions modules when the modules are physically installed. This is called auto-provisioning.
2. Provision all required fiber connections. This is covered in sections [“Adding a Fiber Connection on a ROADM or an ILA Client Port” on page 227](#) through [“Viewing Fiber Connections” on page 234](#). Fiber connections represent the physical fiber connectivity within a ROADM node and across ROADM nodes. Auto-provisioning provisions fiber connections when the fibers are physically installed, so it is usually not necessary for you to perform this step explicitly either.
3. Provision the optical channels that make up the optical service. This is covered in sections [“Adding an Optical Channel” on page 234](#) through [“Deleting an Optical Channel” on page 238](#). An optical channel is a user-traffic-bearing bidirectional channel that is defined by its central frequency (wavelength) and bandwidth. It is cross-connected within the node as part of an overall optical service. Optical channels exist on both

ROADM module line ports and ROADM module client ports, but you only need to explicitly create optical channels on the ROADM module line ports.

4. Provision the optical channel cross-connects. This is part of service activation and is covered in [“Activating an Optical Service in a BT17800 Network” on page 319](#). When using PSM service activation, you just select the endpoints. PSM will create all the necessary cross-connects in the service path from end to end.

For information on auto-provisioning, see the *BT17800 Series Software Configuration Guide*.

---

### Adding a ROADM or an ILA Module

Use this procedure to add a new ROADM or ILA module on a BT17800 Series network element.

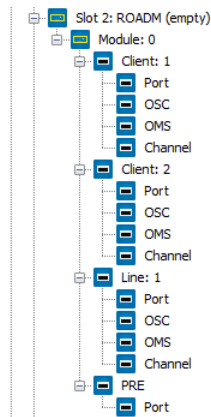
1. Expand the network element in the Network tree to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.
3. Right-click an unprovisioned slot and select **Slot >Provision** to add a module in that slot.

The **Provision Slot** dialog appears.

4. Configure the slot as follows:
  - **PEC** Select a ROADM or an ILA PEC from the list of available PECs in the drop-down menu.
  - **Admin Status** Specify the initial state of the module as **Up** or **Down** or **Testing**.
5. Optionally, specify the **Custom** fields. These fields are for operator use and are not used by the system.
  - a. Click the **Custom** tab.
  - b. In the **Custom** panel, specify the **Custom 1**, **Custom 2**, and **Custom 3** settings as desired.
6. When you are finished, click **OK**.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View >Server >Tasks** window. The new provisioning appears in the Network tree a short while after the task completes successfully.

The module is added along with its client, line, and PRE ports, and the respective OMS and OSC where applicable.



**NOTE:** The PRE module itself is not automatically added. To add the PRE module, see [“Adding a PRE Module” on page 220](#).

### Editing a ROADM or an ILA Module

Use this procedure to edit a ROADM or an ILA module on a BT17800 Series network element.

1. Expand the network element in the Network tree to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.
3. Right-click a ROADM or an ILA module and select **Slot >Edit**.

The **Edit Slot** dialog appears.

4. Configure the slot as follows:
  - **PEC** This is read only.
  - **Admin Status** Set the state of the module to **Up**, **Down**, or **Testing**.
5. Optionally, specify the **Custom** fields. These fields are for operator use and are not used by the system.
  - a. Click the **Custom** tab.
  - b. In the **Custom** panel, specify the **Custom 1**, **Custom 2**, and **Custom 3** settings as desired.
6. When you are finished, click **Apply**.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View >Server >Tasks** window. The new provisioning appears in PSM a short while after the task completes successfully.

### Deleting a ROADM or an ILA Module

---

Use this procedure to delete a ROADM or an ILA module on a BT17800.

1. Expand the network element in the Network tree to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.
3. Right-click a ROADM or ILA module and select **Slot >Delete**.
4. Click **OK** in the confirmation dialog.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View >Server >Tasks** window. The new provisioning appears in PSM a short while after the task completes successfully.

### Adding a PRE Module

---

Use this procedure to add a new PRE module to a ROADM or ILA on a BT17800 Series network element.

1. Expand the network element in the Network tree to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.
3. Right-click a ROADM or ILA module and select **Preamplifier >Provision** to add a PRE module to the ROADM or ILA.

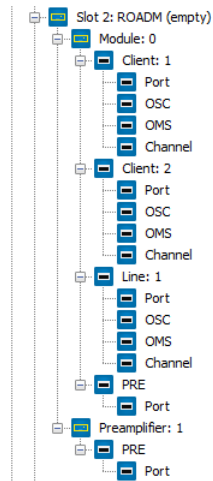
In the ensuing dialog, the **PEC** and **Oper Status** cannot be changed.

4. Optionally, specify the **Custom** fields. These fields are for operator use and are opaque to the system.
  - a. Click the **Custom** tab.
  - b. In the **Custom** panel, specify the **Custom 1**, **Custom 2**, and **Custom 3** settings as desired.
5. When you are finished, click **OK** to add the PRE module.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View >Server >Tasks** window. The new provisioning appears in the Network tree a short while after the task completes successfully.

The PRE module and its port are added.





### Editing a PRE Module

Use this procedure to edit a PRE module on a BTI7800 Series network element.

#### Prerequisites:

- The PRE module is created.
1. Expand the network element in the Network tree to show the shelves in that NE.
  2. Expand a shelf to show the slots in that shelf.
  3. Expand a ROADM or ILA module.

The main module is **Module: *index***, where the *index* is 0. The preamplifier module is **Preamplifier: *index***, where the *index* is 1.

4. Right-click the preamplifier and select **Preamplifier >Edit**.

In the ensuing dialog, the **PEC** and **Oper Status** cannot be changed.

5. Set the **Custom** fields as desired. These fields are for operator use and are opaque to the system.
  - a. Click the **Custom** tab.
  - b. In the **Custom** panel, specify the **Custom 1**, **Custom 2**, and **Custom 3** settings as desired.
6. When you are finished, click **Apply** to apply the changes.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View >Server >Tasks** window. The new provisioning appears in PSM a short while after the task completes successfully.

### Deleting a PRE Module

---

Use this procedure to delete a PRE module on a ROADM or ILA.

**Prerequisites:**

- The PRE module is created.
- 1. Expand the network element in the Network tree to show the shelves in that NE.
- 2. Expand a shelf to show the slots in that shelf.
- 3. Expand a ROADM or ILA module.

The main module is **Module:** *index*, where the *index* is 0. The preamplifier module is **Preamplifier:** *index*, where the *index* is 1.

- 4. Right-click the preamplifier and select **Preamplifier >Delete**.
- 5. Click **OK** in the confirmation dialog.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View >Server >Tasks** window. The new provisioning appears in PSM a short while after the task completes successfully.

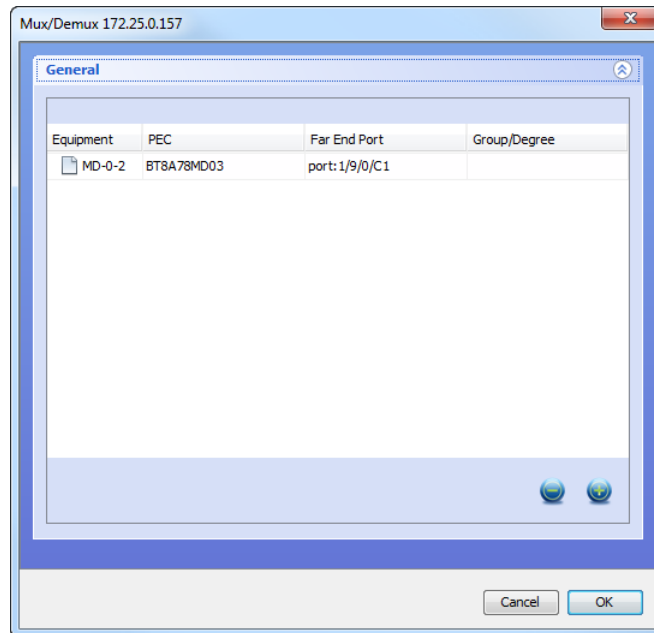
### Adding or Viewing a multiplexer/demultiplexer

---

Use this procedure to view existing multiplexer/demultiplexers or to add a new one on a BT17800 Series network element.

1. Right click a network element in the Network tree and select **Node >Passive >Mux/Demux >Edit**

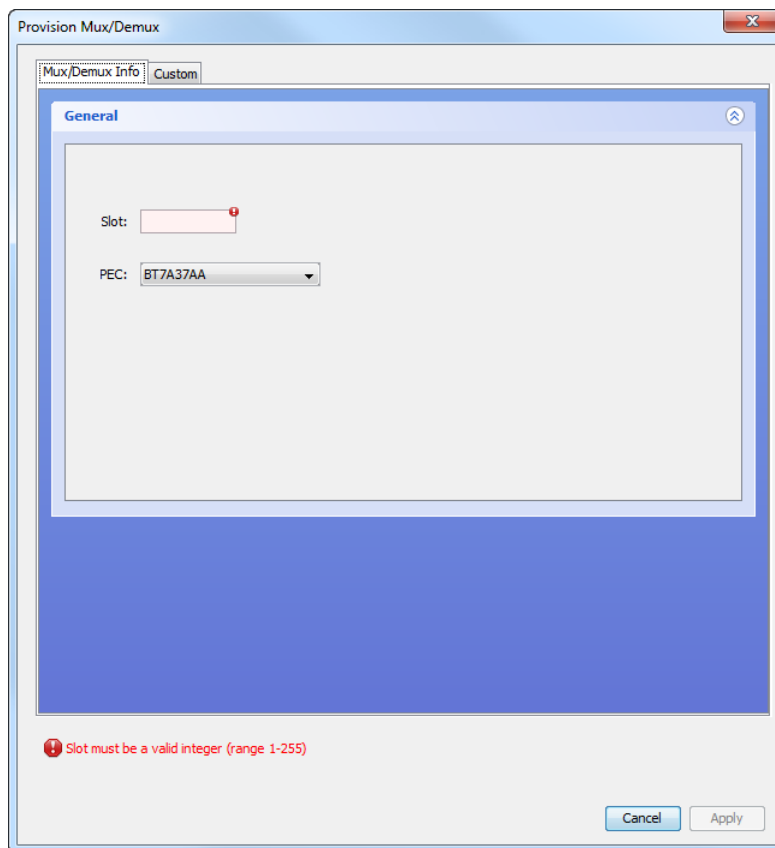
The **Mux/Demux** window appears. This window shows a listing of the existing multiplexer/demultiplexers on the shelf.



**NOTE:** The Group/Degree is not applicable to BT17800 ROADM nodes.

2. Click on the plus icon to add a new multiplexer/demultiplexer.

The **Provision Mux/Demux** window appears.



3. Specify the **Slot** for the multiplexer/demultiplexer.
4. Select a PEC from the list of available PECs.
5. Optionally, specify the **Custom** fields. These fields are for operator use and are opaque to the system.
  - a. Click the **Custom** tab.
  - b. In the **Custom** panel, specify the **Id**, **Custom 1**, **Custom 2**, and **Custom 3** settings as desired.
6. When you are finished, click **Apply**.

The newly added multiplexer/demultiplexer appears in the **Mux/Demux** window.

7. Click **OK**.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View > Server > Tasks** window. The new provisioning appears in PSM a short while after the task completes successfully.

### Deleting a multiplexer/demultiplexer

Use this procedure to delete a multiplexer/demultiplexer on a BT17000 Series network element.

1. Right click a network element in the Network tree and select **Node >Passive >Mux/Demux >Edit**

The **Mux/Demux** window appears.

2. Select a multiplexer/demultiplexer and click on the minus icon to delete it.

The selected multiplexer/demultiplexer disappears from the window.

3. Click **OK**.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View >Server >Tasks** window. The new provisioning appears in PSM a short while after the task completes successfully.

### Editing a Port

Use this procedure to edit a port on a ROADM, ILA, or PRE module on a BT17800 Series network element.

All ports on a module are automatically added when you add the module.

1. Expand the network element in the Network tree to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.
3. Expand a ROADM or ILA module.

The main module is **Module: *index***, where the *index* is **0**. The preamplifier module (if present) is **Preamplifier: *index***, where the *index* is **1**.

4. Expand the main module to see the ports on the main module, or expand the preamplifier to see the port on the PRE module.
5. Expand the desired client, line, or PRE port container, right-click **Port** and select **Optical Port >Edit**
6. Specify the **Id** and **Custom** fields as desired. These fields are for operator use and are opaque to the system.
7. When you are finished, click **Apply** to apply the changes.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View >Server >Tasks** window. The new provisioning appears in PSM a short while after the task completes successfully.

### Editing the OMS

---

Use this procedure to edit the Optical Multiplex Section (OMS) on a ROADM or an ILA client or line port on a BTI7800 Series network element.

1. Expand the network element in the Network tree to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.
3. Expand a ROADM or ILA module.

The main module is **Module: *index***, where the *index* is 0. The preamplifier module (if present) is **Preamplifier: *index***, where the *index* is 1.

4. Expand the main module to see the ports on the main module.
5. Expand the desired client or line port container to see the OMS for that port.
6. Right-click **OMS** and select **OMS >Edit**  
The **Edit OMS** dialog appears.
7. Configure the OMS as follows:
  - **Oper Status** The operational status is read only.
  - **Admin Status** Specify whether the OMS state is **In-Service** or **Out-Of-Service** or **Testing**.
  - **Preamplifier State** Specify whether the preamplifier is **Enabled** or **Disabled**. This is only applicable for line ports. Client ports do not have a preamplifier.
8. Optionally, specify the **Custom** fields. These fields are for operator use and are opaque to the system.
  - a. Click the **Custom** tab.
  - b. In the **Custom** panel, specify the **Id**, **Custom 1**, **Custom 2**, and **Custom 3** settings as desired.
9. When you are finished, click **Apply** to apply the changes.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View >Server >Tasks** window. The new provisioning appears in PSM a short while after the task completes successfully.

### Editing the OSC

Use this procedure to edit the Optical Service Channel (OSC) on a ROADM or an ILA client or line port on a BT17800 Series network element.

1. Expand the network element in the Network tree to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.
3. Expand a ROADM or ILA module.

The main module is **Module:** *index*, where the *index* is 0. The preamplifier module (if present) is **Preamplifier:** *index*, where the *index* is 1.

4. Expand the main module to see the ports on the main module.
5. Expand the desired client or line port container to see the OSC for that port.
6. Right-click **OSC** and select **OSC >Edit**  
The **Edit OSC** dialog appears.
7. Configure the OSC as follows:
  - **Oper Status** The operational status is read only.
  - **Admin Status** Specify whether the OSC state is **In-Service** or **Out-Of-Service**.
8. Optionally, specify the **Custom** fields. These fields are for operator use and are opaque to the system.
  - a. Click the **Custom** tab.
  - b. In the **Custom** panel, specify the **Id**, **Custom 1**, **Custom 2**, and **Custom 3** settings as desired.
9. When you are finished, click **Apply** to apply the changes.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View >Server >Tasks** window. The new provisioning appears in PSM a short while after the task completes successfully.

### Adding a Fiber Connection on a ROADM or an ILA Client Port

Use this procedure to add a fiber connection on a ROADM or an ILA client port on a BT17800 Series network element.

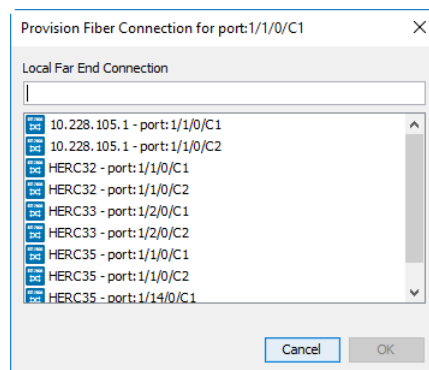
Fiber connections are mandatory. All fiber connections must exist before you can create an optical service.

1. Expand the network element in the Network tree to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.

3. Expand a ROADM or ILA module.

The main module is **Module: index**, where the *index* is 0. The preamplifier module (if present) is **Preamplifier: index**, where the *index* is 1.

4. Expand the main module to see the ports on the main module.
5. Right-click the desired client port container and select **Fiber Connection >Provision**.  
The Provision Fiber Connection dialog appears, listing all client ports in the network.



6. Select the other end of the fiber connection.  
For a ROADM client port, the other end can be a multiplexer/demultiplexer line port or another ROADM client port. To create a split ROADM node, configure a fiber connection between ROADM client ports on two different network elements.  
For an ILA client port, the other end can be another ILA client port.
7. When you are finished, click **OK** to create the fiber connection.  
The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View >Server >Tasks** window. The new provisioning appears in PSM a short while after the task completes successfully.

### Editing a Fiber Connection on a ROADM or an ILA Client Port

Use this procedure to edit a fiber connection on a ROADM or an ILA client port on a BT17800 Series network element.

1. Expand the network element in the Network tree to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.



- Expand a ROADM or ILA module.

The main module is **Module:** *index*, where the *index* is 0. The preamplifier module (if present) is **Preamplifier:** *index*, where the *index* is 1.

- Expand the main module to see the ports on the main module.
- Right-click the desired client port container and select **Fiber Connection >Edit**.
- Configure the fiber connection as follows:
  - **Port** The port at the other end of the fiber connection. This is read only.
  - **IP Address** The IP address of the NE at the other end of the fiber connection. For a regular ROADM node, this is the local IP address. For a split ROADM node, this is the IP address of the NE at the other end of the fiber.
  - **FE Monitoring** Check to enable far end monitoring. Uncheck to disable far end monitoring. When far end monitoring is enabled, the BT17800 checks to see if the configured fiber connection matches the actual physical fiber connection. If there is a mismatch, an alarm is raised.
  - **Fiber Type** This is not applicable to client ports.
- When you are finished, click **OK** to apply the changes.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View >Server >Tasks** window. The new provisioning appears in PSM a short while after the task completes successfully.

### Deleting a Fiber Connection on a ROADM or an ILA Client Port

Use this procedure to delete a fiber connection on a ROADM or an ILA client port on a BT17800 Series network element.

- Expand the network element in the Network tree to show the shelves in that NE.
- Expand a shelf to show the slots in that shelf.
- Expand a ROADM or ILA module.
 

The main module is **Module:** *index*, where the *index* is 0. The preamplifier module (if present) is **Preamplifier:** *index*, where the *index* is 1.
- Expand the main module to see the ports on the main module.
- Right-click the desired client port container and select **Fiber Connection >Delete**.
- Click **OK** in the confirmation dialog.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View > Server > Tasks** window. The new provisioning appears in PSM a short while after the task completes successfully.

### Adding a Fiber Connection on a ROADM or an ILA Line Port

Use this procedure to add a fiber connection on a ROADM or an ILA line port on a BT17800 Series network element.

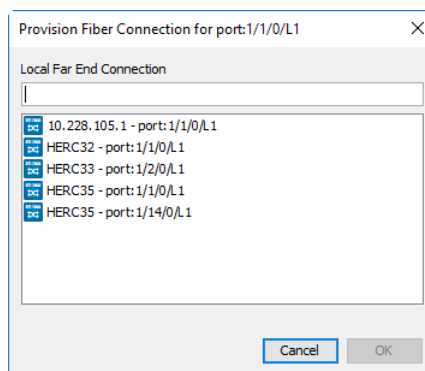
Fiber connections are mandatory. All fiber connections must exist before you can create an optical service.

1. Expand the network element in the Network tree to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.
3. Expand a ROADM or ILA module.

The main module is **Module: index**, where the *index* is **0**. The preamplifier module (if present) is **Preamplifier: index**, where the *index* is **1**.

4. Expand the main module to see the ports on the main module.
5. Right-click the line port container and select **Fiber Connection > Provision**.

The Provision Fiber Connection dialog appears, listing all line ports in the network.



6. Select the other end of the fiber connection.

For a ROADM line port, the other end can be a ROADM or ILA line port.

For an ILA line port, the other end can be a ROADM or ILA line port.

7. When you are finished, click **OK** to create the fiber connection.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View > Server > Tasks** window. The new provisioning appears in PSM a short while after the task completes successfully.

### Editing a Fiber Connection on a ROADM or an ILA Line Port

Use this procedure to edit a fiber connection on a ROADM or an ILA line port on a BT17800 Series network element.

1. Expand the network element in the Network tree to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.
3. Expand a ROADM or ILA module.

The main module is **Module:** *index*, where the *index* is 0. The preamplifier module (if present) is **Preamplifier:** *index*, where the *index* is 1.

4. Expand the main module to see the ports on the main module.
5. Right-click the line port container and select **Fiber Connection >Edit**.
6. Configure the fiber connection as follows:
  - **Port** The port at the other end of the fiber connection. This is read only.
  - **IP Address** The IP address of the NE at the other end of the fiber connection.
  - **FE Monitoring** Check to enable far end monitoring. Uncheck to disable far end monitoring. When far end monitoring is enabled, the BT17800 checks to see if the configured fiber connection matches the actual physical fiber connection. If there is a mismatch, an alarm is raised.
  - **Fiber Type** Select the fiber type from the pulldown menu.
7. When you are finished, click **OK** to apply the changes.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View >Server >Tasks** window. The new provisioning appears in PSM a short while after the task completes successfully.

### Deleting a Fiber Connection on a ROADM or an ILA Line Port

Use this procedure to delete a fiber connection on a ROADM or an ILA line port on a BT17800 Series network element.

1. Expand the network element in the Network tree to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.
3. Expand a ROADM or ILA module.

The main module is **Module:** *index*, where the *index* is 0. The preamplifier module (if present) is **Preamplifier:** *index*, where the *index* is 1.

- Expand the main module to see the ports on the main module.
- Right-click the line port container and select **Fiber Connection >Delete**.
- Click **OK** in the confirmation dialog.

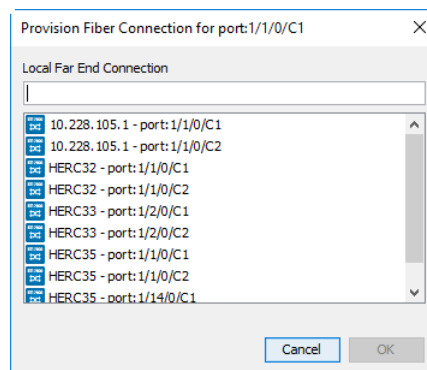
The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View >Server >Tasks** window. The new provisioning appears in PSM a short while after the task completes successfully.

### Adding a Fiber Connection on a UFM Interface

Use this procedure to add a fiber connection on a UFM interface on a BTI7800 Series network element.

- Expand the network element in the Network tree to show the shelves in that NE.
- Expand a shelf to show the slots in that shelf.
- Expand a UFM to see the BICs on the UFM.
- Expand a BIC to see the ports on the BIC.
- Expand a port to see the interface on the port.
- Right-click an interface and select **Fiber Connection >Provision**.

The Fiber Connection dialog appears.



- From the pulldown menu, select the other end of the fiber connection.

The other end should be a multiplexer/demultiplexer client port at the same frequency as the interface.

- When you are finished, click **OK** to create the fiber connection.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View > Server > Tasks** window. The new provisioning appears in PSM a short while after the task completes successfully.

---

### Editing a Fiber Connection on a UFM Interface

Use this procedure to edit a fiber connection on a UFM interface on a BTI7800 Series network element.

1. Expand the network element in the Network tree to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.
3. Expand a UFM to see the BICs on the UFM.
4. Expand a BIC to see the ports on the BIC.
5. Expand a port to see the interface on the port.
6. Right-click an interface and select **Fiber Connection > Edit**.
7. Configure the fiber connection as follows:
  - **Port** The port at the other end of the fiber connection. This is read only.
  - **IP Address** The IP address of the NE at the other end of the fiber connection. For a UFM interface, this is the local IP address since the other end is on the same node.
  - **FE Monitoring** Check to enable far end monitoring. Uncheck to disable far end monitoring. When far end monitoring is enabled, the BTI7800 checks to see if the configured fiber connection matches the actual physical fiber connection. If there is a mismatch, an alarm is raised.
  - **Fiber Type** This is not applicable to UFM interfaces.
8. When you are finished, click **OK** to apply the changes.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View > Server > Tasks** window. The new provisioning appears in PSM a short while after the task completes successfully.

---

### Deleting a Fiber Connection on a UFM Interface

Use this procedure to delete a fiber connection on a UFM interface on a BTI7800 Series network element.

1. Expand the network element in the Network tree to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.

3. Expand a UFM to see the BICs on the UFM.
4. Expand a BIC to see the ports on the BIC.
5. Expand a port to see the interface on the port.
6. Right-click an interface and select **Fiber Connection > Delete**.
7. Click **OK** in the confirmation dialog.

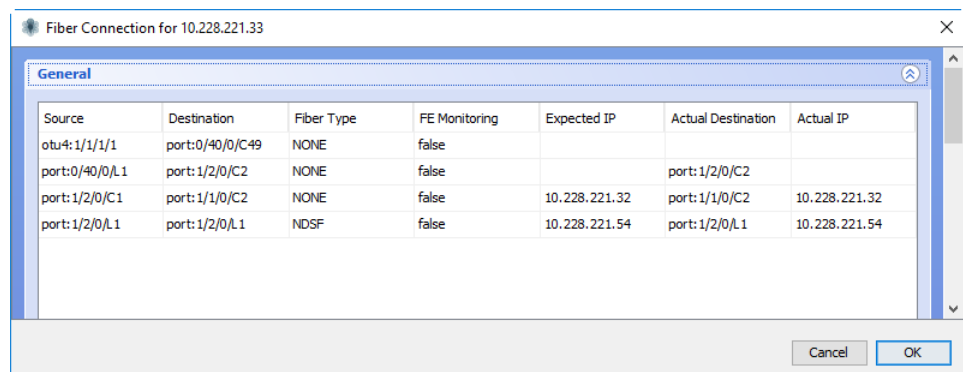
The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View > Server > Tasks** window. The new provisioning appears in PSM a short while after the task completes successfully.

### Viewing Fiber Connections

Use this procedure to view all fiber connections on a network element.

1. Right-click a network element in the Network tree or in the Topology Map view and select **Node > Fiber Connection > View**.

The **Fiber Connection** window appears:



2. Click **OK** to close the window.

### Adding an Optical Channel

Use this procedure to add an optical channel on a ROADM line port on a BTI7800 Series network element.

You only add optical channels to line ports. Optical channels on client ports are automatically added when you create and activate an optical service.

1. Expand the network element in the Network tree to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.

3. Expand a ROADM module.

The main module is **Module: *index***, where the *index* is **0**. The preamplifier module (if present) is **Preamplifier: *index***, where the *index* is **1**.

4. Expand the main module to see the ports on the main module.

5. Expand the line port container.

6. Right-click **Channel** and select **Provision >Single**

The **och** dialog appears.

7. Configure the optical channel as follows:

- **ID** Specify the channel identifier. This must be unique for the port.
- **Bandwidth** Specify the bandwidth of the channel. This is the grid spacing.
- **Channel Name** Specify the channel name. When this field is changed, **Frequency** and **Wavelength** are automatically changed to be consistent with this value.
- **Wavelength** Specify the central wavelength of the channel. When this field is changed, **Frequency** and **Channel Name** are automatically changed to be consistent with this value.
- **Frequency** Specify the central frequency of the channel. When this field is changed, **Channel Name** and **Wavelength** are automatically changed to be consistent with this value.
- **Enable** Check to enable the ODCC. Uncheck to disable the ODCC.
- **Admin Status** Specify whether the optical channel state is **In-Service** or **Out-Of-Service** or **Testing**.
- **Oper Status** The operational status is read only.

8. Optionally, specify the **Custom** fields. These fields are for operator use and are opaque to the system.

- a. Click the **Custom** tab.

- b. In the **Custom** panel, specify the **Id**, **Custom 1**, **Custom 2**, and **Custom 3** settings as desired.

9. When you are finished, click **Apply** to apply the changes.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View >Server >Tasks** window. The new provisioning appears in PSM a short while after the task completes successfully.

### Bulk Adding Optical Channels

Use this procedure to add optical channels in bulk on a ROADM line port on a BT17800 Series network element.

When you use this method to create optical channels, PSM automatically sets the Channel ID for the created optical channels to the Channel Name, which is derived from the frequency that you specify. Additionally, PSM sets the **Admin Status** of the created optical channels to **In-Service**.

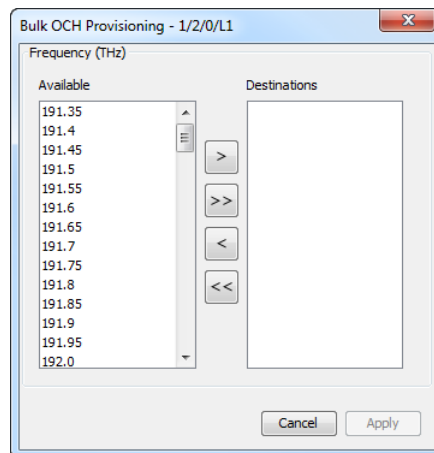
If you want to set a different **Channel ID** or **Admin Status**, then you should not use this method to create optical channels.

1. Expand the network element in the Network tree to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.
3. Expand a ROADM module.

The main module is **Module: *index***, where the *index* is **0**. The preamplifier module (if present) is **Preamplifier: *index***, where the *index* is **1**.

4. Expand the main module to see the ports on the main module.
5. Expand the line port container.
6. Right-click **Channel** and select **Provision > Bulk**

The **Bulk OCH Provisioning** dialog appears.



7. Select from the Available frequencies list and move to the Destinations list.

You can select one, multiple, or all frequencies.

8. When you are finished, click **Apply** to create the optical channels.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View > Server > Tasks** window. The new provisioning appears in PSM a short while after the task completes successfully.



### Editing an Optical Channel

---

Use this procedure to edit an optical channel on a ROADM line port on a BTI7800 Series network element.

1. Expand the network element in the Network tree to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.
3. Expand a ROADM module.

The main module is **Module:** *index*, where the *index* is 0. The preamplifier module (if present) is **Preamplifier:** *index*, where the *index* is 1.

4. Expand the main module to see the ports on the main module.
5. Expand the line port container.
6. Expand **Channel** to see the channels.
7. Right-click a channel and select **Channel >Edit**
8. Configure the optical channel as follows:
  - **ID** This is read only.
  - **Bandwidth** This is read only.
  - **Channel Name** This is read only.
  - **Wavelength** This is read only.
  - **Frequency** This is read only.
  - **Enable** Check to enable the ODCC. Uncheck to disable the ODCC.
  - **Admin Status** Specify whether the optical channel state is **In-Service** or **Out-Of-Service** or **Testing**.
  - **Oper Status** This is read only.
9. Optionally, specify the **Custom** fields. These fields are for operator use and are opaque to the system.
  - a. Click the **Custom** tab.
  - b. In the **Custom** panel, specify the **Id**, **Custom 1**, **Custom 2**, and **Custom 3** settings as desired.
10. When you are finished, click **Apply** to apply the changes.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View >Server >Tasks** window. The new provisioning appears in PSM a short while after the task completes successfully.

### Deleting an Optical Channel

---

Use this procedure to delete an optical channel on a ROADM line port on a BT17800 Series network element.

Optical channels that are part of an existing service cannot be deleted.

1. Expand the network element in the Network tree to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.
3. Expand a ROADM module.

The main module is **Module:** *index*, where the *index* is **0**. The preamplifier module (if present) is **Preamplifier:** *index*, where the *index* is **1**.

4. Expand the main module to see the ports on the main module.
5. Expand the line port container.
6. Expand **Channel** to see the channels.
7. Right-click a channel and select **Channel >Delete**
8. Click **OK** in the confirmation dialog.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View >Server >Tasks** window. The new provisioning appears in PSM a short while after the task completes successfully.

### Viewing Port PMs on a ROADM Element

---

Use this procedure to view PMs on a ROADM, ILA, or PRE port on a BT17800 Series network element.

1. Expand the network element in the Network tree to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.
3. Expand a ROADM or ILA module.

The main module is **Module:** *index*, where the *index* is **0**. The preamplifier module (if present) is **Preamplifier:** *index*, where the *index* is **1**.

4. Expand the main module to see the ports on the main module, or expand the preamplifier module to see the port on the PRE module.
5. Expand the desired client, line, or PRE port container, right-click **Port** and select **Optical Port PMs >View**  
A snapshot of the current PMs is displayed.
6. To refresh the counters, click **Refresh**.
7. To select what columns to display, right-click anywhere in the headings row to bring up a column selection window.  
Check or uncheck column headings as desired.
8. To sort the PMs based on column values, click on the column heading that you want to sort.
9. To save the counters to a CSV file, click **Export**.

#### Viewing OMS PMs on a ROADM Element

Use this procedure to view Optical Multiplexing Section (OMS) PMs on a ROADM or an ILA client or line port on a BT17800 Series network element.

1. Expand the network element in the Network tree to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.
3. Expand a ROADM or ILA module.  
The main module is **Module: *index***, where the *index* is 0. The preamplifier module (if present) is **Preamplifier: *index***, where the *index* is 1.
4. Expand the main module to see the ports on the main module.
5. Expand the desired client or line port container to see the OMS for that port.
6. Right-click **OMS** and select **OMS PMs >View**.  
A snapshot of the current PMs is displayed.
7. To refresh the counters, click **Refresh**.
8. To select what columns to display, right-click anywhere in the headings row to bring up a column selection window.

Check or uncheck column headings as desired.

9. To sort the PMs based on column values, click on the column heading that you want to sort.
10. To save the counters to a CSV file, click **Export**.

---

### Viewing OSC PMs on a ROADM Element

Use this procedure to view Optical Service Channel (OSC) PMs on a ROADM or an ILA client or line port on a BTI7800 Series network element.

1. Expand the network element in the Network tree to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.
3. Expand a ROADM or ILA module.

The main module is **Module:** *index*, where the *index* is 0. The preamplifier module (if present) is **Preamplifier:** *index*, where the *index* is 1.

4. Expand the main module to see the ports on the main module.
5. Expand the desired client or line port container to see the OSC for that port.
6. Right-click **OSC** and select **OSC PMs >View**.  
A snapshot of the current PMs is displayed.
7. To refresh the counters, click **Refresh**.
8. To select what columns to display, right-click anywhere in the headings row to bring up a column selection window.  
Check or uncheck column headings as desired.
9. To sort the PMs based on column values, click on the column heading that you want to sort.
10. To save the counters to a CSV file, click **Export**.

---

### Viewing Optical Channel PMs on a ROADM Element

Use this procedure to view optical channel PMs on a ROADM line port on a BTI7800 Series network element.

1. Expand the network element in the Network tree to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.
3. Expand a ROADM module.  
The main module is **Module: *index***, where the *index* is **0**. The preamplifier module (if present) is **Preamplifier: *index***, where the *index* is **1**.
4. Expand the main module to see the ports on the main module.
5. Expand line port container.
6. Expand **Channel** to see the channels.
7. Right-click a channel and select **Channel PMs >View**  
A snapshot of the current PMs is displayed.
8. To refresh the counters, click **Refresh**.
9. To select what columns to display, right-click anywhere in the headings row to bring up a column selection window.  
Check or uncheck column headings as desired.
10. To sort the PMs based on column values, click on the column heading that you want to sort.
11. To save the counters to a CSV file, click **Export**.

## Provisioning a 96-Channel Amplifier on a BTI7800

The BTI7800 96-Channel Amplifier is provisioned as follows:

1. Add the amplifier module.
2. Create an optical group for the amplifier if the desired optical group does not already exist.
3. Assign the amplifier to the optical group.
4. Edit the amplifier's port, WDM and OSC settings .

### Adding an Amplifier

Use this procedure to add a 96-Channel Amplifier on a BTI7800 Series network element.

1. Expand the network element in the Network tree to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.
3. Right-click an unprovisioned slot and select **Slot >Provision** to add a module in that slot.

The **Provision Slot** dialog appears. This dialog might change depending on the PEC that you select in the next step.

4. Configure the slot as follows:
  - **PEC** Select the 96-Channel Amplifier PEC from the list of available PECs in the drop-down menu.
  - **Admin Status** Specify whether the initial state of the module is **Up** or **Down** or **Testing**.
5. Optionally, specify the **Custom** fields. These fields are for operator use and are opaque to the system.
  - a. Click the **Custom Settings** tab.
  - b. In the **Custom Settings** panel, specify the **Id**, **Custom 1**, **Custom 2**, and **Custom 3** settings as desired.
6. When you are finished, click **OK**.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View >Server >Tasks** window. The new provisioning appears in the Network tree a short while after the task completes successfully.

You can now assign this amplifier to an existing optical group or create a new optical group for this amplifier.

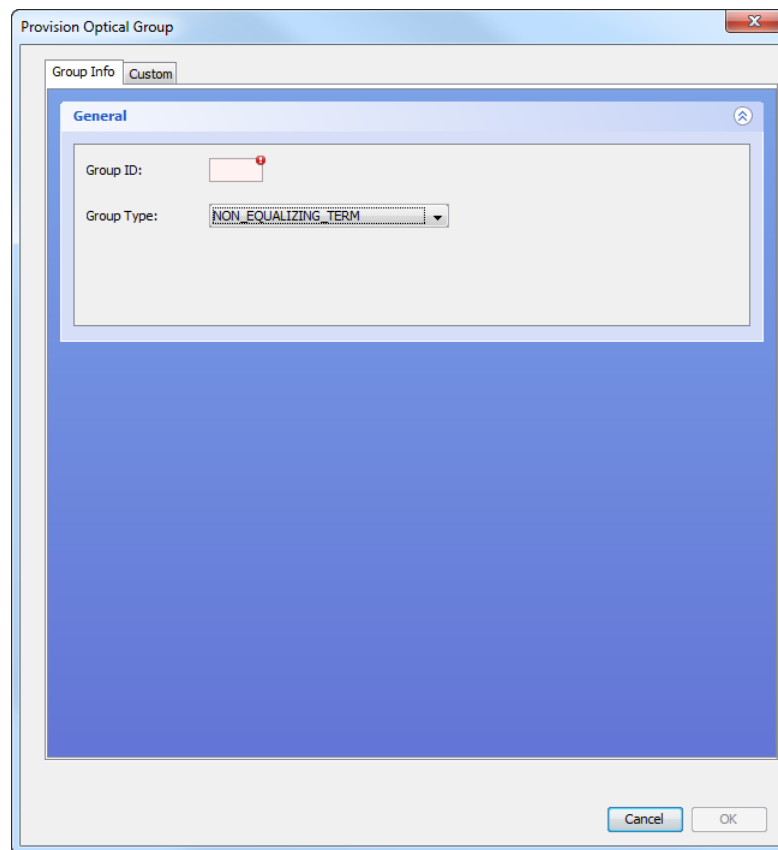
#### Creating an Optical Group for a BTI7800 Series Amplifier

Use this procedure to create an optical group for a 96-Channel Amplifier on a BTI7800 Series network element.

1. Expand the network element in the Network tree to show the shelves in that NE.
2. Right-click on **Optical Groups** and select **Group/Degree >Provision**.

The **Provision Optical Group** dialog appears:

Figure 58: Provision Optical Group



3. Configure the group as follows:
  - **Group ID** Specify the Group ID to distinguish the new group from the other optical groups on the node.
  - **Group Type** Specify the function for the group from the drop-down menu. The only group type supported for the BT17800 is **NON\_EQUALIZING\_TERM**.
4. Optionally, specify the **Custom** fields. These fields are for operator use and are opaque to the system.
  - a. Click the **Custom Settings** tab.
  - b. In the **Custom Settings** panel, specify the **Id**, **Custom 1**, **Custom 2**, and **Custom 3** settings as desired.
5. When you are finished, click **OK**.

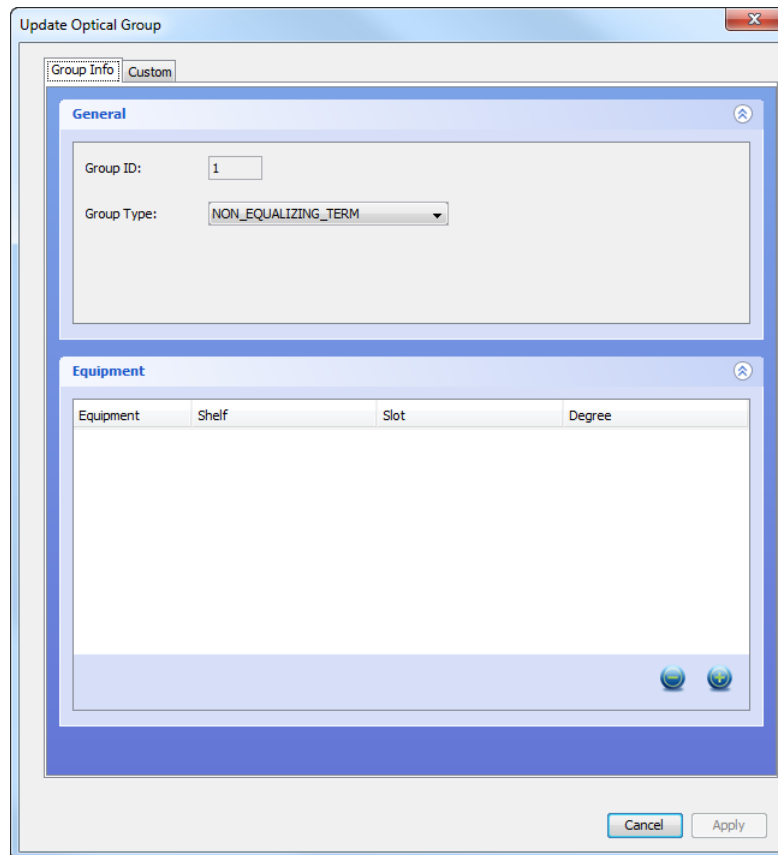
The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View > Server > Tasks** window. The new optical group appears in the Network tree a short while after the task completes successfully.

### Assigning or Unassigning an Amplifier

Use this procedure to assign a 96-Channel Amplifier to an optical group or to unassign a 96-Channel Amplifier from an optical group on a BTI7800 Series network element.

1. Expand the network element in the Network tree.
2. Expand the **Optical Groups** to see the optical groups on that NE.
3. Right-click the optical group in which you want to assign the amplifier, and select **Group/Degree >Edit**.

The **Update Optical Group** dialog appears.



The **Group ID** is set during optical group creation, and cannot be edited. The **Group Type** must be set to **NON\_EQUALIZING\_TERM**.

4. Assign or unassign amplifiers from the group.
  - To assign an amplifier to the group, click on the plus icon. This brings you to the **Assign Optical Equipment** window where you can assign an amplifier. Click **Apply** when you are done. The newly assigned amplifier appears in the Equipment list.



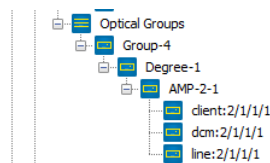
- To unassign an amplifier, select the amplifier from the list and then click on the minus icon. The unassigned amplifier is removed from the Equipment list.
5. Configure the **Custom** fields. These fields are for operator use and are opaque to the system.
    - a. Click the **Custom Settings** tab.
    - b. In the **Custom Settings** panel, edit the **Id**, **Custom 1**, **Custom 2**, and **Custom 3** settings as desired.
  6. When you are finished, click **Apply**.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View > Server > Tasks** window. The changes appear in PSM a short while after the task completes successfully.

### Editing an Amplifier Port

Use this procedure to edit an amplifier port on a 96-Channel Amplifier on a BT17800 Series network element.

1. Expand the network element in the Network tree view to show the shelves in that NE.
2. Expand **Optical Groups** to show the optical groups in that NE.
3. Expand an optical group to show the degree in that group.
4. Expand a degree to show the amplifier associated with that degree.



5. Expand an amplifier to show the ports on that amplifier.
6. Right-click a port and select **Optical Port > Edit**.  
The **Edit Optical Layer Port** dialog appears.
7. Configure the optical port parameters as follows:
  - **State** This is the operational state. It is read-only.
  - **DWDM Type** This is the type of DWDM composite signal expected on the port. It is set to **native**. This is read-only.
  - **Grid Type** This is the DWDM grid spacing for the port. If the equipment only supports a specific grid spacing, then this field is read-only.
  - **Tx Loss** Specify the optical loss in the transmit direction. Set to 0 for no loss.

- **AINS Timer** Optionally, specify the auto-in-service timer.
  - **Active Countdown** This is the countdown for the AINS timer. It is read-only.
8. Optionally, configure the **Custom** fields. These fields are for operator use and are opaque to the system.
    - a. Click the **Custom Settings** tab.
    - b. In the **Custom Settings** panel, edit the **Id**, **Custom 1**, **Custom 2**, and **Custom 3** settings as desired.
  9. When you are finished, click **Apply**.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View > Server > Tasks** window. The changes appear in PSM a short while after the task completes successfully.

---

### Editing WDM Parameters for an Amplifier

Use this procedure to edit WDM parameters on the line port of a 96-Channel Amplifier on a BTI7800 Series network element.

1. Expand the network element in the Network tree.
2. Expand **Optical Groups** to see the optical groups on that NE.
3. Expand an optical group to see the degree in that group.
4. Expand the degree to see the amplifier in that degree.
5. Right-click the amplifier and select **WDM > Edit**.

The **Edit WDM** dialog appears.

Figure 59: Edit WDM Dialog for a BT17800 96-Channel Amplifier Module

WDM Info Custom

**General**

Admin Status: In-Service Oper Status: lower-layer-down

Fiber Type: SSMF

Span

Loss Rx High Threshold: 0.0 Length:

Amp Tilt Trim: 0.0 Post Amp Gain: 4.0

Cancel Apply

6. Configure the WDM parameters as follows:
  - **Admin Status** Select the state from the list of available states in the drop-down menu.
  - **Oper Status** This is the operational state. It is read-only.
  - **Fiber Type** Specify the fiber type from the list of available fiber types in the drop-down menu.
  - **Loss Rx High Threshold** Specify the span loss threshold beyond which an alarm is raised. Set to 0 to disable.
  - **Length** The span length is measured automatically. This is read-only.
  - **Amp Tilt Trim** Set to fine tune the system gain tilt.
  - **Post Amp Gain** Set the system gain.
7. Configure the **Custom** fields. These fields are for operator use and are opaque to the system.
  - a. Click the **Custom Settings** tab.

- b. In the **Custom Settings** panel, edit the **Id**, **Custom 1**, **Custom 2**, and **Custom 3** settings as desired.
8. When you are finished, click **Apply**.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View > Server > Tasks** window. The changes appear in PSM a short while after the task completes successfully.

---

### Editing OSC Parameters for an Amplifier

Use this procedure to edit OSC parameters on the line port of a 96-Channel Amplifier on a BT17800 Series network element. The optical service channel (OSC) is used as a communications medium for control information between amplifiers at both ends of a line span.

1. Expand the network element in the Network tree.
2. Expand the **Optical Groups** to see the optical groups on that NE.
3. Expand an optical group to see the degree in that group.
4. Expand the degree to see the amplifier in that degree.
5. Right-click the amplifier and select **OSC > Edit**.

The **Edit OSC** dialog appears.

Figure 60: Edit OSC Dialog for a BT17800 96-Channel Amplifier Module

OSC Info Custom

**General**

Admin Status: In-Service Oper Status: lower-layer-down

☐ FE IM Mon

Expected Far End

System Name: IP Address: 0.0.0.0

Group: 0 Degree: 0

Actual Far End

System Name: IP Address:

Group: Degree:

Group Type: none

Cancel Apply

6. Configure the OSC parameters as follows:

- **Admin Status** Select the state from the list of available states in the drop-down menu.
- **Oper Status** This is the operational state. It is read-only.
- **FE IM Mon** Select if you want the near end to validate the identity of the far end with the expected far end parameters. If the identity does not match, the system will raise an alarm or condition.
- **System Name (expected)** Set to the expected system name of the far end.
- **IP Address (expected)** Set to the expected management IP address of the far end.
- **Group (expected)** Set to the expected optical group identifier of the far end.
- **Degree (expected)** Set to the expected optical degree of the far end.
- **System Name (actual)** This is the actual system name of the far end. It is read-only.
- **IP Address (actual)** This is the actual management IP address of the far end. It is read-only.
- **Group (actual)** This is the actual optical group identifier of the far end. It is read-only.

- **Degree (actual)** This is the actual optical degree of the far end. It is read-only.
  - **Group Type (actual)**- This is the actual group type of the far end. It is read-only.
7. Optionally, configure the **Custom** fields. These fields are for operator use and are opaque to the system.
    - a. Click the **Custom Settings** tab.
    - b. In the **Custom Settings** panel, edit the **Id**, **Custom 1**, **Custom 2**, and **Custom 3** settings as desired.
  8. When you are finished, click **Apply**.

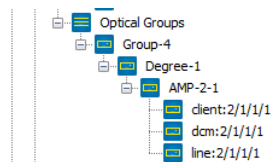
The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View > Server > Tasks** window. The changes appear in PSM a short while after the task completes successfully.

### Changing an Amplifier's Group

---

Use this procedure to change an amplifier's group on a BTI7800 Series network element.

1. Expand the network element in the Network tree view to show the shelves in that NE.
2. Expand **Optical Groups** to show the optical groups in that NE.
3. Expand an optical group to show the degrees in that group.
4. Expand a degree to show the amplifier associated with that degree.



5. Right-click an amplifier and select **Equipment > Edit**.

The **Change Group/Degree** dialog appears.

6. Edit the **Group**.

The **Degree** must be 1 and cannot be changed.

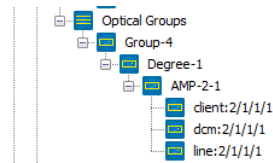
7. When you are finished, click **Apply**.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View > Server > Tasks** window. The changes appear in PSM a short while after the task completes successfully.

### Viewing Port PMs on a 96-Channel Amplifier

Use this procedure to view the port PMs on a 96-Channel Amplifier on a BTI7800 Series network element.

1. Expand the network element in the Network tree view to show the shelves in that NE.
2. Expand **Optical Groups** to show the optical groups in that NE.
3. Expand an optical group to show the degree in that group.
4. Expand a degree to show the amplifier associated with that degree.



5. Expand an amplifier to show the ports on that amplifier.
6. Right-click a port and select **Optical Port PMs >View**.  
A snapshot of the current PMs is displayed.
7. To refresh the counters, click **Refresh**.
8. To select what columns to display, right-click anywhere in the headings row to bring up a column selection window.  
Check or uncheck column headings as desired.
9. To sort the PMs based on column values, click on the column heading that you want to sort.
10. To save the counters to a CSV file, click **Export**.

## Provisioning a Wavelength Protection Switch Module on a BTI7800

### Adding a WPS Module

Use this procedure to add a new Wavelength Protection Switch (WPS) module on a BTI7800 Series network element.

1. Expand the network element in the Network tree to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.

3. Right-click an unprovisioned slot and select **Slot >Provision** to add a module in that slot.

The **Provision Slot** dialog appears. This dialog might change depending on the PEC that you select in the next step.

4. Configure the slot as follows:
  - **PEC** Select the WPS PEC from the list of available PECs in the drop-down menu.
  - **Admin Status** Specify whether the initial state of the module is **Up** or **Down** or **Testing**.
5. Optionally, specify the **Custom** fields. These fields are for operator use and are opaque to the system.
  - a. Click the **Custom Settings** tab.
  - b. In the **Custom Settings** panel, specify the **Custom 1**, **Custom 2**, and **Custom 3** settings as desired.
6. When you are finished, click **OK**.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View >Server >Tasks** window. The new provisioning appears in the Network tree a short while after the task completes successfully.

7. After the new WPS module appears in the Network tree, add a WPS protection group by following the steps in [“Adding a Protection Group” on page 252](#).

Protection ports are automatically added to the WPS group.

8. Configure protection port settings by following the steps in [“Editing a Port” on page 255](#).

---

### Adding a Protection Group

Use this procedure to add a WPS protection group on a BTI7800 Series network element.

When you add a protection group, the client and line ports are automatically added.

1. Expand the network element in the Network tree to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.
3. Right click a WPS module and select **Protection Groups >Provision** to add a protection group on the selected WPS module.

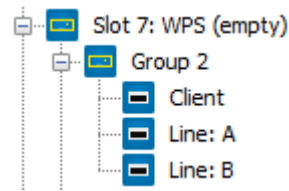
The **Provision Wavelength Protection Group** dialog appears:



The screenshot shows a window titled "Provision Wavelength Protection Group". Inside the window is a sub-section titled "Protection Group" with a blue header. Below this header, there are four input fields: "Group Id" (a dropdown menu with "1" selected), "Revertive-Type" (a dropdown menu with "NON\_REVERTIVE" selected), "Remote Id" (a text input field), and "Prot Id" (a text input field). Below these fields is a "Custom" section with a large text input area. At the bottom right of the window are "Cancel" and "OK" buttons.

4. Configure the protection group as follows:
  - **Group Id** - Select the protection group identifier from the drop-down menu. Only available identifiers are listed.
  - **Revertive-Type** - Select **NON\_REVERTIVE** or **REVERTIVE** from the drop-down menu.
  - **Remote Id** - This field is for operator use and is opaque to the system. PSM does not use this field for topology.
  - **Prot Id** - This is an alternative name for the protection group, and is opaque to the system.
  - **Custom** - This field is for operator use and is opaque to the system.
5. When you are finished, click **OK**.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View > Server > Tasks** window. The new provisioning appears in the Network tree a short while after the task completes successfully. For example:



### Editing a Protection Group

Use this procedure to edit a WPS protection group on a BTI7800 Series network element.

1. Expand the network element in the Network tree to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.
3. Expand a WPS module to show the protection groups on that module.
4. Right click a protection group and select **Group >Edit**.

The **Edit Wavelength Protection Group** dialog appears:

The dialog box is titled 'Edit Wavelength Protection Group wpsgroup:1/7/1'. It has a blue header bar with the title and a close button. Below the header is a section titled 'Protection Group'. Inside this section are four input fields: 'Group Id:' with a dropdown menu showing '1', 'Revertive-Type:' with a dropdown menu showing 'NON\_REVERTIVE', 'Remote Id:' with a text box, and 'Prot Id:' with a text box. Below these is a 'Custom:' section with a large text area. At the bottom right of the dialog are 'Cancel' and 'OK' buttons.

5. Edit the protection group as follows:

- **Group Id** - This is the protection group identifier. It cannot be changed.
  - **Revertive-Type** - Select **NON\_REVERTIVE** or **REVERTIVE** from the drop-down menu.
  - **Remote Id** - This field is for operator use and is opaque to the system. PSM does not use this field for topology.
  - **Prot Id** - This is an alternative name for the protection group, and is opaque to the system.
  - **Custom** - This field is for operator use and is opaque to the system.
6. When you are finished, click **OK**.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View > Server > Tasks** window. The new provisioning appears in the Network tree a short while after the task completes successfully.

---

### Deleting a Protection Group

Use this procedure to delete a WPS protection group on a BT17800 Series network element.

1. Expand the network element in the Network tree to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.
3. Expand a WPS module to show the protection groups on that module.
4. Right click a protection group and select **Group > Delete**.

The **Delete Wavelength Protection Group** confirmation dialog appears.

5. Click **OK** to delete the group.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View > Server > Tasks** window. The new provisioning appears in the Network tree a short while after the task completes successfully.

---

### Editing a Port

Use this procedure to edit a WPS protection group port on a BT17800 Series network element.

WPS protection group ports are automatically created when you add a protection group.

1. Expand the network element in the Network tree to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.

3. Expand a WPS module to show the protection groups on that module.
4. Expand a protection group to show the ports in that group.
5. Right click a port and select **Port >Edit**.

The **Edit Wavelength Protection Port** dialog appears:

The screenshot shows a Windows-style dialog box titled "Edit Wavelength Protection Port wpsport:1/7/L2A". It features a "Port Settings" tab. The settings are as follows:

Field	Value
Port Name	wpsport:1/7/L2A
Status	Active
Threshold (dB)	-35.0
Remote-Id	
Id	
Custom	

At the bottom right of the dialog are "Cancel" and "OK" buttons.

6. Edit the protection port as follows:
  - **Port Name**- This field is automatically assigned and cannot be changed.
  - **Status** - This read-only field shows the operational status of a line port. It is not applicable to a client port.
  - **Threshold (dB)** - Select the threshold at which a loss of light condition is declared. This field applies to both client and line ports. Additionally, on line ports, when the receive power drops below this threshold, an automatic protection switch might take place.
  - **Remote Id** - This field is for operator use and is opaque to the system. PSM does not use this field for topology.

- **Prot Id** - This is an alternative name for the protection group, and is opaque to the system.
  - **Custom** - This field is for operator use and is opaque to the system.
7. When you are finished, click **OK**.

The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View > Server > Tasks** window. The new provisioning appears in the Network tree a short while after the task completes successfully.

## Enabling or Disabling a Port

Use this procedure to administratively enable or disable a port on a BT17800 Series network element.

1. Expand the network element in the Network tree to show the shelves in that NE.
2. Expand a shelf to show the slots in that shelf.
3. Expand a UFM to show the BICs on that UFM.
4. Expand a BIC to show the ports on that BIC.
5. Enable or disable a port as follows.
  - a. To enable a provisioned port, right click the port and select **Admin State > Enable**.
  - b. To disable a provisioned port, right click the port and select **Admin State > Disable**.

## Nodal Management for Juniper Networks Routers and Switches

PSM supports management of the following interfaces on Juniper Networks routers and switches:

- MX Series router
  - 100GE interface on the 100-Gigabit DWDM OTN MIC with CFP2-ACO (MIC3-100G-DWDM)
  - 100GE interface on the CFP2-DCO (CFP2-DCO-T-WDM-1) transceiver on the 100-Gigabit Ethernet MIC with CFP2 (MIC6-100G-CFP2)
  - 100GE interface on the CFP2-DCO (CFP2-DCO-T-WDM-1) transceiver on the 2x100GE + 4x10GE MPC5E (MPC5E-100G10G)
  - 10GE interfaces on the 6x40GE + 24x10GE MPC5E (MPC5E-40G10G)
  - 10GE interfaces on the 6x40GE + 24x10GE MPC5EQ (MPC5EQ-40G10G)
  - 10GE interfaces on the 2x100GE + 4x10GE MPC5E (MPC5E-100G10G)
  - 10GE interfaces on the 2x100GE + 4x10GE MPC5EQ (MPC5EQ-100G10G)

- PTX Series router
  - 100GE interfaces on the 100-Gigabit DWDM OTN PIC with CFP2-ACO (PTX-5-100G-WDM)
  - 100GE interface on the CFP2-DCO (CFP2-DCO-T-WDM-1) transceiver on the 100-Gigabit Ethernet OTN PIC with CFP2 (P2-100GE-OTN)
- QFX Series switch
  - Ports on the QFX10K DWDM 1.2T Line Card (QFX10K-12C-DWDM)

PSM supports this same set of interfaces for service activation. See [“Activating an Optical Service Between Transponder Interface Endpoints” on page 308](#) for more information.



**NOTE:** These interfaces must already exist. You cannot use PSM to create these interfaces.

The following management functions are supported:

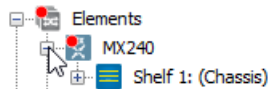
- [Editing an Interface on page 258](#)
- [Enabling or Disabling a Port on page 262](#)
- [Viewing Interface PMs on an MX Series or PTX Series Router or QFX Series Switch on page 263](#)

## Editing an Interface

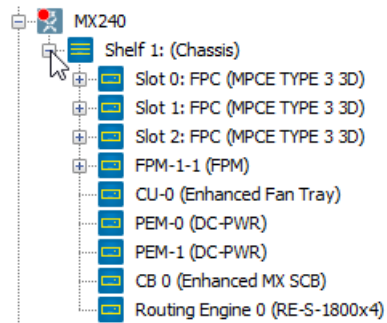
Use this procedure to edit an interface on a port on an MX Series or PTX Series router or QFX Series switch.

This procedure uses the MX Series router as an example but applies equally to MX Series and PTX Series routers and QFX Series switches. There might be slight differences between devices but the general procedure is the same.

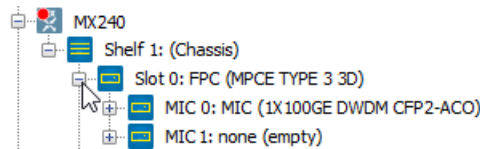
1. Expand an MX Series or PTX Series router or QFX Series switch in the Network tree to show the shelves in that router or switch.



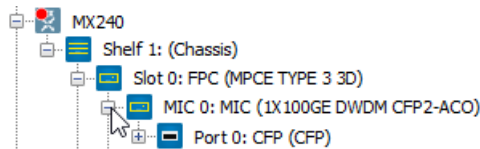
2. Expand a shelf to show the slots in that shelf.



3. Expand a slot to show the MICs/PICs in the MPC/FPC in that slot.



4. Expand a MIC/PIC to show the ports for that MIC/PIC.



5. If you are configuring a QFX10K DWDM 1.2T Line Card (QFX10K-12C-DWDM) on a QFX Series switch, you need to configure the modulation scheme and the optical signal parameters at the port level because the OTU4 signals are modulated within the optical signal on the containing port.

If you are configuring any other interface, go to 7.

To configure the modulation scheme and the optical signal parameters on the port, right click the port and select **Optical>Edit**.

The following window appears:

ot-1/0/0

Settings

**Physical**

Grid: 50 GHz Channel Name: C41

Wavelength: 1550.52 nm Frequency: 193.35 THz

Loopback: NO\_LOOPBACK ☒ Laser Enabled

TX Power: -2 dBm

LOS Alarm Threshold: -22 dBm

LOS Warning Threshold: -21 dBm

Modulation: 8qam FEC: SDFEC\_25

Cancel OK

6. Configure the physical attributes:

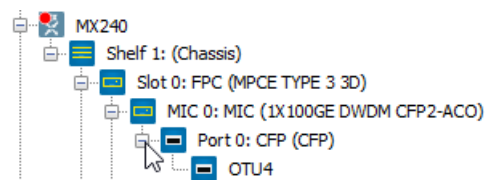
- **Modulation** - Select the modulation scheme.
- For the other physical parameters, see [10](#) and [11](#).



**NOTE:** For some transceivers, you can configure the line encoding.

Proceed to the next step to configure the interface parameters.

7. Expand a port to show the interfaces for that port.



8. Right-click a provisioned interface and select **Interface >Edit**.

The **Edit Interface** dialog appears.



Figure 61: Edit Interface (OTU4)

Settings

**General**

Type:

**OTU**

FEC:

TTI

Transmitted SAPI :

Expected Receive SAPI :

**Physical**

Grid:  Channel Name:

Wavelength:  nm Frequency:  THz

Loopback:  ☒ Laser Enabled

TX Power:  dBm



**NOTE:** The Physical panel does not appear here for interfaces where the optical signal is configured at the port level.

9. Configure the general interface attributes:

- **Type** - The type is automatically set based on the interface and cannot be changed.

10. Configure the protocol attributes. Protocol attributes vary depending on the protocol.

- **FEC** - Specify the type of Forward Error Correction (FEC) from the drop-down menu.
- **Transmitted SAPI** - Specify the transmit Source Access Point Identifier in the Trail Trace Identifier (TTI) panel or click the **Auto Set** button. When you click the **Auto Set** button, PSM automatically configures the SAPI with the IP address and interface name encoded in hexadecimal format. For example, a SAPI of 10.161.33.106-et-1/0/0 is automatically encoded and stored on the device as 0AA1216A010000, where:
  - characters 1 through 8 (0AA1216A) represent the IP address
  - characters 9 and 10 (01) represent the slot
  - characters 11 and 12 (00) represent the PIC/MIC
  - characters 13 and 14 (00) represent the port



**NOTE:** If you specify the SAPI explicitly without using Auto Set and the SAPI is in the IP address and interface name format, PSM automatically encodes the SAPI in hexadecimal format and stores the resulting string on the device. If the SAPI is not in the IP address and interface name format, PSM stores the string as entered without encoding.

- **Expected Receive SAPI** - Specify the expected receive SAPI in the TTI panel.



**NOTE:** If the SAPI is in the IP address and interface name format, PSM automatically encodes the SAPI in hexadecimal format and stores the resulting string on the device. If the SAPI is not in the IP address and interface name format, PSM stores the string as entered without encoding.

11. Configure the physical attributes.

- **Grid** - Specify the frequency grid. This cannot be changed for most transceivers.
- **Channel Name, Wavelength, or Frequency** - Specify the desired channel, the desired wavelength, or the desired frequency. Setting one field automatically sets the others. This can only be specified for tunable transceivers.
- **Loopback** - Not supported.
- **Laser Enabled** - Not supported.
- **TX Power** - Specify the transmit power of the laser.
- **LOS Alarm Threshold** - Specify the Loss of Signal (LOS) threshold above which an alarm is raised.
- **LOS Warning Threshold** Specify the LOS threshold above which a warning is issued.

12. When you are finished, click **OK**.

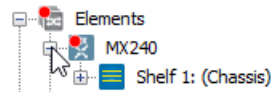
The PSM server sends the configuration request to the router or switch. You can monitor the status of the request through the **View > Server > Tasks** window. The new provisioning appears in PSM a short while after the task completes successfully.

## Enabling or Disabling a Port

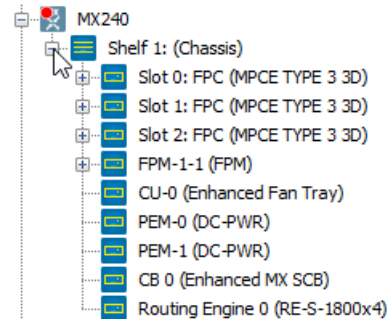
Use this procedure to administratively enable or disable a supported port on an MX Series or PTX Series router or QFX Series switch.

This procedure uses the MX Series router as an example but applies equally to MX Series and PTX Series routers and QFX Series switches. There might be slight differences between devices but the general procedure is the same.

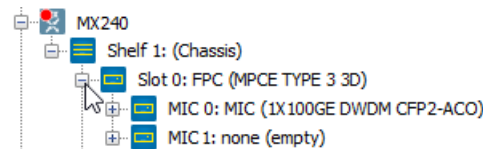
1. Expand an MX Series or PTX Series router or QFX Series switch in the Network tree to show the shelves in that router or switch.



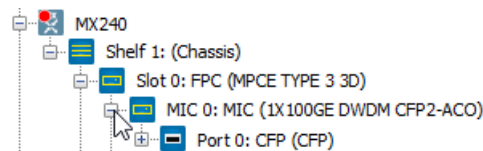
2. Expand a shelf to show the slots in that shelf.



3. Expand a slot to show the PICs or MICs in that slot.



4. Expand a PIC or MIC to show the ports.



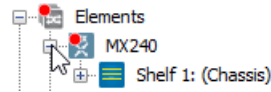
5. Enable or disable a port as follows.
  - a. To enable a provisioned port, right click the port and select **Admin State >Enable**.
  - b. To disable a provisioned port, right click the port and select **Admin State >Disable**.

## Viewing Interface PMs on an MX Series or PTX Series Router or QFX Series Switch

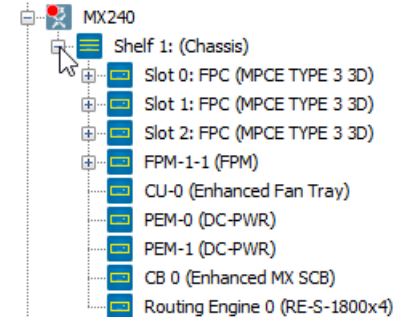
Use this procedure to view current interface PMs on an MX Series or PTX Series router or QFX Series switch.

This procedure uses the MX Series router as an example but applies equally to MX Series and PTX Series routers and QFX Series switches. There might be slight differences between devices but the general procedure is the same.

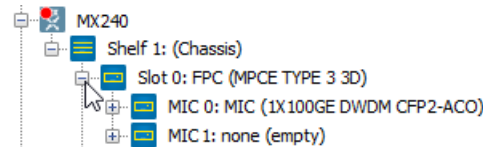
1. Expand an MX Series or PTX Series router or QFX Series switch in the Network tree to show the shelves in that router or switch.



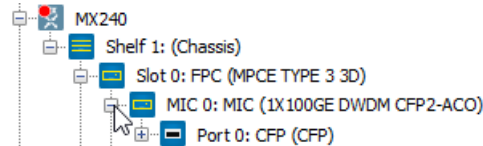
2. Expand a shelf to show the slots in that shelf.



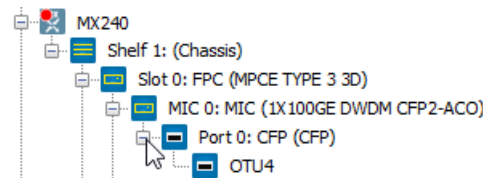
3. Expand a slot to show the PICs or MICs in that slot.



4. Expand a PIC or MIC to show the ports.



5. Expand a port to show the interfaces for that port.



6. Right-click a provisioned interface and select **Interface PMs >View**.

The **Interface Current PM** window appears:

et-0/0/0 Fri 23 Sep 2016 19:04:04 EDT

PM Name	Value
NearEnd ODU Bit Interleaved Parity (NEAR-ODU-BIP8)	0
NearEnd ODU Errored Seconds (NEAR-ODU-ES)	0
NearEnd ODU Errored Seconds (NEAR-ODU-SES)	0
NearEnd ODU Severely Unavailable Seconds (NEAR-ODU-UAS)	233
Near End ODU Background Block Errors (NEAR-ODU-BBE)	0
NearEnd ODU Errored Seconds Ratio (NEAR-ODU-ESR)	0
NearEnd ODU Severely Errored Seconds Ratio (NEAR-ODU-SESR)	0
Near End ODU Background Block Errors Ratio (NEAR-ODU-BBER)	0
FarEnd OTU Bit Interleaved Parity (FAR-OTU-BIP8)	0
FarEnd OTU Errored Seconds (FAR-OTU-ES)	0

Refresh Export

The PMs are listed for the interface selected.



**NOTE:** This window shows a snapshot of the PM counts. The counts do not update automatically in this window. To see the latest counts, click the **Refresh** button.

- To select what columns to display, right-click anywhere in the headings row to bring up a column selection window.  
Check or uncheck column headings as desired.
- To sort the PMs based on column values, click on the column heading that you want to sort.
- To export the PM data to a CSV file, click **Export** and save the file.

## Nodal Management for BTI800 Series Network Elements

This section covers the following topics:

- [Enabling or Disabling a Port on page 265](#)

### Enabling or Disabling a Port

Use this procedure to administratively enable or disable a port on a BTI800 Series network element.

- Expand the network element in the Network tree to show the shelves in that NE.
- Expand a shelf to show the slots in that shelf.

3. Expand a module to show the ports on that module.
4. Enable or disable a port as follows.
  - a. To enable a provisioned port, right click the port and select **Admin State >Enable**.
  - b. To disable a provisioned port, right click the port and select **Admin State >Disable**.

## CHAPTER 9

# Configuring PSM Client Options

- [Introduction on page 267](#)
- [Configuring General Options on page 267](#)
- [Configuring Alerts Options on page 268](#)
- [Configuring Display Options on page 269](#)
- [Configuring Performance Monitoring Options on page 277](#)
- [Configuring Utilities on page 279](#)

## Introduction

---

PSM client options control the behavior of the specific PSM client in which the options are set, and the settings are stored on the computer in which the client is running. Therefore, the options that you set are not applicable if you log in on another PSM client.

Client options control a variety of behaviors, including the specification of external executables to launch from the client for tasks such as connecting to the CLI of a network element.



**NOTE:** This chapter describes procedures to change PSM options on a Windows client. If you are running on OS X, the options window is accessed by `psmclient >Preferences....`

---

## Configuring General Options

---

The PSM client gives you options to control general behavior. This section covers the following topics:

- [Setting Auto-logout on page 267](#)

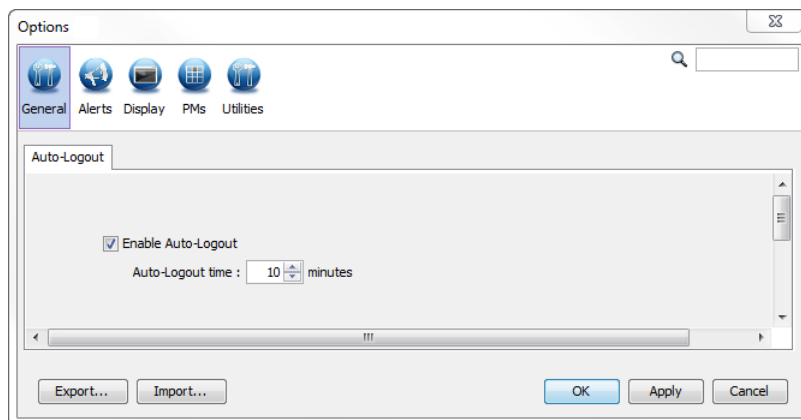
### Setting Auto-logout

The PSM Client allows you to automatically log out a user after a specified idle period. This setting applies to all users logging in on the PSM Client in which this option is set. This setting does not apply to users logging in on a different PSM Client.

1. From the main menu, choose **Tools >Options**.

The Options window is displayed.

2. Click the **General** tab.



3. To enable auto-logout, select the **Enable Auto-Logout** checkbox.
4. Specify the **Auto-Logout** time.  
The PSM Client automatically logs a user out if the user is idle for the specified time.
5. Click **OK**.

---

## Configuring Alerts Options

The PSM client gives you options to control various audible alerts. This section covers the following topics:

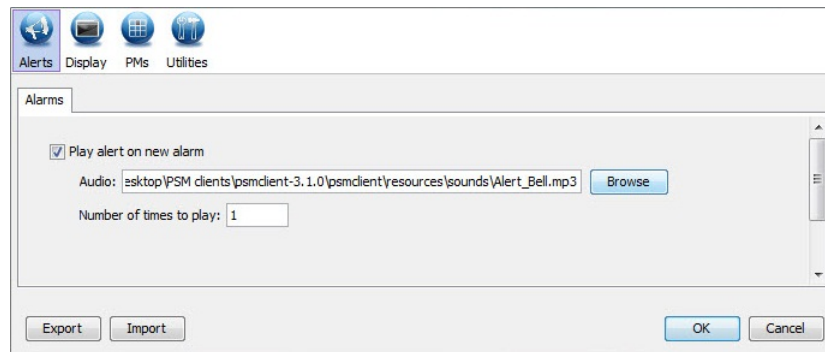
- [Setting Alarm Alerts Options on page 268](#)

### Setting Alarm Alerts Options

The PSM Client gives you options for the alerting of new alarms. To modify these options, use the following procedure.

1. From the main menu, choose **Tools>Options**.  
The **Options** window is displayed.
2. Click the **Alerts** tab.
  - To enable audible alerts, select **Play alert on new alarm**.
  - Browse to and select the audio file that contains the desired alert tone.
  - Select the **Number of times to play** the tone.





3. Click **OK**.

## Configuring Display Options

The PSM client allows you to control various display options. This section covers the following topics:

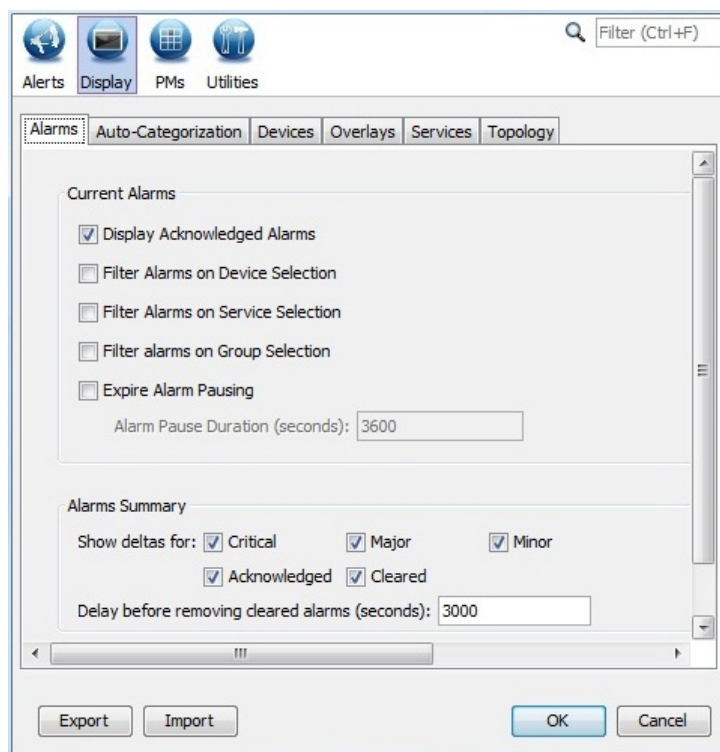
- [Setting Alarm Display Options on page 269](#)
- [Setting Auto-categorization Options on page 270](#)
- [Setting Device Display Options on page 274](#)
- [Setting Overlay Display Options on page 274](#)
- [Setting Service Display Options on page 275](#)
- [Setting Topology Display Options on page 276](#)

### Setting Alarm Display Options

The PSM Client gives you options for the display of alarms. To modify these options, use the following procedure.

1. From the main menu, choose **Tools>Options**.  
The **Options** window is displayed.
2. In the **Options** window, click **Display**.
3. Click the **Alarms** tab.
  - To display acknowledged alarms in the alarms pane, check the **Display Acknowledged Alarms** check box.
  - To filter the alarms in the alarms pane to only display alarms that relate to a selected device when that device is selected in the Topology view or in the Tree view, check the **Filter Alarms on Device Selection** check box.
  - To filter the alarms in the alarms pane to only display alarms that relate to a selected service when that service is selected in the Topology view or in the Tree view, check the **Filter Alarms on Service Selection** check box.

- To filter the alarms in the alarms pane to only display alarms that relate to a particular group when that group is selected in the Topology view or in the Tree view, check the **Filter Alarms on Group Selection** check box.
- To automatically resume alarm notifications after alarm notifications have been suspended, check the **Expire Alarm Pausing** check box and specify the **Alarm Pause Duration** to wait for before resuming.
- To **Show deltas for** alarms in the alarms summary bar, select the alarm severities for which deltas are to be shown. Deltas are incremental alarm counters that provide an indication of how many new alarms have been raised since the counters were last cleared.
- To specify how long to keep cleared alarms in the alarms pane, enter the **Delay before removing cleared alarms** in seconds. A setting of **0** causes the alarm to be removed from the table immediately once it is cleared. Changes to this setting take effect for newly-raised alarms only. Existing alarms continue to use the previously-configured delay value.



4. Click **OK**.

## Setting Auto-categorization Options

Use this procedure to set the auto-categorization options.

When there are many services or customers, the **Network** tree can be difficult to navigate. To reduce the visual clutter, PSM can automatically categorize and aggregate services

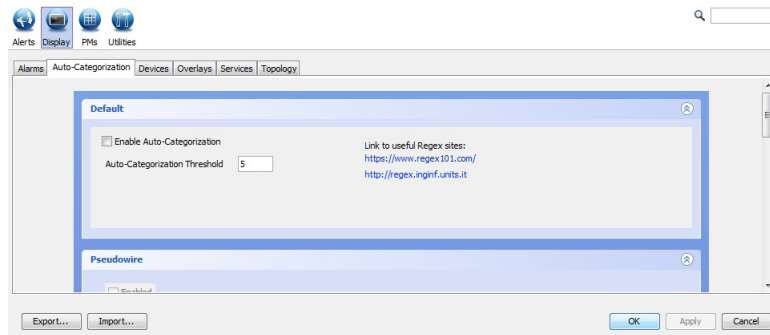
and customers in the tree. You can let PSM choose default category names for you, or you can customize how PSM chooses the category names.

1. From the main menu, choose **Tools >Options**.

The **Options** window is displayed.

2. Click the **Auto-Categorization** tab.

The auto-categorization options appear. There is a general **Default** section followed by a section for each branch of the tree that supports customized categorization.



3. To enable auto-categorization, select the **Enable Auto-Categorization** check box.

This enables auto-categorization for items in the **Network** tree.

4. Specify the **Auto-Categorization Threshold**.

When the number of items in a branch exceeds this threshold, PSM begins auto-categorization for that branch.

5. To use the default PSM categories, click **OK**. Otherwise go to 6.

The **Network** tree is updated to show the new categorization. The default categories are based on alphabetical categorization. For example:

Figure 62: Customers Branch Without Auto-categorization

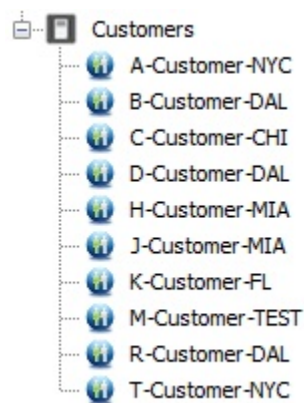
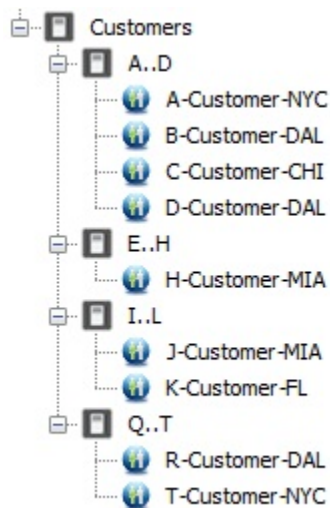


Figure 63: Customers Branch with Auto-categorization Using Default Categories



6. To customize the categorization, use regular expressions to specify how you want the categories to be created.

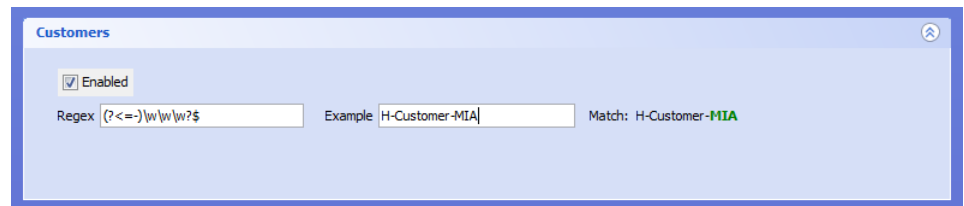
The idea is to use regular expressions to match parts of the name of each entry. The matched parts then become the category names to which the entries are assigned.

- a. Select the **Enabled** check box for the branch that you want to customize.
- b. Type the regular expression in the **Regex** field. For example:

The regular expression `(?<=)\w\w\w?$` looks at the end of each name for two or three alphanumeric characters prefixed by a hyphen. The two or three alphanumeric characters then form the category to which this entry belongs.

- c. To test your regular expression, enter a string in the **Example** field.

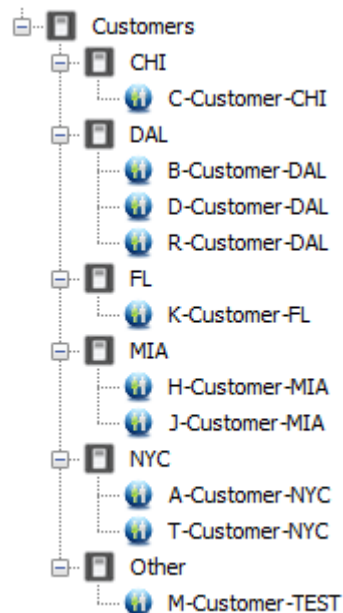
PSM will test your regular expression against the example string. For example:



The matched part of the string is shown in green. This green part represents the category name to which the example string belongs. You can repeatedly test your regular expression by entering different strings in the **Example** field.

- d. Click **Apply** to apply your regular expression against the respective branch in the tree.

This results in a set of matched strings. Some names might have matched strings while others do not. The first matched string in a name defines the category that the entry belongs to. If the category does not exist in the branch, PSM will create the category. Names that do not have any matched strings are placed in the **Other** category. Here is the resulting Customers branch for the regular expression above.



For a basic introduction to regular expressions, see [“Regular Expressions” on page 578](#).

- e. Repeat for all branches that you want to customize.
7. Click **OK** to exit when you are done.

## Setting Device Display Options

The PSM Client gives you options for the display of NEs. To modify these options, use the following procedure.

1. From the main menu, choose **Tools>Options**.

The **Options** window is displayed.

2. Click the **Devices** tab.

If you want to display the IP address in addition to the device name in the **Tree** view and/or the **Map** view, then select the applicable check boxes.



**NOTE:** If you select the **Tree** view, the IP address is also displayed in the **NE** column in the **Alarms** window.



3. Click **OK**.

## Setting Overlay Display Options

Use this procedure to modify the appearance of how data widgets are overlaid on the background window.

This setting affects the appearance of the real-time PM data widgets and the link details widgets.

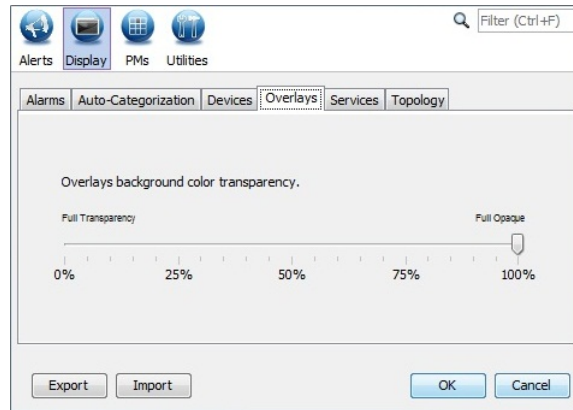
1. From the main menu, choose **Tools>Options**.

The **Options** window is displayed.

2. In the **Options** window, click **Display**.

3. Click the **Overlays** tab.

Adjust the transparency of the data widgets. Choose any value from "0%" for completely transparent to "100%" for completely opaque.



4. Click **OK**.

## Setting Service Display Options

To modify the appearance of how Ethernet services are shown, use the following procedure.

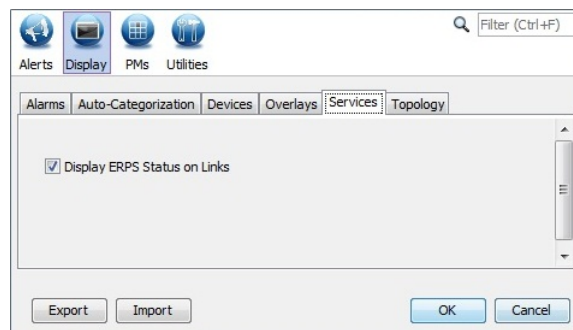
1. From the main menu, choose **Tools>Options**.

The **Options** window is displayed.

2. In the **Options** window, click **Display**.

3. Click the **Services** tab.

To display a visual representation of the ERPS status in the Ethernet services topology view, select **Display ERPS status on links**.



The ERPS status is represented by a , , or a . For more information, see [“Visualizing an ERPS Service” on page 414](#).

4. Click **OK**.

## Setting Topology Display Options

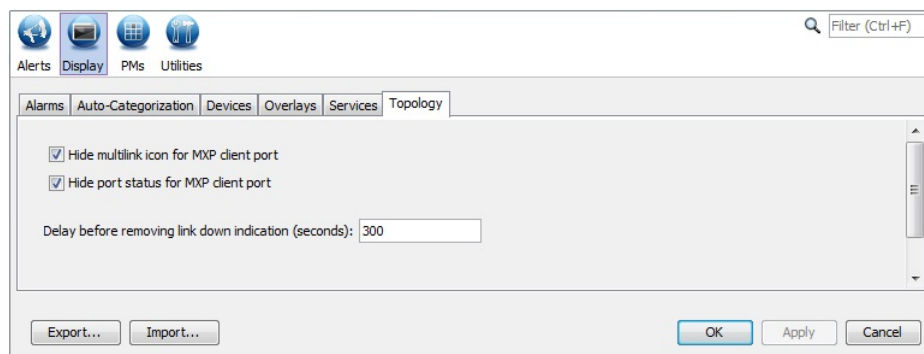
To modify the appearance of how links are displayed in the topology view, use the following procedure.

1. From the main menu, choose **Tools>Options**.

The **Options** window is displayed.

2. In the **Options** window, click **Display**.

3. Click the **Topology** tab.




- a. To exclude MXP client port to MXP client port connections when determining whether to display the multi-link icon in the topology view, select **Hide multilink icon for MXP client port**.

This is useful when you are viewing the topology for MXP links and you only want to see the multi-link icon for line port connections.

- b. To disregard the port status of MXP client ports when determining the link color to display in the topology view, select **Hide port status for MXP client port**.

This is useful when you want the color of the MXP link to reflect the state of the line port connections only. If you select this option, and the MXP link only contains client port connections, then the color of the link is grey.

- c. To allow the link down indication to persist for a period of time, specify the **Delay before removing link down indication (seconds)**.

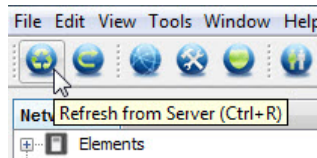
This setting allows you to see when a link goes down and comes back up. When a link goes down and comes back up, the link down indication  is shown in the topology Map view for the specified number of seconds before being removed.

4. Click **OK**.





**NOTE:** For changes to these options to take effect for existing connections, you must click the Refresh from Server icon.



## Configuring Performance Monitoring Options

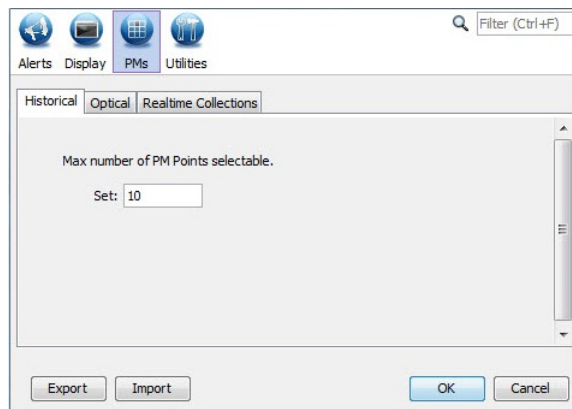
The PSM Cclient allows you to control the display and collection of performance monitoring counters (PMs). This section covers the following topics:

- [Setting Historical PM Graphing Options on page 277](#)
- [Setting Optical Graphing Options on page 278](#)
- [Setting Real-time Collections Options on page 278](#)

### Setting Historical PM Graphing Options

To set the graphing options for historical PMs, use the following procedure:

1. From the main menu, choose **Tools>Options**.  
The **Options** window is displayed.
2. In the **Options** window, click **PMs**.
3. Click the **Historical** tab.
  - In the **Max number of PM Points selectable** box, specify the maximum number of PM metrics to display in the graph.



4. Click **OK**.

## Setting Optical Graphing Options

To modify the information shown in the "All Channels" optical PM graph, use the following procedure:

1. From the main menu, choose **Tools>Options**.

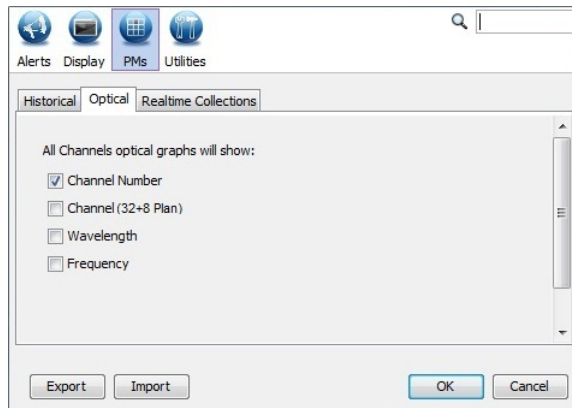
The **Options** window is displayed.

2. In the **Options** window, click **PMs**.

3. Click the **Optical** tab.

- To display the channel number in the domain (horizontal) axis of the "All Channels" graph, select the **Channel Number** check box.
- To display the channel (32+8 Plan) number in the domain (horizontal) axis of the "All Channels" graph, select the **Channel(32+8 Plan)** check box.
- To display the wavelength in the domain (horizontal) axis of the "All Channels" graph, select the **Wavelength** check box.
- To display the frequency in the domain (horizontal) axis of the "All Channels" graph, select the **Frequency** check box.

Multiple check boxes can be selected.

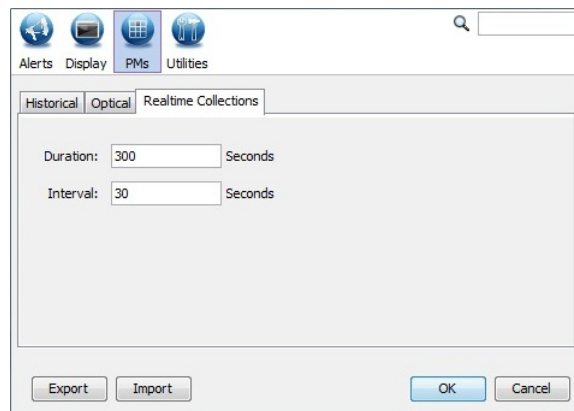


4. Click **OK**.

## Setting Real-time Collections Options

To modify how long real-time PM data is collected and how frequently the counts are updated, use the following procedure.

1. From the main menu, choose **Tools>Options**.  
The **Options** window is displayed.
2. In the **Options** window, click **PMs**.
3. Click the **Realtime Collections** tab.
  - Select the **Duration** over which the real-time PM data is to be collected.
  - Select the **Interval** or frequency with which the real-time PM data is updated.



4. Click **OK**.

## Configuring Utilities

The PSM client makes use of external executables for the following utilities:

- CLI
- Node Controller
- Ping
- SNMP Ping
- Traceroute

The PSM client is preconfigured to provide these utilities using specific executables on your computer. You can customize where the PSM client looks for these executables. If the network element being managed requires a specific node controller executable, you can also specify where that node controller executable can be found.

- [Setting Utility Executables on page 280](#)
- [Configuring the proNX 900 Node Controller on page 282](#)

## Setting Utility Executables

Use this procedure to configure the CLI, Ping, SNMP Ping, and Traceroute utility executables and parameters.



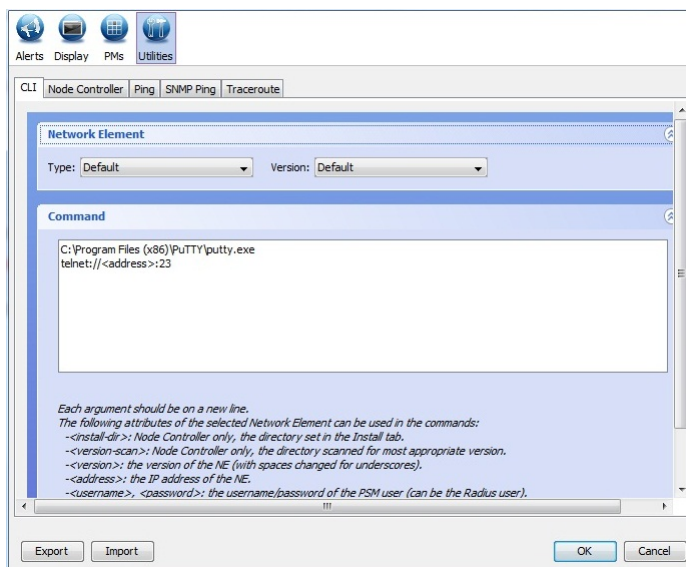
**NOTE:** To use SNMP Ping on Windows, net-snmp or a similar application must be installed. See [“Installing Net-SNMP” on page 555](#).

1. Select **Tools >Options**.

The Options window is displayed.

2. Click the **Utilities** tab.

The Utilities panel is displayed.



3. For each tab in the Utilities panel, specify the desired executables and parameters.
  - a. Select the utility that you want to configure (**CLI, Ping, SNMP Ping, Traceroute**).
  - b. Select the Network Element **Type** from the drop-down menu.

If you want to apply your changes to all network element types, then leave the **Type** at **Default**. If you want to tailor the executable to a particular type of network element, then select the specific type from the drop-down menu.



**NOTE:** Once you make a change to the parameters of a specific type of network element, the Default parameters no longer apply for that type of network element.

- c. Select the Network Element **Version** from the drop-down menu.

If you want to apply your changes to all versions of the selected network element type, then leave the **Version** at **Default**. If you want to tailor the executable to a particular version of the selected network element type, then select the specific version from the drop-down menu.



**NOTE:** Once you make a change to the parameters of a specific version, the **Default** parameters no longer apply for that version of network element.

- d. Specify the command syntax for the selected utility.

You can specify the name and path to the executable and the parameters to use.

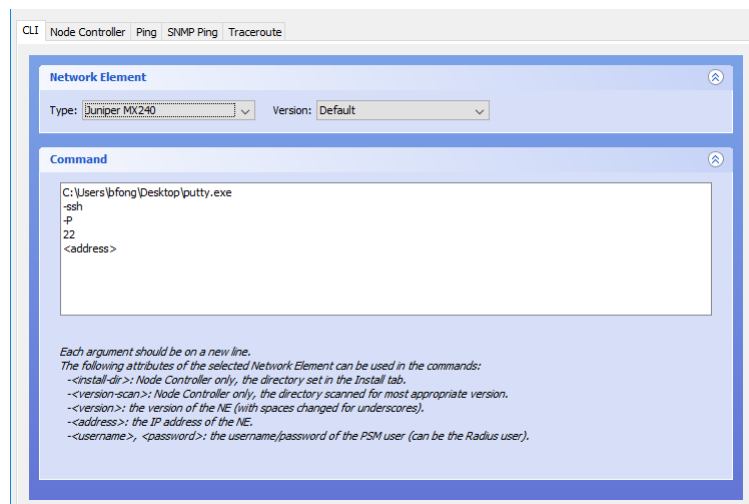
For example, the command to launch the CLI (`C:\Users\user\Desktop\putty.exe -ssh -P 22 <login_username>@<IP_address_of_selected_NE>`) is represented by this configuration:

```

C:\Users\user\Desktop\putty.exe
-ssh
-P
22
user@<address>
  
```

The **<username>** construct is a variable that represents the username of the current PSM user (that is, the username you used to log in to the current PSM client session). The **<address>** construct is a variable that represents the IP address of the selected NE. The above configuration launches the `putty.exe` executable from the specified path and sets up an SSH connection to the selected NE using the username of the current PSM user.

If you are running `putty.exe` on Windows and you want to explicitly specify the username when launching the CLI, then remove the **<username>** construct. For example:



This forces putty.exe to prompt you for the username to use when you launch the CLI.



**NOTE:** The above are examples of applications and parameters to use. The validity of the parameters depends on the application chosen.

4. When you are done, click **OK**.

This procedure is complete.



**NOTE:** To connect to the CLI, see [“Connecting to the CLI on a Network Element” on page 114](#). To launch the Node Controller on the BT17000, see [“Launching the proNX 900 Node Controller” on page 134](#). To launch the other utilities, see [“Performing Diagnostics” on page 540](#).

## Configuring the proNX 900 Node Controller

Use this procedure to configure how to launch the proNX 900 Node Controller.

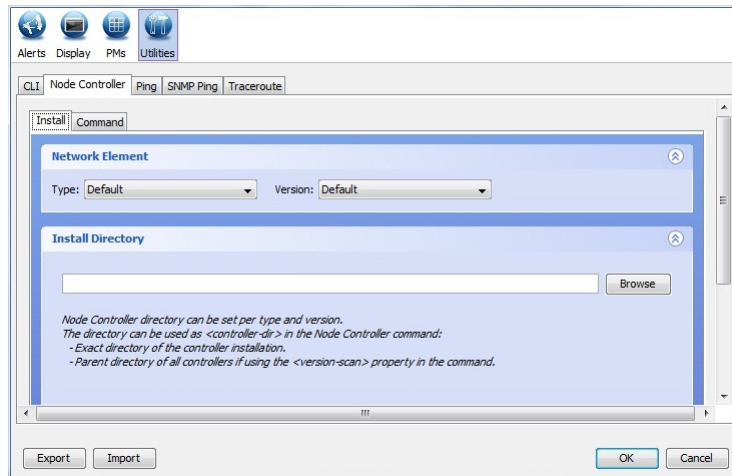
The proNX 900 Node Controller is the nodal manager for the BT17000 Series network elements.



**NOTE:** The proNX 900 Node Controller might not be supported on all PSM client platforms. See the *BT17000 Series Common Equipment Installation Guide* for a list of platforms that support the proNX 900 Node Controller.

**Prerequisites:**

- The proNX 900 Node Controller software that is compatible with the network elements in your network must be installed on your local computer.
1. From the main menu, choose **Tools>Options**.  
The Options window is displayed.
  2. Click the **Utilities** button and then click the **Node Controller** tab.
  3. There are several methods by which you can specify the path to the proNX 900 application software on your local computer:
    - If all of your versions of proNX 900 are in one directory, you can browse to that directory and select it. Afterwards, when you launch proNX 900, PSM chooses the correct version of the proNX 900 for the selected NE and launches it. If it cannot find an exact match, PSM chooses the best match and prompts you to confirm. Continue at 4.
    - Manually determine the path to the executable file for each NE type and version, and then copy and paste the path into the proNX 900 Node Controller tab for that version. Continue at 5.
  4. To browse to and select the directory that contains the desired proNX 900 version(s), click the **Install** tab and perform the following steps.



- a. Click **Browse** and navigate to the proNX 900 installation directory, for example:

C:\Program Files (x86)\BTI\



**NOTE:** If you are running the PSM Client on a 32-bit Windows operating system, you might need to specify a different path for the installation directory, for example: C:\Program Files\BTI .

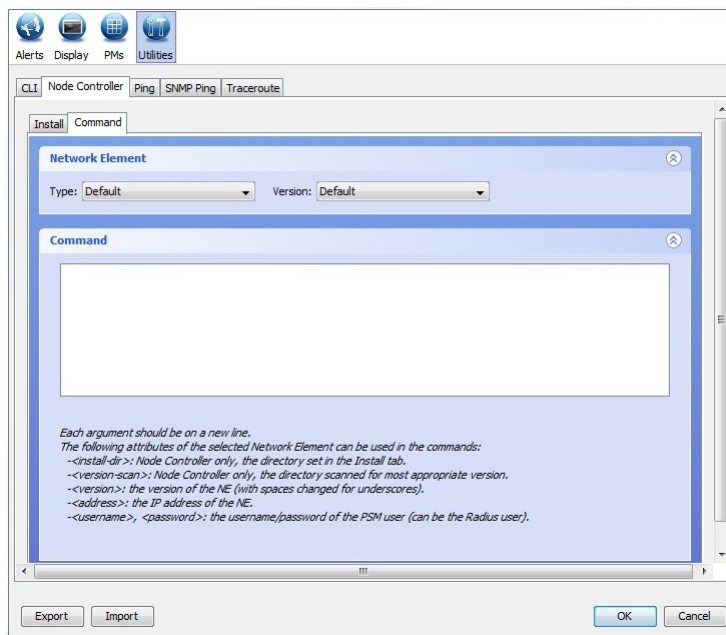
- b. Select the directory and click **Open**.

The path to the directory is pasted into the **Install Directory** field.

- c. Click **OK**.

This procedure is complete. You can now launch the proNX 900 as instructed in the first step.

5. To manually cut and paste the path to the executable file, click the **Command** tab and perform the following steps.



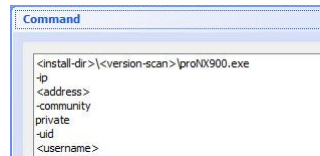
- a. Select the NE **Type** and proNX 900 **Version** that you want to launch from the drop-down menus.
- b. In your file system, navigate to the proNX 900 executable file, for example **C:\Program Files (x86)\BTI\proNX900\_9.3.0\_C001\proNX900.exe**. Copy the entire path.



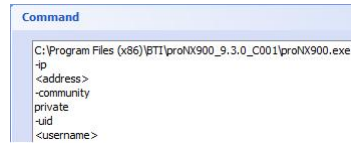
**NOTE:** If you are running the PSM Client on a 32-bit Windows operating system, you might need to specify a different path for the installation directory, for example: **C:\Program Files\BTI**.

- c. In the first line of the **Command** window, paste the new path to the proNX 900 application executable file over the existing path shown. The first image shows an unaltered command string in the first line, and the second image shows the command string after the path to the executable file has been pasted in.





```
Command
<install-dir>\<version-scan>proNX900.exe
-ip
<address>
-community
private
-uid
<username>
```



```
Command
C:\Program Files (x86)\BTI\proNX900_9.3.0_C001\proNX900.exe
-ip
<address>
-community
private
-uid
<username>
```

- d. In the same command window, scroll down and check the user ID (uid) and password (pid) as follows:
- if you want to launch the proNX 900 without requiring the user to log in, ensure that the user ID (uid) and password (pid) are the same as the NE user ID and password.
  - alternatively, you can remove the user ID and password in the command window, forcing the user to log in when the proNX 900 launches.
- e. As desired, repeat these steps for each NE Type and Version of proNX 900. When you are finished click **OK**.

This procedure is complete.



# Bulk Configuration Of Network Elements

- [Introduction on page 287](#)
- [Creating New Users on Multiple Network Elements on page 287](#)
- [Configuring RADIUS Server Parameters on Multiple Network Elements on page 291](#)
- [Configuring NTP Server Parameters on Multiple Network Elements on page 297](#)

## Introduction

---

PSM allows you to perform configuration operations on multiple network elements concurrently. This is useful when you intend to configure the same information on multiple network elements, such as configuring user accounts and RADIUS and NTP server access, which typically are the same across multiple network elements.

This bulk configuration capability makes use of PSM server scripts to communicate with and configure the network elements.

## Creating New Users on Multiple Network Elements

---

Use this procedure to add the same set of new users to multiple network elements.



**NOTE:** The PSM server treats each network element separately, launching individual tasks to communicate with and configure each NE. A task failure for one NE does not affect tasks for the other NEs.



**NOTE:** PSM connects to each NE using the login credentials that you supplied when you connected to the PSM server. Therefore each NE must be configured with these same login credentials for this procedure to be successful.



**NOTE:** PSM connects to each NE using the applicable protocol for that NE type. When connecting to an NE over SSH (e.g. BTI7800), the SSH key provided by the NE must match the expected key (if the key was previously stored). If the key supplied by the NE does not match the expected key, the task times out and fails. Under normal situations, the supplied key matches the expected key. However, if the NE operating system has been re-installed, the keys might not match. In this situation, you will need to remove the expected key from the PSM server machine's ~/.ssh/known\_hosts file. One method of doing this is to issue the following Linux command from a Linux shell on the PSM server machine:

```
# sed -i '/NE_IP_address/d' ~/.ssh/known_hosts
```

where **NE\_IP\_address** is the IP address of the NE.

This procedure is supported on BTI7000 Series, BTI7800 Series, BTI800 Series, and BTI700 Series (excluding BTI718E) NEs.

1. To create one or more new users, select one or more network elements from the main topology window or from the tree view.
2. Right-click and select **Scripts>Network Elements>Create New Users**.

The "Create New Users" dialog appears with the list of selected network elements at the top:

Username	Password	Role	Timeout



**NOTE:** The "Selected Network Element(s)" box has limited space to display network elements. In situations where the number of selected network elements is large, some network elements might not be displayed. This is normal behavior and does not affect script execution, which runs for all selected network elements, regardless of whether they appear in the list or not.

3. Click **Add** to add a user.

A new row appears.

4. Click inside each field and add the necessary information. Select the "Role" from a pull-down menu.

Username	Password	Role	Timeout
JohnDoe	#\$%34*%7	superuser	30

- Username - the username for the new user. It must be unique on the NEs that are being configured. After entering the Username, make sure you click outside of the Username box to exit Username entry mode.
- Password - the password must be at least six characters long and no more than ten characters long, even though this constraint might not exist when adding users to the NEs directly (using the CLI). Allowable characters are **a-z**, **A-Z**, **0-9**, and the following special characters: **!@#\$%^&()\_+[]{}~`<>.** After entering the password, make sure you click outside of the Password box to exit Password entry mode.

- Role - the privileges that the new user will have. The mapping of roles on the NE is below:

Create New Users Role	Mapped to role on BTI7000 Series
superuser	superuser
provisioning	provisioning
maintenance	maintenance
surveillance	surveillance

Create New Users Role	Mapped to role on BTI7800 Series
superuser	superuser
provisioning	provisioning
surveillance	surveillance

Create New Users Role	Mapped to role on BTI800 Series
superuser	admin
provisioning	operator
surveillance	viewer

Create New Users Role	Mapped to role on BTI700 Series
superuser	administrators
provisioning	operators
maintenance	users
surveillance	guests

- Timeout - the idle timeout before automatically logging the user out. This only applies to the BTI7000 Series NEs, and has no effect on the other NE types.
5. Add as many users as desired. You can delete a row by selecting it and clicking **Delete**.
  6. When you are finished, click **OK**.

The PSM server launches a task for each NE being configured.

7. Look at the Tasks window to verify that each task has completed successfully. A "Create New Users" task can fail for an NE if a user being added already exists on that NE.

In the following example, the "Create New Users" task was successful for 10.1.205.9 but failed for 10.1.205.8.

Tasks			
Task Id	Description	Type	State
1074594	Create New Users	Script Execution Request	FAILURE
1074596	Create New Users (10.1.205.9)	Script Execution	SUCCESS
1074597	Create New Users (10.1.205.8)	Script Execution	FAILURE



**NOTE:** A failure usually indicates that at least one username being added already exists on the NE. The script does not add duplicate usernames, but continues to add all non-duplicate usernames. It is good practice to log in to each failed NE (using the proNX 900) to verify which users have been added successfully and which failed.

This procedure is now complete.

## Configuring RADIUS Server Parameters on Multiple Network Elements

Use this procedure to configure the same RADIUS server parameters across multiple network elements.



**NOTE:** The PSM server treats each network element separately, launching individual tasks to communicate with and configure each NE. A task failure for one NE does not affect tasks for the other NEs.



**NOTE:** PSM connects to each NE using the login credentials that you supplied when you connected to the PSM server. Therefore each NE must be configured with these same login credentials for this procedure to be successful.



.....

**NOTE:** PSM connects to each NE using the applicable protocol for that NE type. When connecting to an NE over SSH (e.g. BTI7800), the SSH key provided by the NE must match the expected key (if the key was previously stored). If the key supplied by the NE does not match the expected key, the task times out and fails. Under normal situations, the supplied key matches the expected key. However, if the NE operating system has been re-installed, the keys might not match. In this situation, you will need to remove the expected key from the PSM server machine's ~/.ssh/known\_hosts file. One method of doing this is to issue the following Linux command from a Linux shell on the PSM server machine:

```
# sed -i '/NE_IP_address/d' ~/.ssh/known_hosts
```

where NE\_IP\_address is the IP address of the NE.

.....

This procedure is supported on BTI7000 Series, BTI7800 Series, BTI800 Series, and BTI700 Series NEs.

1. To configure RADIUS server parameters, select one or more network elements from the main topology window or from the tree view. Only compatible network elements can be selected together.
2. Right-click and select **Scripts>Network Elements>Configure Radius Server**.

The "Create Radius Server" dialog appears with the list of selected network elements at the top. Depending on the type of network element selected, you will see one of the following two dialogs:



Figure 64: Configure Radius Server

Configure Radius Server

Selected Network Element(s)

10.1.203.1

Radius Server Parameters

Radius Server Name:

Radius Server IP Address:

Radius Server Role: primary

Radius Server Port: 1812

Radius Server Key:

Radius Server Priority: remote

Cancel OK

Figure 65: Configure Radius Server (BT1718E)

Configure Radius Server

Selected Network Element(s)

172.27.7.117

Primary Radius Server Parameters

Primary Radius Server Name:

Primary Radius Server IP Address:

Primary Radius Server Role: primary

Primary Radius Server Port: 1812

Primary Radius Server Key:

Primary Radius Server Priority: remote

Add Remove

Cancel OK

For BT17000 Series, BT17800 Series, BT1800 Series and BT1700 Series (excluding the BT1718E) NEs, you are adding a single RADIUS server in this procedure. Repeat the entire procedure to add a second RADIUS server.

For the BTI718E, you are adding the primary and the secondary servers simultaneously in this procedure. Click the **Add** button to expand the dialog to specify up to a maximum of two secondary servers.



**NOTE:** For both dialogs, the "Selected Network Element(s)" box has limited space to display network elements. In some situations where the number of selected network elements is large, some network elements might not be displayed. This is normal behavior and does not affect script execution, which runs for all selected network elements, regardless of whether they appear in the list or not.

### 3. Configure the RADIUS parameters:

Attribute		BTI7000 Series
Radius Server Name		Not applicable.
Radius Server IP Address		Sets the IP address.
Radius Server Role:		
	primary	Sets the <i>Role</i> attribute to <i>primary</i> .
	secondary	Sets the <i>Role</i> attribute to <i>secondary</i> .
	disabled	Sets the <i>Role</i> attribute to <i>disabled</i> . The specified server is configured but not used.
Radius Server Port		Sets the <i>Port</i> attribute to the specified value.
Radius Server Key		Sets the <i>Key</i> (shared secret) attribute to the specified value.
Radius Server Priority		
	disabled	Sets the <i>Authentication Priority</i> attribute to <i>disabled</i> . The NE uses local database authentication only.
	local	Sets the <i>Authentication Priority</i> attribute to <i>local</i> . The NE uses local database authentication first, then RADIUS server authentication.
	remote	Sets the <i>Authentication Priority</i> attribute to <i>remote</i> . The NE uses RADIUS server authentication first, then local database authentication.
Attribute		BTI7800 Series
Radius Server Name		Not applicable.

Attribute	BTI7800 Series
Radius Server IP Address	Sets the IP address.
Radius Server Role	Not applicable.
Radius Server Port	Sets the authentication port to the specified value.
Radius Server Key	Sets the shared secret to the specified value.
Radius Server Priority	Not applicable.

Attribute	BTI800 Series
Radius Server Name	Not applicable.
Radius Server IP Address	Sets the IP address.
Radius Server Role:	
	primary Specifies that this is the primary server for the BTI810. Not applicable for the BTI805, BTI821, BTI822.
	secondary Specifies that this is the secondary server for the BTI810. Not applicable for the BTI805, BTI821, BTI822.
	disabled Not applicable.
Radius Server Port	Sets the authentication port.
Radius Server Key	Sets the shared secret.
Radius Server Priority	
	disabled Not applicable.
	local Sets the <i>auth-order</i> attribute to <i>local</i> . The NE uses local database authentication first, then RADIUS server authentication.
	remote Sets the <i>auth-order</i> attribute to <i>radius</i> . The NE uses RADIUS server authentication first, then local database authentication.

Attribute	BTI700 Series
Radius Server Name	Sets the <i>NAME</i> attribute to the specified value.
Radius Server IP Address	Sets the IP address.
Radius Server Role:	

Attribute		BT1700 Series
	primary	Sets the <i>mode</i> attribute to <i>main</i> and the state to <i>active</i> .
	secondary	Sets the <i>mode</i> attribute to <i>backup</i> , and the state to <i>active</i> .
	disabled	Sets the state to <i>suspend</i> .
Radius Server Port		Sets the <i>auth-port</i> attribute to the specified value.
Radius Server Key		Sets the <i>SECRET</i> attribute to the specified value.
Radius Server Priority		
	disabled	Sets <i>line vty 1 2 login local</i> . The NE uses local authentication for the first two sessions.
	local	Sets <i>line vty 1 2 login local</i> . The NE uses local authentication for the first two sessions.
	remote	Sets <i>line vty 1 2 login radius</i> . The NE uses RADIUS authentication for the first two sessions.

- When you are finished, click **OK**.

The PSM server launches a task for each NE being configured.

- Look at the Tasks window to verify that each task has completed successfully.

In this example, the "Configure Radius Server" task was successful for 10.1.205.8.

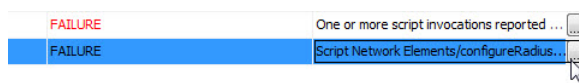
Tasks			
Task Id	Description	Type	State
1096179	Configure Radius Server	Script Execution Request	FINISHED
1096181	Configure Radius Server (10.1.205.8)	Script Execution	SUCCESS

A task might fail under these conditions:

- You are adding a RADIUS server to a BT17000 Series NE that already has two RADIUS servers defined. The task fails and no changes take effect.
- You are adding a RADIUS server to a BT17000 Series NE that has that particular RADIUS server already defined (regardless of the role). The task fails and no changes take effect.



**NOTE:** Other failure conditions exist. Expand the task details of any failed task to see why the task has failed. Since a failed task might still lead to changes on the NE, you will also need to check the NE on task failure.



This procedure is now complete.

## Configuring NTP Server Parameters on Multiple Network Elements

Use this procedure to configure the same NTP server parameters on multiple network elements. It is highly recommended that PSM and all NEs in the network use NTP servers for obtaining the time in order to avoid time discrepancies.



**NOTE:** The PSM server treats each network element separately, launching individual tasks to communicate with and configure each NE. A task failure for one NE does not affect tasks for the other NEs.



**NOTE:** PSM connects to each NE using the login credentials that you supplied when you connected to the PSM server. Therefore each NE must be configured with these same login credentials for this procedure to be successful.



**NOTE:** PSM connects to each NE using the applicable protocol for that NE type. When connecting to an NE over SSH (e.g. BT17800), the SSH key provided by the NE must match the expected key (if the key was previously stored). If the key supplied by the NE does not match the expected key, the task times out and fails. Under normal situations, the supplied key matches the expected key. However, if the NE operating system has been re-installed, the keys might not match. In this situation, you will need to remove the expected key from the PSM server machine's `~/.ssh/known_hosts` file. One method of doing this is to issue the following Linux command from a Linux shell on the PSM server machine:

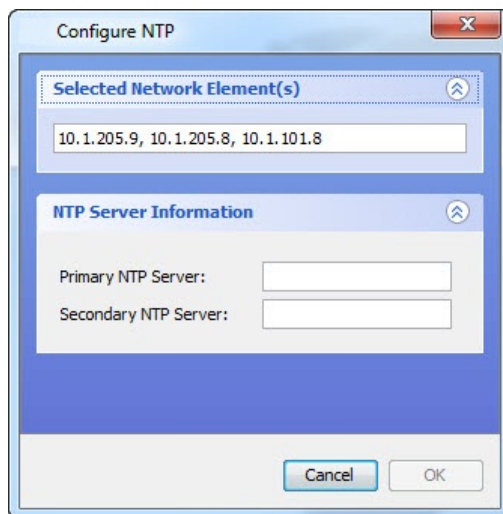
```
# sed -i '/NE_IP_address/d' ~/.ssh/known_hosts
```

where `NE_IP_address` is the IP address of the NE.

This procedure is supported for the BT17000 Series, the BT17800 Series, and the BT1800 Series NEs.

1. To configure NTP server parameters, select one or more network elements from the main topology window or from the tree view.
2. Right-click and select **Scripts>Network Elements>Configure NTP**.

The "Configure NTP" dialog appears with the list of selected network elements at the top:



**NOTE:** The "Selected Network Element(s)" box has limited space to display network elements. In some situations where the number of selected network elements is large, some network elements might not be displayed. This is normal behavior and does not affect script execution, which runs for all selected network elements, regardless of whether they appear in the list or not.

3. Configure the IP address of the **Primary NTP Server** and the **Secondary NTP Server** as desired.



**NOTE:** Not all network elements under management use the concept of primary and secondary NTP servers.

The BTI7000 Series network element keeps a list of up to five NTP servers to use. This procedure appends the new NTP servers to the existing list, with the specified **Primary NTP Server** added ahead of the specified **Secondary NTP Server**. From this list, the NE uses the server with the best stratum value. If you try to add an NTP server when the number of NTP servers is at the maximum number, the task will fail.

The BTI7800 Series network element manages a list of NTP servers with no arbitrary limit. This procedure appends the new NTP servers to the existing list, with the specified **Primary NTP Server** added ahead of the specified **Secondary NTP Server**. The NE tries to use the NTP server at the beginning of this list first. If it fails, then the next NTP server in the list is tried, and so on.

The BTI800 Series network element keeps a list of up to three NTP servers to use. This procedure appends the new NTP servers to the existing list, with the specified **Primary NTP Server** added ahead of the specified **Secondary NTP Server**. The NE tries to use the NTP server that is specified as the **Preferred Server**. The **Preferred Server** is

designated in the **System Information** panel. If you try to add an NTP server when the number of NTP servers is at the maximum number, the task will fail.

4. When you are finished, click **OK**.

The PSM server launches a task for each NE being configured.

5. Look at the Tasks window to verify that each task has completed successfully. A "Configure NTP" task might fail if the NTP server being added is already on the NE list of servers to use.

In this example, the "Configure NTP" task was successful for 10.1.205.8.

Tasks			
Task Id	Description	Type	State
1100680	Configure NTP	Script Execution Request	FINISHED
1100682	Configure NTP (10.1.205.8)	Script Execution	SUCCESS



**NOTE:** A task might fail if the primary or secondary NTP server being added already exists in the NTP server list on that NE. No configuration changes take effect on any failed NE.

This procedure is now complete.





## CHAPTER 11

# Managing Optical and Transport Services

- [Optical Services on page 301](#)
- [Transport Services on page 323](#)
- [Working with Optical/Transport Services and Topology Tables on page 334](#)
- [Saving a Service Image on page 336](#)

## Optical Services

---

An optical service provides optical (wavelength) connectivity between optical service endpoints. An optical service endpoint can be a transponder interface that connects to the optical network or it can be an optical port on equipment within the optical network.

PSM allows users to manage optical services in a BTI7000 or BTI7800 optical network.

In a BTI7000 optical network, the transponder interface endpoints can be BTI7800 UFM interfaces or select interfaces on MX Series or PTX Series routers or QFX Series switches.

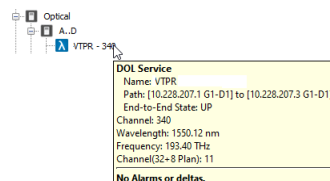
In a BTI7800 optical network, the transponder interface endpoints can be BTI7800 UFM interfaces only.

- [Visualizing an Optical Service on page 301](#)
- [Activating an Optical Service in a BTI7000 Network on page 306](#)
- [Activating an Optical Service in a BTI7800 Network on page 319](#)
- [Viewing the Cross-Connects in an Optical Service on page 321](#)
- [Updating an Optical Service on page 321](#)
- [Deleting an Optical Service on page 321](#)
- [Viewing the Optical Services Table on page 322](#)
- [Viewing the Optical Services Per Span Table on page 322](#)
- [Viewing the Optical Topology Table on page 323](#)

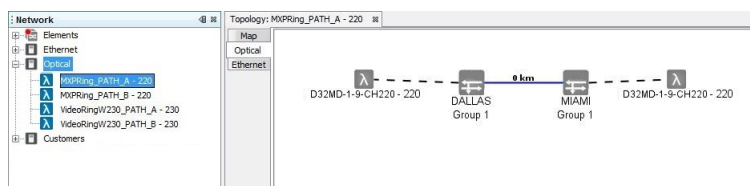
## Visualizing an Optical Service

PSM allows users several ways to visualize an optical service. An optical service can be visualized at the network, service, group, and module levels. Service paths can be highlighted and detailed information can be displayed through tool tips or in table form. The examples in this section are taken from a BTI7000 DOL service.

1. To see a summary of an optical service, hover over the service in the Network tree under the Optical branch.

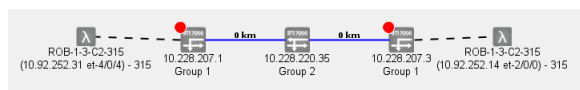



2. To see an optical service in its own panel, select it in the Network tree under the Optical branch.

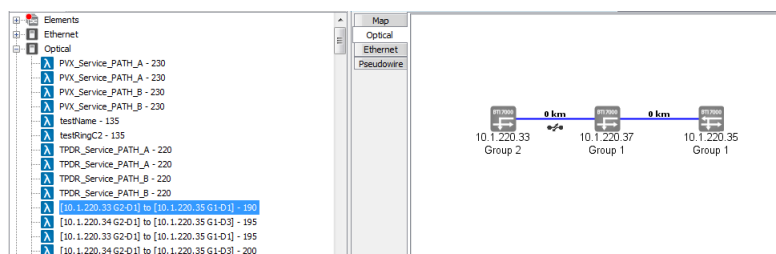


PSM displays the network elements that this service spans along with the service endpoints indicating the endpoint ports and wavelength.

If the service endpoint has a Remote ID configured, the Remote ID is shown in parentheses.



If the service includes a split ROADM node, the link connecting the two network elements comprising the ROADM node is shown with a  icon. For example, in the following figure, 10.1.220.33 and 10.1.220.37 are both part of a single ROADM node, with each NE providing a degree:



For more information on how PSM recognizes split ROADM nodes on BT17000 network elements, see [“Configuring a Split ROADM Node” on page 176](#).

For more information on how PSM recognizes split ROADM nodes on BT17800 network elements, see [“Adding a Fiber Connection on a ROADM or an ILA Client Port” on page 227](#).

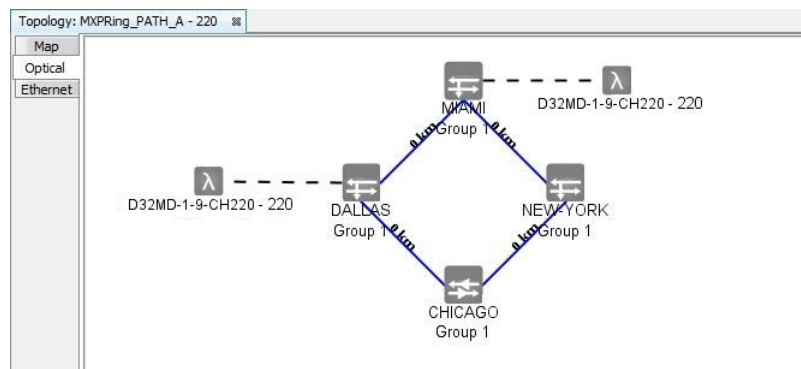


**NOTE:** If this is your first time visualizing this service, you will see the administratively-defined default layout if it exists. If a default layout does not exist for this service, then you will see the layout that PSM automatically generates. See 13.

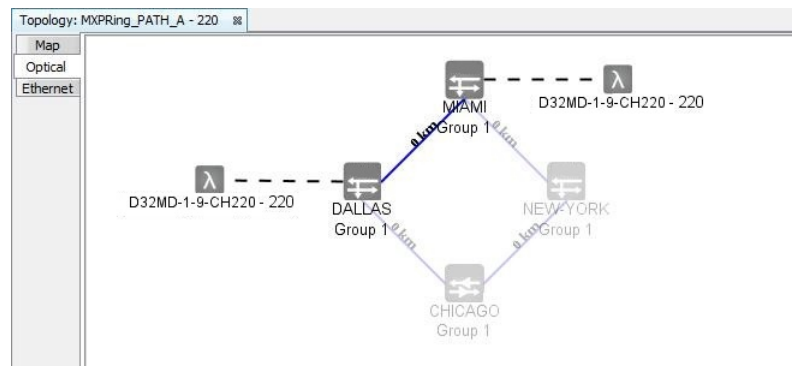


**NOTE:** If this is your second or subsequent time visualizing this service, you will see the layout that existed when you last exited this service view.

3. To see a complete service view, right-click the background and select **Show All Topology**.



4. To see a service path:
  - a. Right-click the endpoint and select **Highlight Service**.



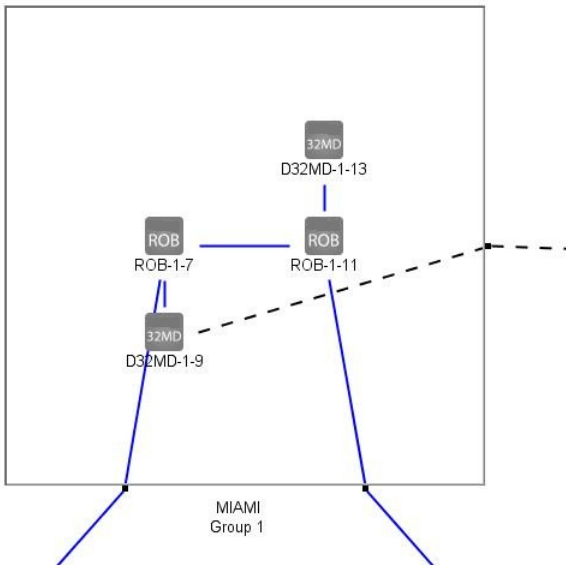
Only groups that are part of the service are highlighted.

- b. To clear the highlighting, right-click the background and select **Clear Highlighting**.
5. To see the optical port or interface associated with the service endpoint, right-click the endpoint and select **Navigate > Optical Port** or **Navigate > Interface**.

The optical port or interface associated with the endpoint is highlighted in the Network tree.

6. To see the physical equipment in a group, double-click the optical group icon:

The physical equipment and connections within the group are shown in a zoomed-in view.

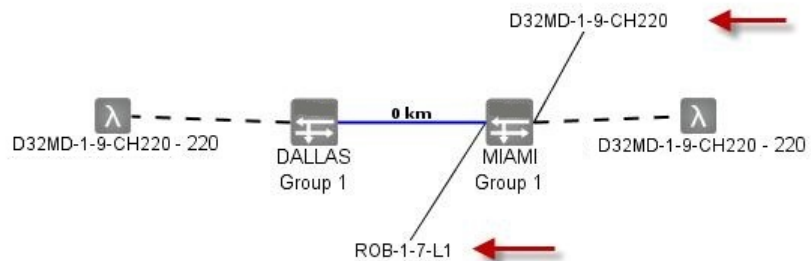


7. To change the size of the service view:
  - a. Right-click the background and select **Zoom In** to increase the view size
  - b. Right-click the background and select **Zoom Out** to decrease the view size
  - c. Right-click the background and select **Reset Zoom** to return the view size to its original size

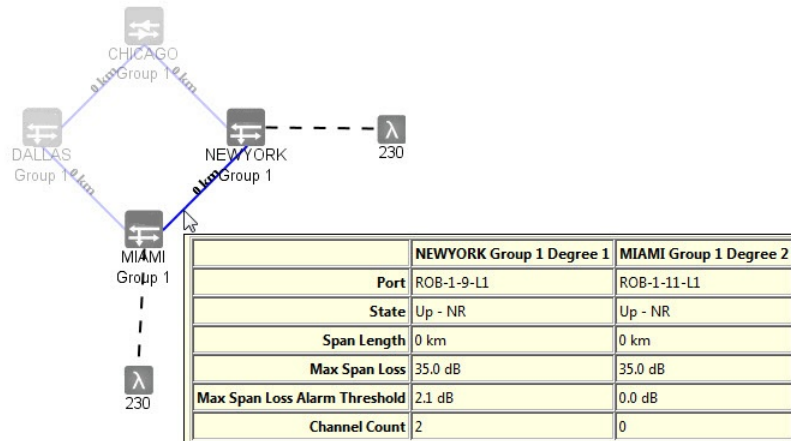
Alternatively, you can use your mouse scroll wheel.

8. To show port labels:

- a. Select an optical group icon. Right-click and choose **Show Port Labels**.



- b. Right-click and clear **Show Port Labels** to hide port labels.
9. To see details on a link, hover over the link.



10. Right-click a network element and select **Network Element** to see the regular NE menu options.
11. To move elements in this view, drag elements to the desired location.
12. To move all of the ports and switches in the service, choose **Select All** and drag the service within the window.
13. You can save the current layout as the default, or revert to the default, or revert to the layout that PSM automatically generates.
  - a. To save the current layout as the default layout for this service, right-click the background and select **Save Layout as Default**.



**NOTE:** You must have administrator privileges to execute this command.

Once the current layout is saved as the default, subsequent users who visualize this service will be able to see the current layout.

- b. To reset the current layout to the default, right-click the background and select **Reset Layout to Default**.
- c. To reset the current layout to the layout that PSM automatically generates, right-click the background and select **Reset Layout**.
14. To save the service screen view as an image:

- a. Select **Save Service Image**.

The **Save Service Image** dialog appears.

- b. Navigate to the desired folder and enter the filename.

The default file format is png. To save the file in jpg format, enter .jpg at the end of the filename.

- c. Click **Save**.


You have successfully completed this procedure.

## Activating an Optical Service in a BTI7000 Network

- [Activating an Optical Service Between BTI7000 Optical Port Endpoints on page 306](#)
- [Activating an Optical Service Between Transponder Interface Endpoints on page 308](#)
- [Examples Of Path Selection in a BTI7000 Optical Network on page 316](#)

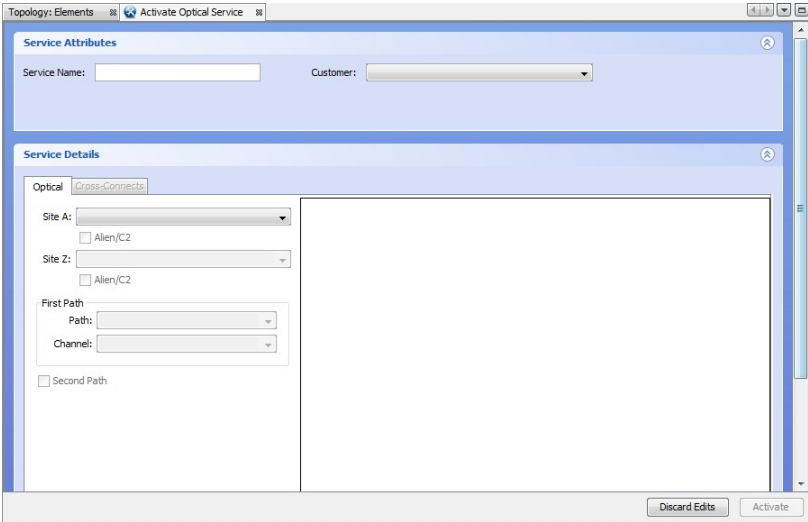
### Activating an Optical Service Between BTI7000 Optical Port Endpoints

Use this procedure to configure and activate an optical service between BTI7000 optical ports across a BTI7000 network. The BTI7000 optical network is called the BTI7000 Series Dynamic Optical Layer (DOL).

1. Select **Tools >Service Activation >Optical >Ports**. Alternatively, click the **Service Activation**  button on the toolbar, and select **Optical >Ports**.

Optical ports service activation is used when the specified endpoints are ports on optical equipment, such as a service between BTI7000 DOL endpoints.

The Activate Optical Service panel opens.



2. In the Service tab, enter the required information as described in the following table.

Table 34: Fields in the Activate Optical Service Dialog

Field	Description	Required field?
Service Name	User-defined name that uniquely identifies the service.	Yes
Customer	Select from the drop-down list. To add a customer to the list, select Edit>Add Customer from the main menu. For more information on adding customers, see <i>Adding a Customer</i> .	Optional
Site A	Choose from a drop-down menu of existing sites.	Yes
Site Z	Choose from a drop-down menu of existing sites.	Yes
Alien/C2	When selected, the service is not provisioned to add or drop on the multiplexer/demultiplexer, but on the Alien/C2 port of the ROADM module.  <b>NOTE:</b> This option is not available for selection in a split ROADM node. In a split ROADM node, the Alien/C2 interface is used to connect the ROADM modules together and cannot be configured for Add/Drop wavelengths.	Optional
Path	Choose from a drop-down list of possible paths from Site A to Site Z. Each path has the following format:  <div style="text-align: center;"> <code>&lt;Site A&gt; to &lt;Site Z&gt; [via &lt;Site N1&gt;[; &lt;Site N2&gt;[;...]]]</code> </div> where <code>&lt;Site Nx&gt;</code> represents a decision point for a ROADM with more than two degrees. Each decision point specifies the incoming and outgoing degrees for the path through that NE. See "Examples Of Path Selection in a BT17000 Optical Network" on page 316 .  <b>NOTE:</b> By default, the maximum number of spans that a path can have is 10. If your path requires more than 10 spans, contact Juniper Networks Support to increase this limit.	Yes
Channel	Choose from a drop-down list of existing channels.	Yes
Second Path	When selected, the Path and Channel for the protected path can be specified. This selection is greyed out if no alternative path exists.	Optional

### 3. Click **Activate**.

The PSM server sends the activation request to the network element. You can monitor the status of the request through the **View > Server > Tasks** window. The new service appears in the Network tree a short while after the task completes successfully. As part of service activation, PSM creates all the necessary optical cross-connects along the path between the specified endpoints.

You must wait for the activation tasks to complete before performing any other operation on the NEs affected by this activation.

You have successfully completed this procedure.

### Activating an Optical Service Between Transponder Interface Endpoints

Use this procedure to set up a BTI7000 optical service between transponder interfaces residing on BTI7800 Series network elements, MX Series or PTX Series routers, or QFX Series switches.

This procedure creates a new service that can be viewed in PSM as either a transport service or an optical service. The transport service component shows the transponder endpoints connected across the transport network. The optical service component shows the underlying optical network between the multiplexer/demultiplexer endpoints.

#### Prerequisites:

- The BTI7000 optical network must be set up and an optical channel (wavelength) must be available between the two endpoints across the network.
- If an interface endpoint is on an MX Series or PTX Series router or QFX Series switch, the interface endpoint must already exist. You cannot use PSM to create an interface endpoint on a router or switch.
- The interface endpoints must be configured properly with the same modulation, FEC, and line encoding, and use the same wavelength. To configure an interface on a BTI7800 UFM, see [“Editing an Interface” on page 205](#). To configure an interface on an MX Series or PTX Series router or QFX Series switch using PSM, see [“Editing an Interface” on page 258](#).

Table 35 on page 308 shows the optical service endpoint pairings that PSM supports.



**NOTE:** PSM does not perform compatibility validation of the interface endpoints prior to service activation other than to ensure that the endpoints are allowed according to [Table 35 on page 308](#) and that the wavelengths configured at both interface endpoints are the same.

If you configure the interface endpoints to have incompatible modulation schemes or FEC settings, PSM will set up the optical service but will not be able to set up the transport service. PSM will show the unsuccessful transport service as semi-stranded (with incompatible endpoints). This is no different than if you were to connect the misconfigured endpoints together directly instead of through an optical network.

**Table 35: Supported Interface Endpoints for the BTI7000 Optical Service**

Site A (interface)	Site Z (interface)	Notes
BTI7800 UFM <i>otu4</i>	BTI7800 UFM <i>otu4</i>	Site A and Site Z are interfaces on the UFM3 and UFM4.
BTI7800 UFM <i>100ge</i>	BTI7800 UFM <i>100ge</i>	Site A and Site Z are interfaces on the UFM3.
BTI7800 UFM6 <i>och</i>	BTI7800 UFM6 <i>och</i>	Site A and Site Z are line interfaces on the UFM6.



Table 35: Supported Interface Endpoints for the BT17000 Optical Service (continued)

Site A (interface)	Site Z (interface)	Notes
MX Series or PTX Series <i>et</i>	MX Series or PTX Series <i>et</i>	<p>Site A and Site Z are interfaces on the following:</p> <p>MX Series router:</p> <ul style="list-style-type: none"> <li>100-Gigabit DWDM OTN MIC with CFP2-ACO (MIC3-100G-DWDM)</li> <li>100-Gigabit Ethernet MIC with CFP2 (MIC6-100G-CFP2 ) with a CFP2-DCO</li> <li>2x100GE + 4x10GE MPC5E (MPC5E-100G10G) with a CFP2-DCO</li> </ul> <p>PTX Series router:</p> <ul style="list-style-type: none"> <li>100-Gigabit DWDM OTN PIC with CFP2-ACO (PTX-5-100G-WDM)</li> <li>100-Gigabit Ethernet OTN PIC with CFP2 (P2-100GE-OTN) with CFP2-DCO</li> </ul>
MX Series <i>xe</i>	MX Series <i>xe</i>	<p>Site A and Site Z are 10GE interfaces on the following MPCs on an MX Series router:</p> <ul style="list-style-type: none"> <li>6x40GE + 24x10GE MPC5E (MPC5E-40G10G)</li> <li>6x40GE + 24x10GE MPC5EQ (MPC5EQ-40G10G)</li> <li>2x100GE + 4x10GE MPC5E (MPC5E-100G10G)</li> <li>2x100GE + 4x10GE MPC5EQ (MPC5EQ-100G10G)</li> </ul>
QFX Series <i>ot</i>	QFX Series <i>ot</i>	Site A and Site Z are line interfaces on the QFX10K DWDM 1.2T Line Card (QFX10K-12C-DWDM) on a QFX series switch.
BT17800 UFM6 <i>och</i>	QFX Series <i>ot</i>	<p>Site A is a line interface on the UFM6.</p> <p>Site Z is a line interface on the QFX10K DWDM 1.2T Line Card (QFX10K-12C-DWDM) on a QFX series switch.</p>
BT17800 UFM6 <i>och</i>	BT17800 UFM <i>otu4</i>	<p>Site A is a line interface on the UFM6.</p> <p>Site Z is an interface on the UFM3 or UFM4.</p>

Table 35: Supported Interface Endpoints for the BTI7000 Optical Service (continued)

Site A (interface)	Site Z (interface)	Notes
BTI7800 UFM6 <i>och</i>	MX Series or PTX Series <i>et</i>	<p>Site A is a line interface on the UFM6.</p> <p>Site Z is an interface on the following:</p> <p>MX Series router:</p> <ul style="list-style-type: none"> <li>• 100-Gigabit DWDM OTN MIC with CFP2-ACO (MIC3-100G-DWDM)</li> <li>• 100-Gigabit Ethernet MIC with CFP2 (MIC6-100G-CFP2 ) with a CFP2-DCO</li> <li>• 2x100GE + 4x10GE MPC5E (MPC5E-100G10G) with a CFP2-DCO</li> </ul> <p>PTX Series router:</p> <ul style="list-style-type: none"> <li>• 100-Gigabit DWDM OTN PIC with CFP2-ACO (PTX-5-100G-WDM)</li> <li>• 100-Gigabit Ethernet OTN PIC with CFP2 (P2-100GE-OTN) with CFP2-DCO</li> </ul>
BTI7800 UFM <i>otu4</i>	MX Series or PTX Series <i>et</i>	<p>Site A is an interface on the UFM3.</p> <p>Site Z is an interface on the following:</p> <p>MX Series router:</p> <ul style="list-style-type: none"> <li>• 100-Gigabit DWDM OTN MIC with CFP2-ACO (MIC3-100G-DWDM)</li> <li>• 100-Gigabit Ethernet MIC with CFP2 (MIC6-100G-CFP2 ) with a CFP2-DCO</li> <li>• 2x100GE + 4x10GE MPC5E (MPC5E-100G10G) with a CFP2-DCO</li> </ul> <p>PTX Series router:</p> <ul style="list-style-type: none"> <li>• 100-Gigabit DWDM OTN PIC with CFP2-ACO (PTX-5-100G-WDM)</li> <li>• 100-Gigabit Ethernet OTN PIC with CFP2 (P2-100GE-OTN) with CFP2-DCO</li> </ul>
QFX Series <i>ot</i>	BTI7800 UFM <i>otu4</i>	<p>Site A is a line interface on the QFX10K DWDM 1.2T Line Card (QFX10K-12C-DWDM) on a QFX series switch.</p> <p>Site Z is an interface on the UFM3 or UFM4.</p>

Table 35: Supported Interface Endpoints for the BTI7000 Optical Service (continued)

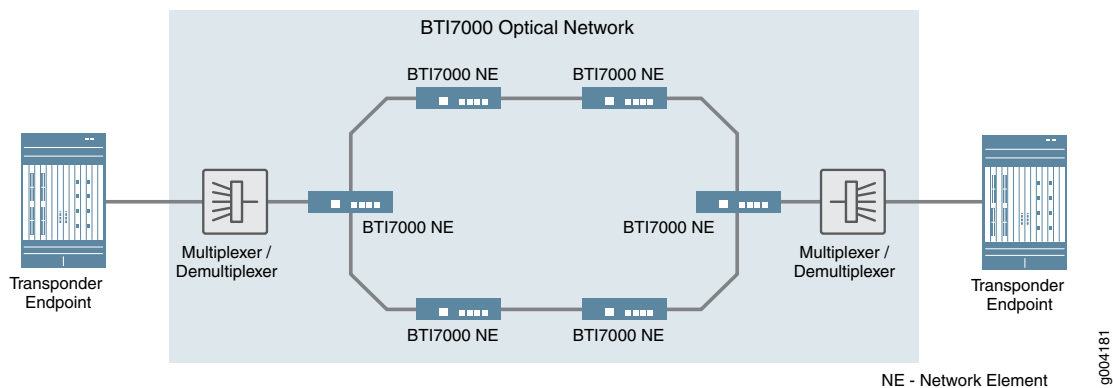
Site A (interface)	Site Z (interface)	Notes
QFX Series <i>ot</i>	MX Series or PTX Series <i>et</i>	<p>Site A is a line interface on the QFX10K DWDM 1.2T Line Card (QFX10K-12C-DWDM) on a QFX series switch.</p> <p>Site Z is an interface on the following:</p> <p>MX Series router:</p> <ul style="list-style-type: none"> <li>• 100-Gigabit DWDM OTN MIC with CFP2-ACO (MIC3-100G-DWDM)</li> <li>• 100-Gigabit Ethernet MIC with CFP2 (MIC6-100G-CFP2 ) with a CFP2-DCO</li> <li>• 2x100GE + 4x10GE MPC5E (MPC5E-100G10G) with a CFP2-DCO</li> </ul> <p>PTX Series router:</p> <ul style="list-style-type: none"> <li>• 100-Gigabit DWDM OTN PIC with CFP2-ACO (PTX-5-100G-WDM)</li> <li>• 100-Gigabit Ethernet OTN PIC with CFP2 (P2-100GE-OTN) with CFP2-DCO</li> </ul>



**NOTE:** The Site A and Site Z designations in the table above are used only to distinguish between the two interface endpoints. They are assigned arbitrarily and are interchangeable.

Figure 66 on page 312 shows devices with transponder interfaces connected across a BTI7000 optical network. The transponder interfaces attach to the optical network through a port on a BTI Series multiplexer/demultiplexer. Each port on the multiplexer/demultiplexer is associated with a different wavelength. Therefore, the attachment point on the multiplexer/demultiplexer determines the optical channel to use through the network.

Figure 66: Optical Service Between Transponder Endpoints



**NOTE:** The connection between the multiplexer/demultiplexer port and the locally-attached interface must be manually configured. This connection is not automatically learned. See step 1.

Alternatively, you can activate an optical service where one or both router endpoints connect to the C2 port of a BTI7000 DOL ROADM module. This is not shown. In this situation, because the C2 port is not associated with a specific wavelength, PSM can only activate this type of service if it can determine the desired wavelength. PSM can determine the desired wavelength if the device interface endpoint has a configured wavelength or if the other service endpoint is connected to a multiplexer/demultiplexer. For more information on this special configuration, contact Juniper Networks Support.

1. Before you can activate this service, you must configure the actual connection between the multiplexer/demultiplexer port and the locally-attached interface endpoint if you have not already done so.

This is performed by configuring the Remote ID on the respective multiplexer/demultiplexer port. For information on how to do this, see [“Setting the Remote ID on a Multiplexer/Demultiplexer” on page 80](#).



**NOTE:** Each port on the multiplexer/demultiplexer is associated with a specific wavelength. The multiplexer/demultiplexer port on which you configure the Remote ID must be at the same wavelength as the interface endpoint to which it is connected.

For example, this configures the Remote ID on channel 570 (195.70 THz) on the multiplexer/demultiplexer to point to a locally-attached BT17800 UFM interface at 10.228.220.104, slot 2, subslot 1, port 1. Note that the UFM interface must also be configured for the 195.70 THz frequency.

Provision Remote ID on Port D96MD-0-1-Channel: 570

**Local Port ID**

10.228.207.3-D96MD-0-1-Channel: 570

**Far End**

Remote Id: 10.228.220.104-OTU4-1-2-1-1

Clear Reset

Edit

Hostname/IP Address: 10.228.220.104

CP Type: OTU4

Shelf: 1

Slot: 2

BIC: 1

Port: 1

Alien: ☐

Bidirectional: ☐

Cancel OK

The following example configures the Remote ID on channel 185 (191.85 THz) on the multiplexer/demultiplexer to point to a locally-attached router interface at 192.168.7.50, slot 1, MIC 0, port 0. Note that the interface must also be configured for the 191.85 THz frequency.

**Provision Remote ID on Port D96MD-0-1-Channel: 185**

**Local Port ID**

10.228.207.1-D96MD-0-1-Channel: 185

**Far End**

Remote Id: 192.168.7.50-JUNOS-1-0-0

Clear Reset

Edit

Hostname/IP Address: 192.168.7.50

CP Type: JUNOS

FPC: 1

PIC/MIC: 0

Port: 0

Alien: ☐

Bidirectional: ☐


Cancel OK

Click **OK**. The PSM server sends the configuration request to the network element. You can monitor the status of the request through the **View > Server > Tasks** window.

2. Repeat step 1 to configure the connection between the other multiplexer/demultiplexer and the other router. You must use the same channel number.
3. Verify that the Remote ID configuration has taken effect.

Right-click the multiplexer/demultiplexer port/channel at each end and select **Remote ID > Edit** and confirm that the settings are correct in the resulting **Provision Remote Port ID** dialog. Do not proceed to the next step until the Remote IDs are correct at both ends.

4. Create the service.

Select **Tools > Service Activation > Optical > Interfaces**. Alternatively, click the **Service Activation**  button on the toolbar, and select **Optical > Interfaces**.

Optical interfaces service activation is used when the specified endpoints are interfaces that connect to the optical network, such as a service between transponder interface endpoints across a BT17000 DOL network.

The **Activate Optical Service** panel appears.

The screenshot shows a web interface with two main panels. The top panel, titled 'Service Attributes', contains a 'Service Name' text input field and a 'Customer' dropdown menu. The bottom panel, titled 'Service Details', has a tabbed interface with the 'Optical' tab selected. Under the 'Optical' tab, there are three sections: 'Site A' with a dropdown menu and a blue button, 'Site Z' with a dropdown menu and a grey button, and 'Path' with a 'Selected:' dropdown menu. To the right of these fields is a large empty rectangular area.

5. In the **Optical** tab, enter the required information as described in the following table.

**Table 36: Fields in the Activate Optical Service Panel**

Field	Description	Required field?
Service Name	User-defined name that uniquely identifies the service.	Yes
Customer	Select from the drop-down list. To add a customer to the list, select Edit>Add Customer from the main menu. For more information on adding customers, see <i>Adding a Customer</i> .	Optional
Site A	Choose the interface endpoint from the drop-down menu. The drop-down menu lists all possible endpoints. It does not matter which end you choose as Site A.	Yes
Site Z	Choose the other interface endpoint from the drop-down menu. The drop-down menu lists all possible endpoints for Site A. PSM creates this list based on the Remote ID configurations and the availability and compatibility of Site Z.	Yes
Path	Choose from a drop-down list of possible paths from Site A to Site Z. Depending on the optical network topology, there might be more than one path through the network.  <b>NOTE:</b> By default, the maximum number of spans that a path can have is 10. If your path requires more than 10 spans, contact Juniper Networks Support to increase this limit.	Yes

6. Click **Activate**.

The PSM server sends the activation request to the device. You can monitor the status of the request through the **View > Server > Tasks** window. The new service appears in the Network tree a short while after the task completes successfully. As part of service activation, PSM creates all the necessary optical cross-connects along the path between the specified endpoints.

You must wait for the activation tasks to complete before performing any other operation on the NEs affected by this activation.



**NOTE:** This procedure creates a new service that can be viewed in PSM as either a transport service or an optical service. The transport service component shows the transponder endpoints connected across the transport network. The optical service component shows the underlying optical network between the multiplexer/demultiplexer endpoints. For information on how to view these services, see [“Visualizing a Transport Service” on page 324](#) and [“Visualizing an Optical Service” on page 301](#) respectively.



**NOTE:** If an optical service already exists between the multiplexer/demultiplexer ports and you subsequently configure the Remote IDs on those ports, then PSM automatically creates the accompanying transport service.

---

### Examples Of Path Selection in a BTI7000 Optical Network

---

When you activate an optical service, you need to select the first (primary) path and channel, and optionally the second (protected) path and channel between the service endpoints. All paths and channels are selected from drop-down menus in the **Activate Optical Service** dialog. The drop-down menus list all the valid possibilities. A second path can only be selected if an alternative path exists. Otherwise the **Second Path** check box is greyed out and cannot be selected.

The path itself might contain decision points. A decision point refers to the decision that needs to be made when traversing ROADMs with more than 2 degrees. When more than 2 degrees exist, there can be multiple outgoing degrees for each incoming degree. The decision point qualifies the path by specifying the incoming and outgoing degrees through these nodes.

#### **Selecting Paths and Channels**

[Figure 67 on page 317](#) shows the selection of the first path and channel for a service between NEW-YORK and MIAMI. The topology is a ring with 2-degree ROADMs in NEW-YORK, MIAMI, and DALLAS, and a line amplifier node in CHICAGO. The first path is chosen to be the shortest path around the ring.



Figure 67: Selecting the First Path and Channel

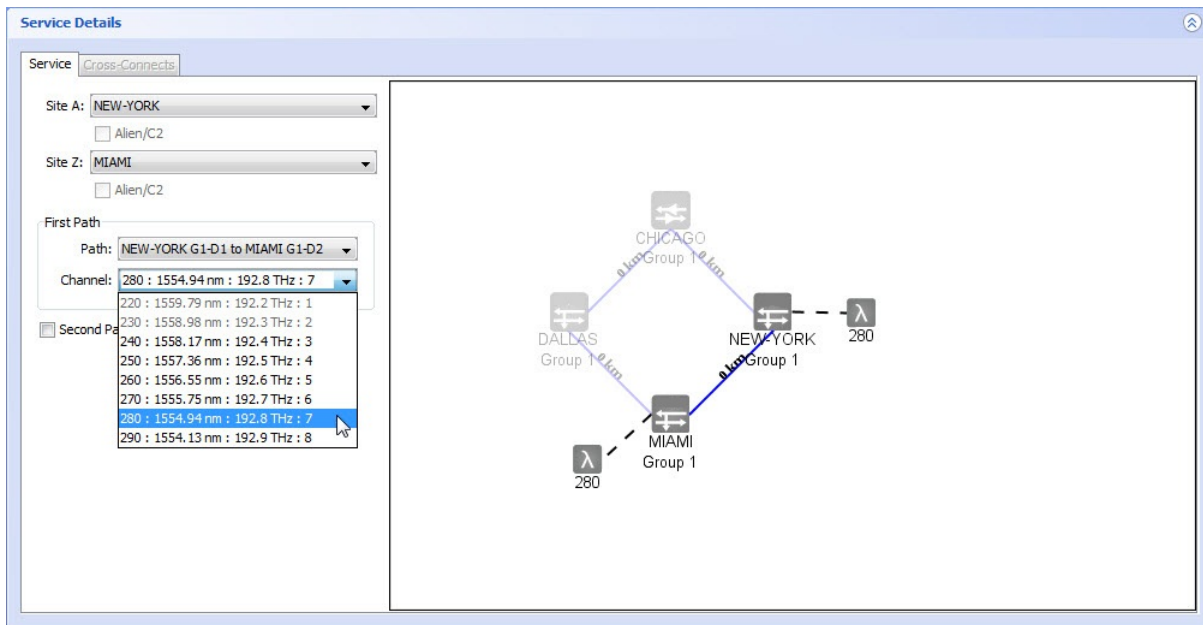
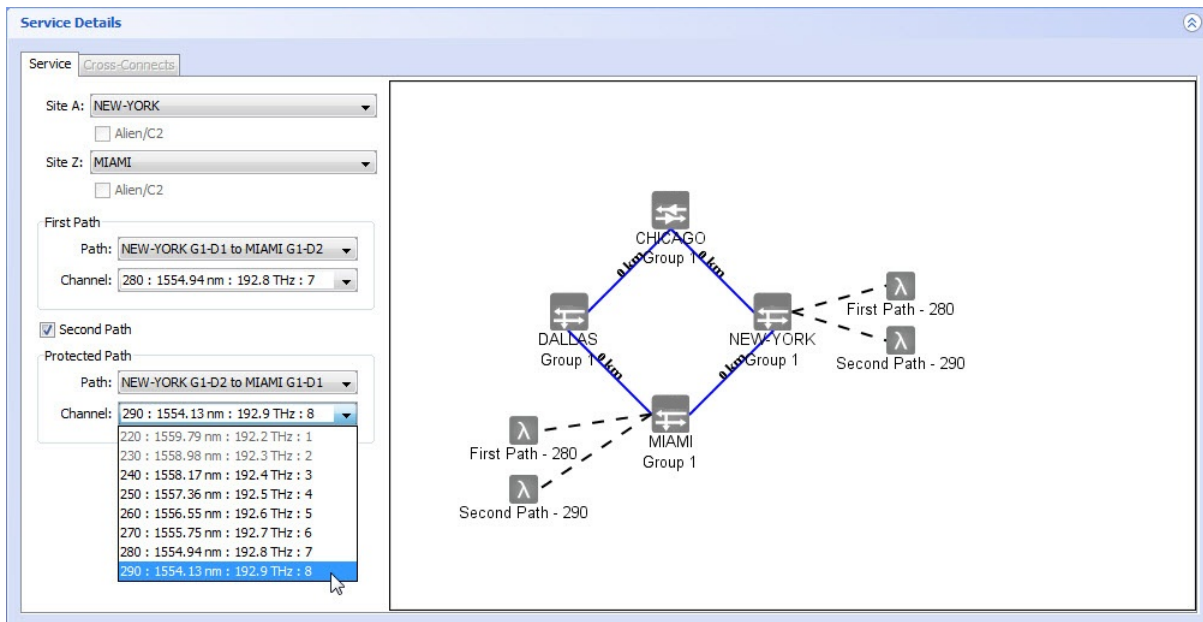


Figure 68 on page 317 shows the selection of the second path and channel. In this topology, a second path is possible via CHICAGO and DALLAS.

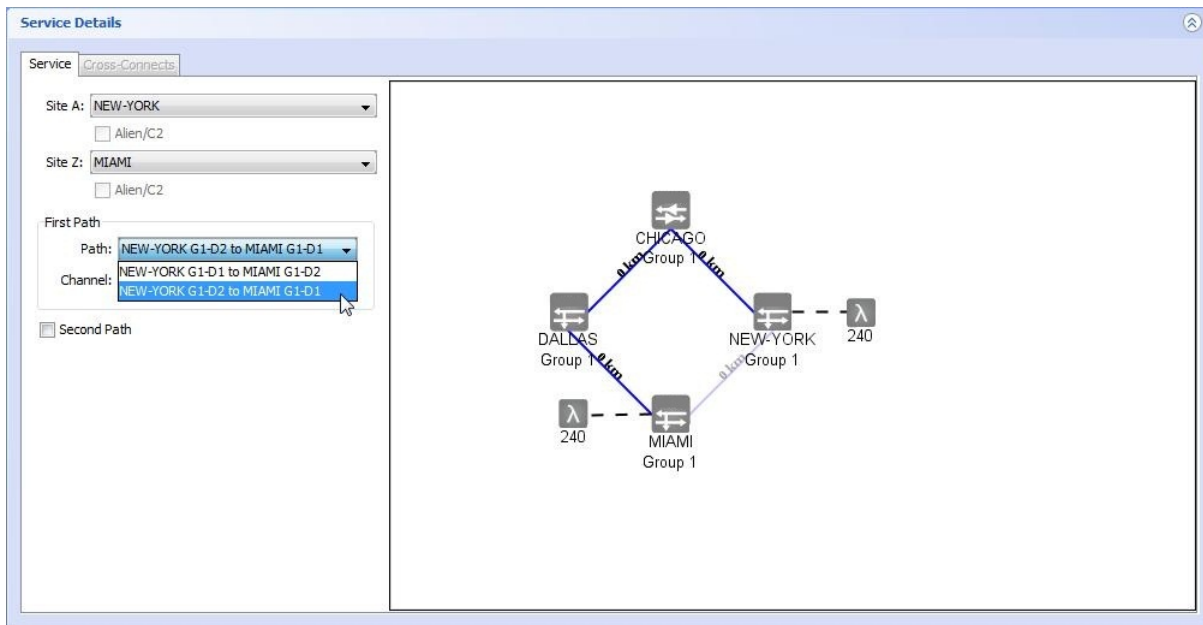
Figure 68: Selecting the Second Path and Channel



### Selecting a Path with No Decision Points

Figure 69 on page 318 shows the selection of a path with no decision points. The topology is a ring with 2-degree ROADMs in NEW-YORK, MIAMI, and DALLAS, and a line amplifier node in CHICAGO. The path merely specifies the start and end points.

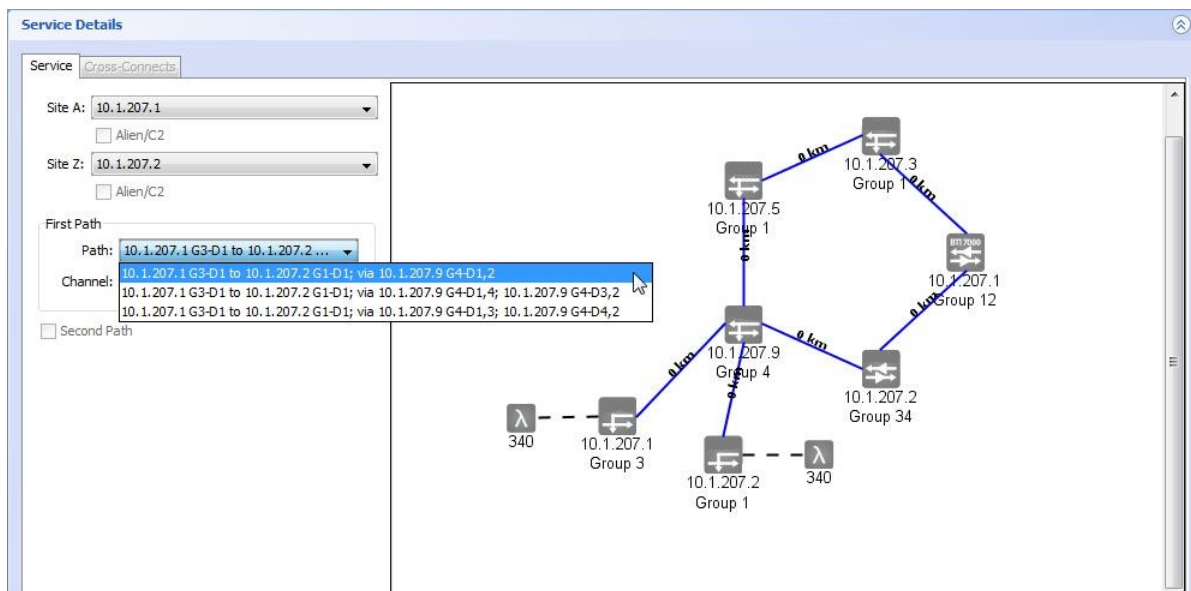
Figure 69: Selecting a Path with No Decision Points



### Selecting a Path with One Decision Point

Figure 70 on page 318 shows the selection of a path with one decision point. A 4-degree ROADM is at 10.1.207.9 while the other sites contain 2-degree ROADMs. The decision point is at 10.1.207.9 going from degree 1 to degree 2, representing the most direct path between 10.1.207.1 and 10.1.207.2.

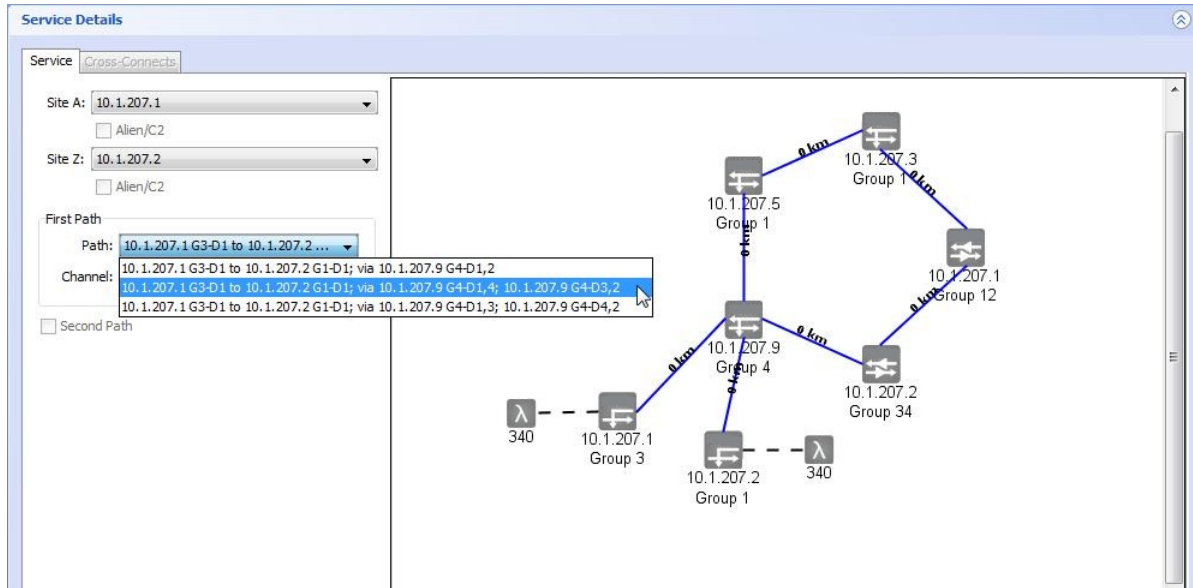
Figure 70: Selecting a Path with One Decision Point



### Selecting a Path with Two Decision Points

Figure 71 on page 319 shows the selection of a path with two decision points. The first decision point is at 10.1.207.9 going from degree 1 to degree 4 traversing the ring in one direction, and the second decision point is at 10.1.207.9 going from degree 3 to degree 2, re-entering the 4-degree ROADM from the other side of the ring.

Figure 71: Selecting a Path with Two Decision Points



### Activating an Optical Service in a BTI7800 Network

Use this procedure to configure and activate an optical service on a BTI7800 network.

#### Prerequisites

- All required intra-node fiber connections are created. These are the fiber connections that connect the endpoint to the ROADM module and between ROADM modules.
- All required inter-node fibers are physically connected. These are the line span fibers that connect ROADM nodes together.
- All required line port optical channels are created on all nodes that the service traverses.

1. Select **Tools >Service Activation >Optical >Interfaces**. Alternatively, click the **Service Activation** button on the toolbar, and select **Optical >Interfaces**.

Optical interfaces service activation is used when the specified endpoints are interfaces that connect to the optical network, such as a service between UFM interface endpoints across a BTI7800 Series optical network.

The Activate Optical Service panel appears.

The screenshot shows two panels. The top panel, 'Service Attributes', has a 'Service Name' text box and a 'Customer' dropdown menu. The bottom panel, 'Service Details', has a tabbed interface with 'Optical' selected. Under the 'Optical' tab, there are three sections: 'Site A' with a dropdown and a blue icon, 'Site Z' with a dropdown and a grey icon, and 'Path' with a 'Selected:' dropdown menu.

2. In the **Optical** tab, enter the required information as described in the following table.

**Table 37: Fields in the Activate Optical Service Panel**

Field	Description	Required field?
Service Name	User-defined name that uniquely identifies the service.	Yes
Customer	Select from the drop-down list. To add a customer to the list, select Edit>Add Customer from the main menu. For more information on adding customers, see <i>Adding a Customer</i> .	Optional
Site A	<p>Choose from a drop-down menu of existing sites and channels. PSM provides a list of all possible endpoints. The Site A endpoint can be an interface on a UFM or, if configuring an alien wavelength, an optical channel on a ROADM client port.</p> <p>An alien wavelength is a wavelength that is added and dropped to a local external endpoint. The external endpoint can be on a UFM on a different BT17800, or on other vendors' equipment. Since the endpoint is external and beyond the management of PSM, the endpoint you select for an alien wavelength is an optical channel on the ROADM client port.</p>	Yes
Site Z	<p>Choose from a drop-down menu of existing sites and channels. PSM provides a list of all possible endpoints that can be reached from Site A. PSM creates this list based on the fiber connections and the existence and availability of the optical channel from Site A all along the path to Site Z.</p> <p>The Site Z endpoint can be an interface on a UFM or, if the endpoint is external (alien wavelength), an optical channel on a ROADM client port.</p>	Yes
Path	<p>Choose from a drop-down list of possible paths from Site A to Site Z.</p> <p><b>NOTE:</b> By default, the maximum number of spans that a path can have is 10. If your path requires more than 10 spans, contact Juniper Networks Support to increase this limit.</p>	Yes

3. Click **Activate**.

The PSM server sends the activation request to the network element. You can monitor the status of the request through the **View > Server > Tasks** window. The new service appears in the Network tree a short while after the task completes successfully. As

part of service activation, PSM creates all the necessary optical cross-connects along the path between the specified endpoints.

## Viewing the Cross-Connects in an Optical Service

Use this procedure to view the cross-connects in an activated optical service.

1. In the Network tree, double-click the service you want to view. Alternatively, select the service, right-click and choose **View**.

The Service Attributes window opens.

2. Click on the **Cross Connects** tab to see the cross-connects that make up the service on all network elements .

## Updating an Optical Service

Use this procedure to change the service name and customer of an activated optical service.

1. On the Network tree, double-click the service you want to update. Alternatively, select the service, right-click and choose **View**.

The Service Attributes window opens.

2. Modify the Customer or Service Name.

3. Click **Apply**.

The optical service is updated. If you update an optical service that is supporting a transport service with BT17800, MX Series , PTX Series, or QFX Series endpoints, the transport service is updated implicitly.

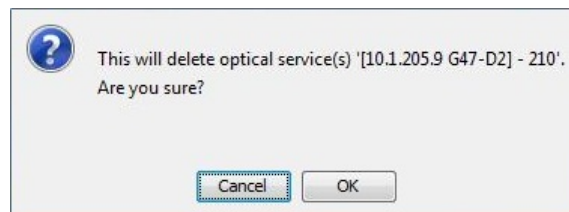
## Deleting an Optical Service

Use this procedure to delete an optical service.

When a service is deleted, the associated modules and ports remain in the UP state.

1. In the Network tree, right-click an optical service and choose **Delete**.

An information window opens asking for confirmation.



2. Click **OK**.

The optical service is deleted from the network elements and the PSM server. If you delete an optical service that is supporting a transport service with BT17800, MX Series, PTX Series, or QFX Series endpoints, the transport service is deleted implicitly.

## Viewing the Optical Services Table

You can view a list of the optical services with information such as Customer, Service Name, Channel, Site A, Site Z, End-To-End State, Intermediate Nodes, and more.

1. To view the optical services table, from the main menu choose **View > Optical > Services**.

The Optical Services tab is displayed.

Topology: Network Element Groups						
Optical Services						
Customer	Service Name	Channel	Site A	Site Z	End-To-End State	Intermediate Nodes
BT1	VideoRing_PATH_A	230	NEW-YORK G1-D1	MIAMI G1-D2	Up	
BT1	MXPRing_PATH_B	220	DALLAS G1-D1	MIAMI G1-D2	Up	CHICAGO G1-D2, CHICAGO G1-D1,...
BT1	MXPRing_PATH_A	220	DALLAS G1-D2	MIAMI G1-D1	Up	
BT1		260	10.1.207.5 G1-D1	10.1.207.5 G...	Up	10.1.207.3 G1-D2, 10.1.207.3 G1-...
BT1	VideoRing_PATH_B	230	MIAMI G1-D1	NEW-YORK G...	Up	DALLAS G1-D2, DALLAS G1-D1, CHI...
BT1		220	10.1.207.5 G1-D1	10.1.207.5 G...	Up	10.1.207.3 G1-D2, 10.1.207.3 G1-...



**NOTE:** To apply filters to this table, see “Working with Optical/Transport Services and Topology Tables” on page 334

2. Use the scroll bar on the right side of the window to scroll through the list of services.

## Viewing the Optical Services Per Span Table

You can view a list of the optical services per span with information such as Span Source, Span Far-End, Channel, Service Name, Customer Name, Service Site A, Service Site Z, Source Port State, Source Port Admin State, Far-End Port State, Far-End Port Admin State information, and more.

1. To view the optical services per span table, from the main menu choose **View > Optical > Services per Span**.

The Optical Services per Span tab is displayed.

Topology: Network Element Groups									
Optical Services per Span									
Span Source	Span Far-End	Channel	Service Name	Service Site A	Service Site Z	Source...	Source Por...	Far-End ...	Far-End ...
CHICAGO G1-D1	NEW-YORK G1-D2	230	VideoRing_PATH_B	MIAMI G1-D1	NEW-YORK G1-D2	Up - NR	In-Service (IS)	Up - NR	In-Service (...)
DALLAS G1-D1	CHICAGO G1-D2	230	VideoRing_PATH_B	MIAMI G1-D1	NEW-YORK G1-D2	Up - NR	In-Service (IS)	Up - NR	In-Service (...)
MIAMI G1-D1	DALLAS G1-D2	230	VideoRing_PATH_B	MIAMI G1-D1	NEW-YORK G1-D2	Up - NR	In-Service (IS)	Up - NR	In-Service (...)
NEW-YORK G1-D1	MIAMI G1-D2	230	VideoRing_PATH_A	NEW-YORK G...	MIAMI G1-D2	Up - NR	In-Service (IS)	Up - NR	In-Service (...)
CHICAGO G1-D1	NEW-YORK G1-D2	220	MXPRing_PATH_B	DALLAS G1-D1	MIAMI G1-D2	Up - NR	In-Service (IS)	Up - NR	In-Service (...)
DALLAS G1-D1	CHICAGO G1-D2	220	MXPRing_PATH_B	DALLAS G1-D1	MIAMI G1-D2	Up - NR	In-Service (IS)	Up - NR	In-Service (...)
NEW-YORK G1-D1	MIAMI G1-D2	220	MXPRing_PATH_B	DALLAS G1-D1	MIAMI G1-D2	Up - NR	In-Service (IS)	Up - NR	In-Service (...)



**NOTE:** To apply filters to this table, see “Working with Optical/Transport Services and Topology Tables” on page 334

2. Use the scroll bar on the right side of the window to scroll through the list of services per span.

## Viewing the Optical Topology Table

You can view a table of the optical topology with information such as Source Site, Source Degree, Source Port, Far-End Site, Far-End Degree, Administrative Status, State, Span Length (km), Max. Span Loss (dB), Channel Count information, and more.

The optical topology table has a row for each end of the link (that is, for each connection shown in the topology view, there are two rows in the table). If only one end of the link is discovered, only one row is displayed. This table contains the same information shown in the tool tip, but can be manipulated with the sorting and filtering functionality available for all tables.

1. To view the optical topology table, from the main menu choose **View > Optical > Topology**.

The Optical Topology tab displays.

Topology: [10.1.207.5 G1-D1] to [10.1.207.5 G1-D2] - 220											
Source Site	Source Group/Deg...	Source Port	Far-End ...	Far-End Group/Degree	Administrative Status	State	Span Length ...	Max. Span L...	Max. Span Lo...	Channel Count	
SRN2	G1-D1	DLA-1-34.1	10.1.104.3	G44-D3	In-Service (IS)	Up - NR	0	30.0	0.0	0	
SRN2	G1-D2	DLA-1-14.1	10.1.103.6	G1-D1	In-Service (IS)	Up - NR	51	30.0	0.0	0	
NEW-YORK	G1-D1	ROB-1-94.1	MIAMI	G1-D2	In-Service (IS)	Up - NR	0	35.0	0.0	2	
NEW-YORK	G1-D2	ROB-1-154.1	CHICAGO	G1-D1	In-Service (IS)	Up - NR	0	30.0	0.0	2	
NEW-YORK	G0-D0	MWP-1-34.1				Down ~...	null			null	
NEW-YORK	G0-D0	MWP-1-3-C3				Down ~...	null			null	
MIAMI	G1-D1	ROB-1-74.1	DALLAS	G1-D2	In-Service (IS)	Up - NR	0	35.0	0.0	2	
MIAMI	G1-D2	ROB-1-114.1	NEW-YORK	G1-D1	In-Service (IS)	Up - NR	0	35.0	0.0	2	
DALLAS	G1-D1	ROB-1-134.1	CHICAGO	G1-D2	In-Service (IS)	Up - NR	0	30.0	0.0	2	
DALLAS	G1-D2	ROB-1-174.1	MIAMI	G1-D1	In-Service (IS)	Up - NR	0	35.0	0.0	2	



**NOTE:** To apply filters to this table, see [“Working with Optical/Transport Services and Topology Tables”](#) on page 334

2. Use the scroll bar on the right side of the window to scroll through the optical topology details.

## Transport Services

A transport service provides SONET/SDH, OTN, or physical Ethernet connectivity between transport service endpoints. A transport service endpoint is a client interface on transport equipment.

PSM allows you to manage transport services for BT17800 Series network elements. The service spans between UFM client interfaces through a series of cross-connects across the network.

Additionally, PSM allows you to manage the transport service component of a BTI7000 optical service that has BTI7800, MX Series or PTX Series router or QFX Series switch endpoints.

- [Visualizing a Transport Service on page 324](#)
- [Activating a Transport Service on page 328](#)
- [Updating a Transport Service on page 332](#)
- [Deleting a Transport Service on page 332](#)
- [Viewing the Transport Services Table on page 332](#)
- [Viewing the Transport Services Per Span Table on page 333](#)
- [Viewing the Transport Topology Table on page 333](#)
- [Viewing the Transponder Tuning Grid on page 334](#)

## Visualizing a Transport Service

Use this procedure to visualize a transport service in a BTI7800 network or a transport service with BTI7800, MX Series, PTX Series, or QFX Series endpoints across a BTI7000 optical network.



.....

**NOTE:** Not all transport services are explicitly created. If you create an optical service with BTI7800, MX Series, PTX Series, or QFX Series endpoints across a BTI7000 optical network, PSM automatically creates the resulting transport service between the interface endpoints. If you create an optical service across a BTI7000 optical network and subsequently configure the Remote IDs to point to supported interfaces on BTI7800, MX Series, PTX Series, or QFX Series endpoints, PSM also automatically creates the resulting transport service between the interface endpoints.

.....



1. To see a summary of a transport service, hover over the service in the Network tree under the Transport branch (Figure 72 on page 325 and Figure 73 on page 325).

Figure 72: Hovering Over a Transport Service

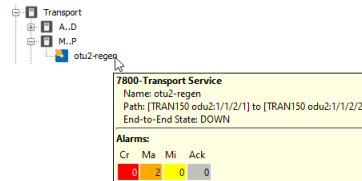
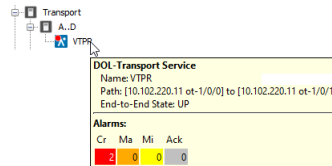
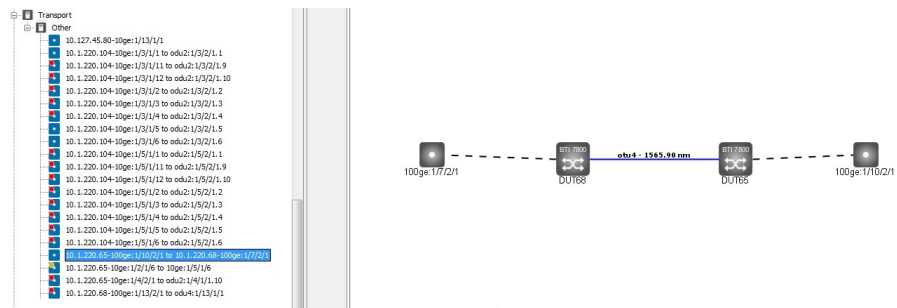


Figure 73: Hovering Over the Transport Service Component of a BT17000 Optical Service




2. To see a transport service in its own panel, select it in the Network tree under the Transport branch.



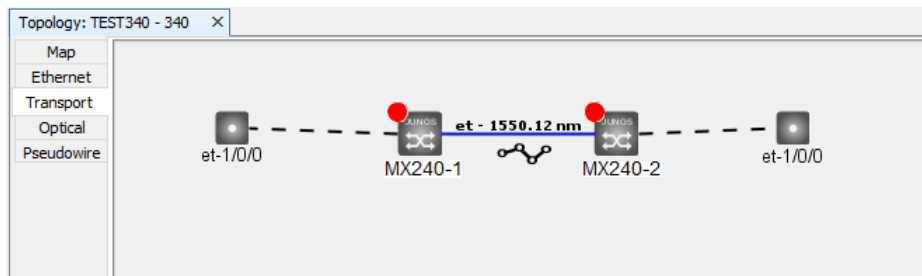
**NOTE:** If this is your first time visualizing this service, you will see the administratively-defined default layout if it exists. If a default layout does not exist for this service, then you will see the layout that PSM automatically generates. See 11.



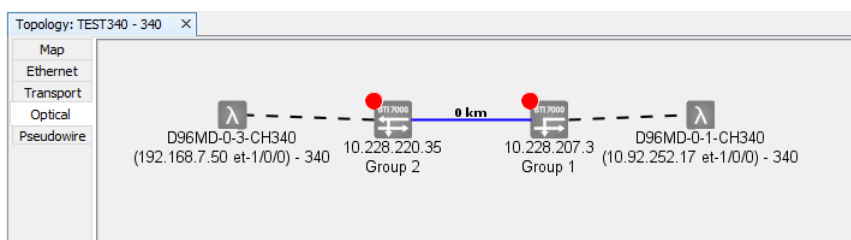
**NOTE:** If this is your second or subsequent time visualizing this service, you will see the layout that existed when you last exited this service view.

3. If a link in the transport service is running over an underlying optical service, the link is shown with a  icon. This is how the transport service component of a BT17000 optical service with transponder interface endpoints is displayed.

For example:



If you right-click the link and select **Optical Service** (or right-click the service in the Network tree and select **Navigate >Optical Service**), PSM displays the underlying optical service in the Optical service view:



To go back to the Transport service view, select the Transport tab as you normally do when you navigate between views. For more information on the Optical service view, see [“Visualizing an Optical Service” on page 301](#).

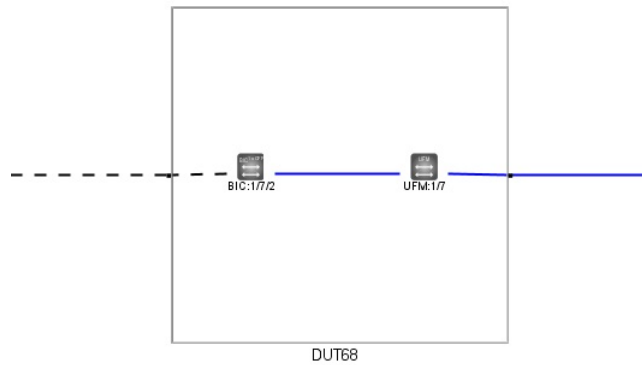
4. To see the interface associated with a service endpoint, right-click the endpoint and select **Navigate >Interface**.

The interface associated with the endpoint is highlighted in the Network tree.

5. To see details on a network element, link, or port, hover over the network element, link, or port.

6. To see the equipment on a network element, double-click the NE.

The equipment and connections are shown in a zoomed-in view.



7. To change the size of the service view:
  - a. Right-click the background and select **Zoom In** to increase the view size
  - b. Right-click the background and select **Zoom Out** to decrease the view size
  - c. Right-click the background and select **Reset Zoom** to return the view size to its original size

Alternatively, you can use your mouse scroll wheel.

8. Right-click a network element and select **Network Element** to see the regular NE menu options.
9. To move elements in this view, drag elements to the desired location.
10. To move all of the ports and switches in the service, choose **Select All** and drag the service within the window.
11. You can save the current layout as the default, or revert to the default, or revert to the layout that PSM automatically generates.
  - a. To save the current layout as the default layout for this service, right-click the background and select **Save Layout as Default**.



**NOTE:** You must have administrator privileges to execute this command.

Once the current layout is saved as the default, subsequent users who visualize this service will be able to see the current layout.

- b. To reset the current layout to the default, right-click the background and select **Reset Layout to Default**.

- c. To reset the current layout to the layout that PSM automatically generates, right-click the background and select **Reset Layout**.
12. To save the service screen view as an image:
  - a. Select **Save Service Image**.  
The **Save Service Image** dialog appears.
  - b. Navigate to the desired folder and enter the filename.  
The default file format is png. To save the file in jpg format, enter .jpg at the end of the filename.
  - c. Click **Save**.

You have successfully completed this procedure.

## Activating a Transport Service

Use this procedure to configure and activate a transport service for BT17800 Series network elements.

In general, a transport service connects two client interfaces together through a series of cross-connects across a network. However, a service can also consist of a single cross-connect where both ends of the service reside on a single UFM.

You can configure and activate a transport service between BT17800 Series network elements only. See [Table 38 on page 328](#) for the supported client interface endpoints. The A and Z designations in the table are used only to distinguish between the two service endpoints. They are assigned arbitrarily and are interchangeable. For more information on cross-connects, refer to the *BT17800 Series Software Configuration Guide*.

**Table 38: Supported Service Activation Endpoint**

Site A			Site Z		
Client	Module	Line	Line	Module	Client
10ge	UFM3	otu2	otu2	UFM3	10ge
	UFM4			UFM4	
10ge	UFM3	otu2e	otu2e	UFM3	10ge
10ge	UFM3	odu2/otu4	odu2/otu4	UFM3	10ge
	UFM4			UFM4	
10ge	UFM3	odu2e/otu4	odu2e/otu4	UFM3	10ge
10ge	UFM6	odu2e/otu4/och	odu2e/otu4/och	UFM6	10ge
oc192	UFM3	otu2	otu2	UFM3	oc192
	UFM4			UFM4	

Table 38: Supported Service Activation Endpoint (continued)


Site A			Site Z		
Client	Module	Line	Line	Module	Client
oc192	UFM3	odu2/otu4	odu2/otu4	UFM3	oc192
	UFM4			UFM4	
oc192	UFM3	odu2/otu4	odu2/otu4/och	UFM6	oc192
	UFM4				
oc192	UFM6	odu2/otu4/och	odu2/otu4/och	UFM6	oc192
stm64	UFM3	otu2	otu2	UFM3	stm64
	UFM4			UFM4	
stm64	UFM3	odu2/otu4	odu2/otu4	UFM3	stm64
	UFM4			UFM4	
stm64	UFM3	odu2/otu4	odu2/otu4/och	UFM6	stm64
	UFM4				
stm64	UFM6	odu2/otu4/och	odu2/otu4/och	UFM6	stm64
wanoc192	UFM3	otu2	otu2	UFM3	wanoc192
	UFM4			UFM4	
wanoc192	UFM3	odu2/otu4	odu2/otu4	UFM3	wanoc192
	UFM4			UFM4	
wanstm64	UFM3	otu2	otu2	UFM3	wanstm64
	UFM4			UFM4	
wanstm64	UFM3	odu2/otu4	odu2/otu4	UFM3	wanstm64
	UFM4			UFM4	
8gfc	UFM6	odu2/otu4/och	odu2/otu4/och	UFM6	8gfc
10gfc	UFM6	odu2e/otu4/och	odu2e/otu4/och	UFM6	10gfc
otu2	UFM3	otu2	otu2	UFM3	otu2
	UFM4			UFM4	

Table 38: Supported Service Activation Endpoint (continued)

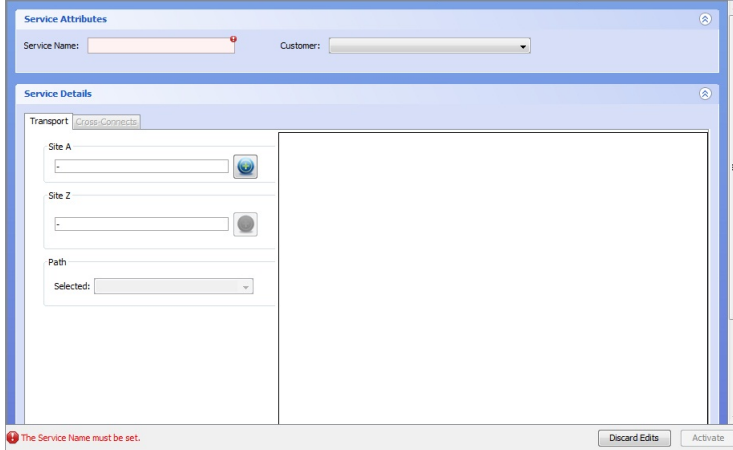
Site A			Site Z		
Client	Module	Line	Line	Module	Client
otu2	UFM3	odu2/otu4	odu2/otu4	UFM3	otu2
	UFM4			UFM4	
otu2	UFM3	odu2/otu4	odu2/otu4/och	UFM6	otu2
	UFM4				
otu2	UFM6	odu2/otu4/och	odu2/otu4/och	UFM6	otu2
otu2e	UFM3	otu2e	otu2e	UFM3	otu2e
otu2e	UFM3	odu2e/otu4	odu2e/otu4	UFM3	otu2e
otu2e	UFM3	odu2e/otu4	odu2e/otu4/och	UFM6	otu2e
otu2e	UFM6	odu2e/otu4/och	odu2e/otu4/och	UFM6	otu2e
40ge	UFM6	odu3/otu4/och	odu3/otu4/och	UFM6	40ge
100ge	UFM3	otu4	otu4	UFM3	100ge
	UFM4			UFM4	
100ge	UFM3	otu4	otu4/och	UFM6	100ge
	UFM4				
100ge	UFM6	otu4/och	otu4/och	UFM6	100ge
otu4	UFM3	otu4	otu4	UFM3	otu4
	UFM4			UFM4	
otu4	UFM3	otu4	otu4/och	UFM6	otu4
	UFM4				
otu4	UFM6	otu4/och	otu4/och	UFM6	otu4



**NOTE:** The UFM6 line port is represented by an optical channel (och) interface. The optical channel can contain up to two OTU4 signals. In order to interwork with UFM3 and UFM4 OTU4 line interfaces, you must configure the optical channel interface on the UFM6 for a single OTU4 signal using QPSK modulation. For more information, see [“Adding an Interface” on page 198](#).

1. Select **Tools >Service Activation >Transport**. Alternatively, click the **Service Activation**  button on the toolbar, and select **Transport**, or right-click **Transport** in the Network tree and select **Service Activation**.

The **Activate Transport Service** dialog opens.



2. Enter the required information as described in the following table.

**Table 39: Fields in the Activate Transport Service Dialog**

Field	Description	Required field?
Service Name	User-defined name that uniquely identifies the service.	Yes
Customer	Select from the drop-down list. To add a customer to the list, select Edit>Add Customer from the main menu. For more information on adding customers, see <i>Adding a Customer</i> .	Optional
Site A	Click and choose from a drop-down menu of existing sites. See <a href="#">Table 38 on page 328</a> for the supported client interface endpoints.	Yes
Site Z	Click and choose from a drop-down menu of existing sites. See <a href="#">Table 38 on page 328</a> for the supported client interface endpoints. Only those endpoints that can be reached from Site A are shown.	Yes
Path	Choose from a drop-down list of possible paths from Site A to Site Z.	Yes

3. Click **Activate**.

The PSM server sends the activation request to the network element. You can monitor the status of the request through the **View >Server >Tasks** window. The new service appears in the Network tree a short while after the task completes successfully. As part of service activation, PSM creates all the necessary transport cross-connects along the path between the specified endpoints.

You have successfully completed this procedure.

## Updating a Transport Service

Use this procedure to change the service name and customer of an activated transport service.

1. In the Network tree, double-click the service you want to update. Alternatively, select the service, right-click, and choose **View**.

The Service Attributes window opens.

2. Modify the **Customer** or **Service Name**. Click **Update**.

The transport service is updated. If you update a transport service with BTI7800, MX Series, PTX Series, or QFX Series endpoints across a BTI7000 optical network, the underlying optical service is updated implicitly.

## Deleting a Transport Service

Use this procedure to delete a transport service.

When a service is deleted, the state of the associated modules and ports remains unchanged.

1. In the Network tree, right-click a transport service and choose **Delete**.

A dialog opens asking for confirmation.

2. Click **OK**.

The transport service is deleted from the network elements and the PSM server. If you delete a transport service with BTI7800, MX Series, PTX Series, or QFX Series endpoints across a BTI7000 optical network, the underlying optical service is deleted implicitly.

## Viewing the Transport Services Table

Use this procedure to view the transport services table for BTI7800 Series network elements.

1. From the main menu choose **View > Transport > Services**.

The Transport Services tab is displayed.

Customer	Service Name	Site A	Site Z	End-To-End State
		10.1.220.104 10ge:1/8/1/8	10.1.220.104 odu2:1/8/2/1.8	Down
		10.1.220.68 stm64:1/1/1/9	10.1.220.68 odu2:1/1/2/1.2	Down
		10.1.220.68 10ge:1/2/1/7	10.1.220.68 odu2:1/2/2/1.7	Down
		10.1.220.68 oc192:1/14/1/6	10.1.220.68 oc192:1/5/1/6	Up
		10.1.220.68 10ge:1/4/1/3	10.1.220.68 odu2:1/4/2/1.3	Down
		10.1.220.104 10ge:1/8/1/4	10.1.220.104 odu2:1/8/2/1.4	Down
		10.1.220.68 10ge:1/2/1/10	10.1.220.68 odu2:1/2/2/1.10	Down





**NOTE:** To apply filters to this table, see “Working with Optical/Transport Services and Topology Tables” on page 334

2. Use the scroll bar on the right side of the window to scroll through the list of services.

## Viewing the Transport Services Per Span Table

Use this procedure to view the transport services per span table for BTI7800 Series network elements.

1. From the main menu choose **View >Transport >Services per Span**.

The Transport Services per Span tab is displayed.

Span Source	Span Source...	Span Source Port	Span Far-End	Span Far End Ip	Span Far ...
10.1.220.104	10.1.220.104	odu2:1/2/2/1.4	10.1.220.104	10.1.220.104	odu2:1/4/2/...
10.1.220.68	10.1.220.68	odu2:1/14/2/1.6	10.1.220.68	10.1.220.68	odu2:1/5/2/...
10.1.220.68	10.1.220.68	odu2:1/14/1/7	10.1.220.68	10.1.220.68	odu2:1/5/1/7
10.1.220.68	10.1.220.68	odu2:1/5/2/1.9	10.1.220.68	10.1.220.68	odu2:1/14/2...



**NOTE:** To apply filters to this table, see “Working with Optical/Transport Services and Topology Tables” on page 334

2. Use the scroll bar on the right side of the window to scroll through the list of services per span.

## Viewing the Transport Topology Table

Use this procedure to view the transport topology table for BTI7800 Series network elements.

1. From the main menu choose **View >Transport >Topology**.

The Transport Topology tab displays.

Source Site Name	Source Site IP	Source Port	Far End Site Name	Far End Site IP
10.1.220.104	10.1.220.104	otu2:1/2/1/11	10.1.220.104	10.1.220.104
10.1.220.104	10.1.220.104	otu2:1/4/1/11	10.1.220.104	10.1.220.104
10.1.220.104	10.1.220.104	otu4:1/2/2/1	10.1.220.104	10.1.220.104
10.1.220.104	10.1.220.104	otu4:1/4/2/1	10.1.220.104	10.1.220.104
10.1.220.68	10.1.220.68	otu2:1/14/1/7	10.1.220.68	10.1.220.68
10.1.220.68	10.1.220.68	otu2:1/5/1/7	10.1.220.68	10.1.220.68
10.1.220.68	10.1.220.68	otu4:1/14/2/1	10.1.220.68	10.1.220.68
10.1.220.68	10.1.220.68	otu4:1/5/2/1	10.1.220.68	10.1.220.68
10.1.220.68	10.1.220.68	otu4:1/12/1/1	10.1.220.68	10.1.220.68



**NOTE:** To apply filters to this table, see “Working with Optical/Transport Services and Topology Tables” on page 334

2. Use the scroll bar on the right side of the window to scroll through the optical topology details.

## Viewing the Transponder Tuning Grid

Use this procedure to view and optionally export the transponder tuning grid for BT17000 Series, BT17800 Series, and BT1800 Series network elements.

The transponder tuning grid shows the wavelengths, real-time optical PM data, and other information on transponder ports for the selected network element.

1. In the Network tree or the Topology Map view, right-click a network element and select **Node > Tuning Grid > View**. Alternatively, right-click a shelf in the Network tree and select **Tuning Grid > View**. This option is greyed out if the network element (or shelf) does not contain at least one transponder card with at least one provisioned port containing an XFP.

The **Tuning Grid** window appears.

Tuning Grid At Mon 03 Jun 2013 12:43:32 EDT

Port	Protocol	Wavelength (nm;Thz;Ch:DOL)	OPT (dBm)	OPR (dBm)	BER	ES	UAS	State	Vendor
TPR-1-7-3	TENGELANFEC	0.0 : n/a : n/a : n/a	1.5	-12.6	0.0	0.0	0.0	Normal, Working	JDSU
TPR-1-7-2	TENGELAN	1330.0 : n/a : n/a : n/a	-2.2	-1.9	n/a	0.0	0.0	Normal	FINISAR CORP.
TPR-1-7-1	TENGELANFEC	0.0 : n/a : n/a : n/a	1.5	-12.8	0.0	0.0	0.0	Normal, Standby	JDSU

Refresh Export

2. To export the tuning grid in CSV format, select **Export** and enter the name of the file.
3. To refresh the real-time optical PM data, select **Refresh**.

## Working with Optical/Transport Services and Topology Tables

PSM can display optical/transport services, optical/transport services per span, and optical/transport topology information in table format. These tables can be manipulated to show information in different forms, depending on the need.

### Sorting the Tables

The tables can be sorted in the following ways:

- To sort the tables by a column, click the column title.

- To change the order (ascending or descending) of a column, click the column heading until the arrow shows ascending or descending order as desired.
- To show or hide columns, right-click the table title bar and check the column names you want to show, and uncheck the column names you want to hide in the drop-down menu. Different tables have different column selections. [Figure 74 on page 335](#) shows the column selections for the optical topology table.

Figure 74: Optical Topology Column Selection

Source Site Name	Source Group-Degree	Source Port	Far End Site Name	Far End Group-Degree	Administrative Status
Chicago	G1-D1	DLA-1-3-L1	NewYork	G1-D2	In-Service (IS)
Chicago	G1-D2	DLA-1-4-L1	10.10.20.100	G1-D1	In-Service (IS)
Dallas	G1-D1	ROB-1-7-L1	10.10.20.100	G1-D4	In-Service (IS)
Dallas	G1-D2	ROB-1-15-L1	Miami	G1-D1	In-Service (IS)
Kanata-B103	G1-D1	DLA-1-1-L1	10.127.210.22	G1-D2	In-Service (IS)
Kanata-B103	G1-D2	DLA-1-2-L1	10.127.11.21	G1-D1	In-Service (IS)
Miami	G1-D1	ROB-1-7-L1	Dallas	G1-D2	In-Service (IS)
Miami	G1-D2	ROB-1-11-L1	10.10.20.100	G1-D3	In-Service (IS)

## Filtering the Tables

The optical information tables behave as follows:

- If there is no filtering applied, the window title reflects the table being displayed, for example "Optical Topology".
- If a filter is applied, the title changes to indicate the presence of the filter, for example "Optical Topology (Filtered)".
- Each time a new entity or filter is chosen, the previous filtering is cleared and the tables display the entries that pertain to the newly chosen criteria.

To filter the tables to show only a particular set of entries, right-click a cell in the column of the table that has the data you want to filter with, and choose the filter option **Show only rows where** to filter out (hide) all other entries from the table. In the following screen for the optical services per span table, the filter chosen is to show only entries using channel 230.

Span Source	Span Far-End	Channel	Service Name	Service Site A	Service Site Z	Source P...
CHICAGO G1-D1	NEW-YORK G1-D2	230	VideoRing_PATH_B	MIAMI G1-D1	NEW-YORK G1-D2	Up - NR
DALLAS G1-D1	CHICAGO G1-D2	230	VideoRing_PATH_B	MIAMI G1-D1	NEW-YORK G1-D2	Up - NR
MIAMI G1-D1	DALLAS G1-D2	230	VideoRing_PATH_B	MIAMI G1-D1	NEW-YORK G1-D2	Up - NR
NEW-YORK G1-D1	MIAMI G1-D2	230	VideoRing_PATH_B	NEW-YORK G1-D1	MIAMI G1-D2	Up - NR
CHICAGO G1-D1	NEW-YORK G1-D2	220	MXPring_PATH_B	AMI G1-D2	Up - NR	
DALLAS G1-D1	CHICAGO G1-D2	220	MXPring_PATH_B	AMI G1-D2	Up - NR	
NEW-YORK G1-D1	MIAMI G1-D2	220	MXPring_PATH_B	AMI G1-D2	Up - NR	
DALLAS G1-D2	MIAMI G1-D1	220	MXPring_PATH_A	AMI G1-D1	Up - NR	
10.1.207.1 G12-D2	10.1.207.2 G34-D1	260		.1.207.5 G1-D2	Up - NR	
10.1.207.1 G12-D2	10.1.207.2 G34-D1	220		.1.207.5 G1-D2	Up - NR	
10.1.207.2 G34-D2	10.1.207.9 G4-D3	260		.1.207.5 G1-D2	Up - NR	
10.1.207.2 G34-D2	10.1.207.9 G4-D3	220		10.1.207.5 G1-D1	10.1.207.5 G1-D2	Up - NR



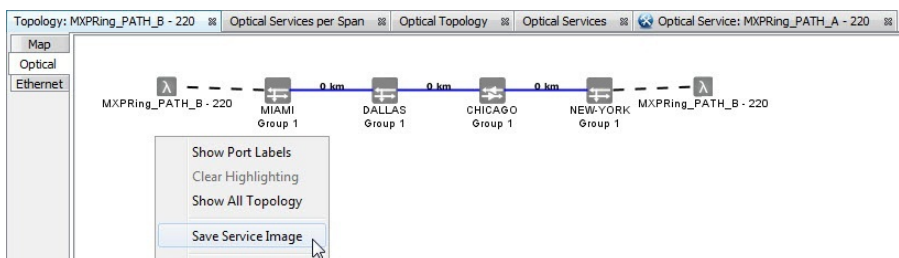
**NOTE:** The **View** and **Delete** options in the right-click menu are not filtering options. **View** brings up the "Service Attributes" and "Service Details" panels, and **Delete** deletes the optical service.

To remove filtering, right-click any cell in the table and choose **Show only rows where>No Filter**.

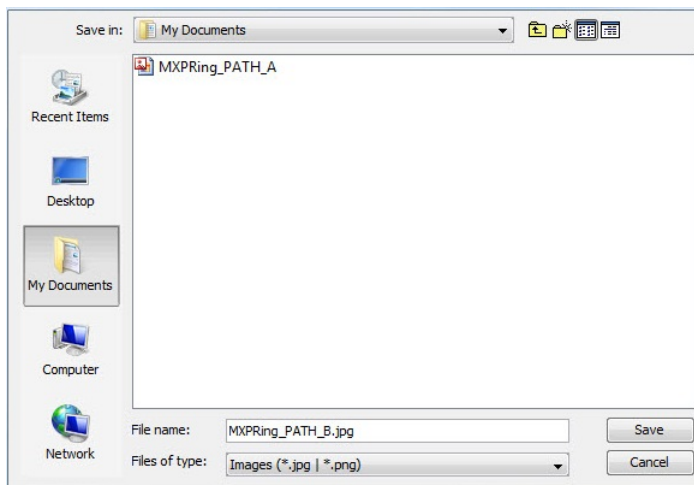
## Saving a Service Image

Use this procedure to save the service screen view to either a jpg or png image file. The default file format is .png. To save the file in jpg format, enter .jpg at the end of the file name.

1. In the main window, right-click and choose **Save Service Image**.



The windows file explorer window appears.



2. Navigate to the desired folder, specify a file name, and click **Save**.

Your service view is saved as an image.

## CHAPTER 12

# Managing Ethernet Services

- [Introduction on page 337](#)
- [Service Visualization on page 337](#)
- [Understanding Ethernet Service States on page 342](#)
- [Service Activation on page 344](#)
- [Modifying a Service on page 399](#)
- [Deleting a Service on page 402](#)
- [Adding SLA/CFM to a Service on page 402](#)
- [Running a Y.1731 Link Trace on page 408](#)
- [Running a Y.1731 Loopback on page 409](#)
- [Running an RFC 2544 Benchmarking Test on page 410](#)
- [Ethernet Ring Protection Switching \(ERPS\) on page 414](#)
- [Routing Considerations in Mixed Networks on page 421](#)
- [Managing Profiles on page 426](#)

## Introduction

---

An Ethernet service provides Ethernet connectivity between Ethernet service endpoints. An Ethernet service endpoint can be a UNI, NNI, or ENNI on a packet-aware module.

PSM can be used to manage Ethernet services on the BT17000 Series, the BT1700 Series, and the BT1800 Series network elements.

## Service Visualization

---


PSM automatically discovers all Ethernet services in the network and displays them in a graphical view.

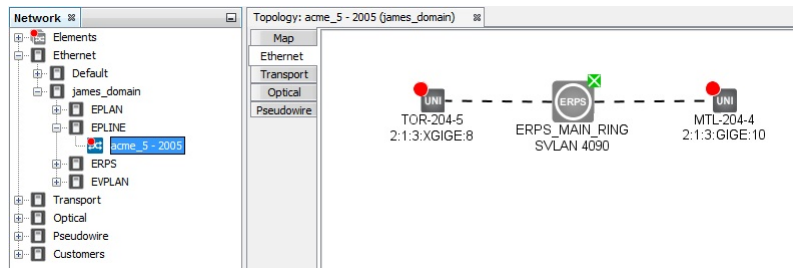
- [Visualizing an Ethernet Service on page 337](#)
- [Service Visualization Scheme on page 341](#)

## Visualizing an Ethernet Service

Use some or all of the techniques in this procedure to visualize an Ethernet service.

1. In the Network tree, select the desired Ethernet service.

The selected Ethernet service opens in the main Topology window. If the service is protected by ERPS, the service is shown connected to an ERPS icon. The ERPS icon represents an ERPS ring. The green  indicates that the ERPS ring is blocking its RPL link, which is normal.



See “Service Visualization Scheme” on page 341 for details on this view, and see “Ethernet Ring Protection Switching (ERPS)” on page 414 for details on ERPS.



**NOTE:** If this is your first time visualizing this service, you will see the default layout that PSM automatically generates. The default layout can be changed. See 9.

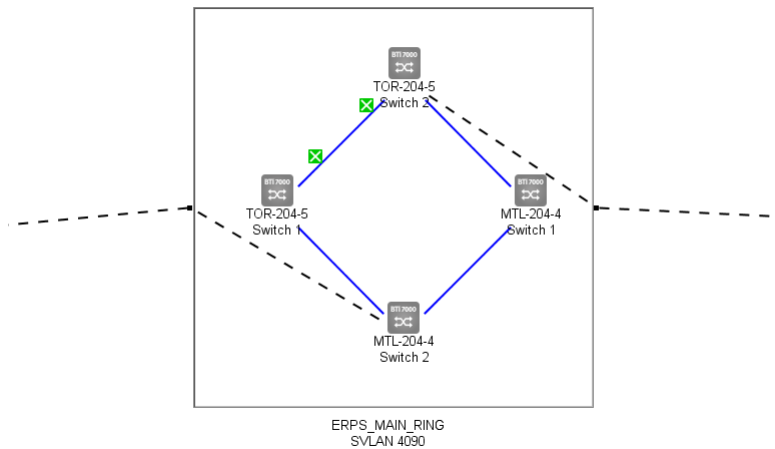



**NOTE:** If this is your second or subsequent time visualizing this service, you will see the layout that existed when you last exited this service view.

2. Double-click the ERPS icon to zoom in to see the network elements comprising the ERPS ring. Double-click again to zoom back out.



**NOTE:** Double-clicking to zoom works only on the default PSM layout or a smaller (more zoomed out) layout.

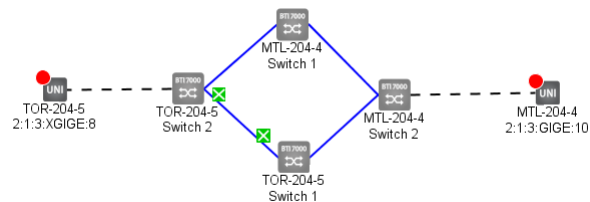


The green  indicates the RPL link that is blocked.

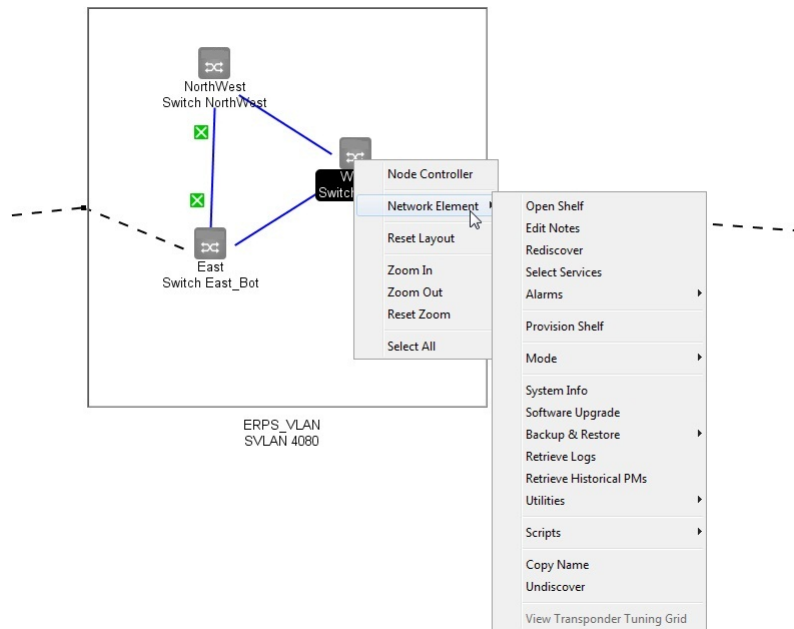


**NOTE:** The ERPS service itself can be visualized as well. For more information, see [“Visualizing an ERPS Service” on page 414](#).

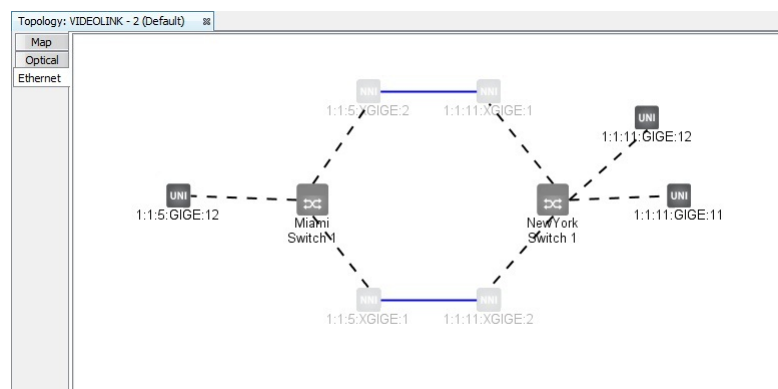
3. Alternatively, right-click the ERPS icon and choose **Expand ERPS Ring**.



4. To change the size of the service view:
  - a. Right-click the background and select **Zoom In** to increase the view size. Alternatively, you can zoom in by scrolling the mouse scroll wheel away from you.
  - b. Right-click the background and select **Zoom Out** to decrease the view size. Alternatively, you can zoom out by scrolling the mouse scroll wheel towards you.
  - c. Right-click the background and select **Reset Zoom** to return the view size to its original size.
5. Right-click a network element and select **Network Element** to see the regular NE menu options.



6. To move elements in this view, click and drag elements to the desired location.
7. To move all of the ports and switches in the service, right-click the background and choose **Select All** and drag the service within the window.
8. By default, the connected NNI ports are hidden. To view the connected ports, right-click the background and choose **Show Connected Ports**. The screenshot below shows a service with connected NNI ports displayed.



**NOTE:** Choosing Show Connected Ports again toggles the setting.



9. You can save the current layout as the default, or revert to the default, or revert to the layout that PSM automatically generates.
  - a. To save the current layout as the default layout for this service, right-click the background and select **Save Layout as Default**.



**NOTE:** You must have administrator privileges to execute this command.

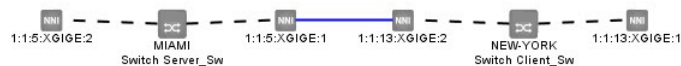
Once the current layout is saved as the default, subsequent users who visualize this service will see the current layout.

- b. To reset the current layout to the default, right-click the background and select **Reset Layout to Default**.
  - c. To reset the current layout to the layout that PSM automatically generates, right-click the background and select **Reset Layout**.
10. To save the service screen view as an image:
  - a. Select **Save Service Image**.  
The **Save Service Image** dialog appears.
  - b. Navigate to the desired folder and enter the filename.  
The default file format is png. To save the file in jpg format, enter .jpg at the end of the filename.
  - c. Click **Save**.
11. To select all NEs in the service, click **Select Network Elements**.  
This brings you back to the main Topology Map view and shows all NEs in the service selected.

## Service Visualization Scheme

The service visualization scheme provides visual details about the service, as shown in the screens below and explained as follows:

- Grey indicates ports (UNI or NNI) added by the user.
- Faded grey indicates NNI ports added by the system using GVRP.
- Dashed black lines indicate logical connections on the switch showing which ports are members of the switch.
- Solid blue lines indicate physical connections (fiber optic or Ethernet cables).
- The name of the NE (e.g. MIAMI) and the name of the switch (e.g. Switch Server\_Sw):



If the name of the NE has not been defined, the IP address is shown instead.

- Detailed information about a switch or port or link appear by simply hovering over the icon in the Ethernet service topology view, as shown below:

Figure 75: Hovering Over a Switch

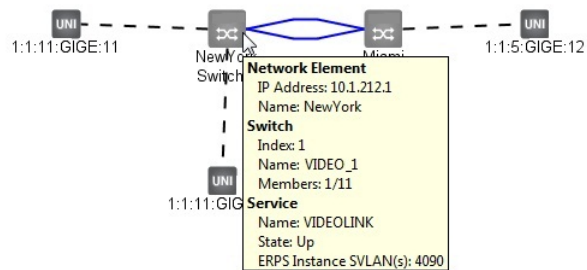


Figure 76: Hovering Over a UNI

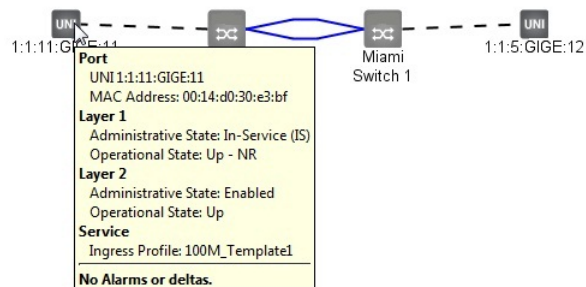
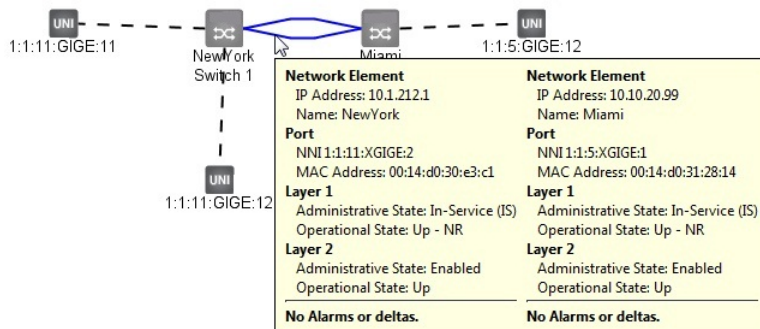


Figure 77: Hovering Over a Link



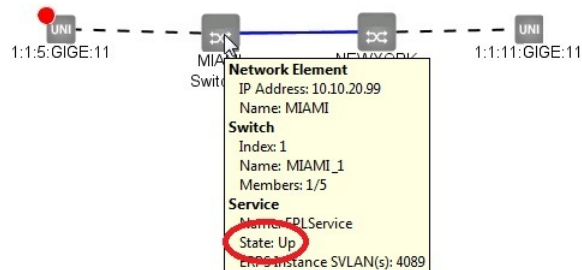
## Understanding Ethernet Service States

PSM provides information on the state of an Ethernet service.

Each switch maintains a state for every service configured on the switch. This state (one per service) represents the state of the network connections to the remote MEPs, and does not include the state of the endpoint UNIs. This state behaves as follows:

- Up - all remote MEPs are Up
- Down - one or more remote MEPs are Down
- Unknown - no remote MEPs exist

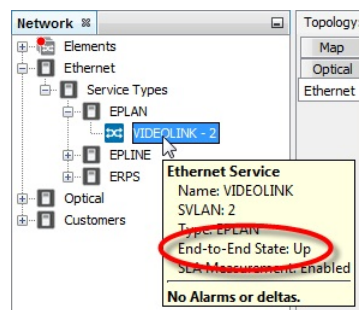
This state is shown in PSM by hovering over an NE in the Ethernet service topology view.



Additionally, PSM maintains an End-to-End service state, which is an overall state that considers the service states on all switches that have UNIs belonging to this service. The End-to-End service state behaves as follows:

- Up - all service states for this service are Up
- Down - all service states for this service are Down
- Troubled - a mix of service states that are Up and Down
- Unknown - all service states for this service are Unknown

The End-to-End service state is shown in PSM by hovering over an NE in the Ethernet service tree view. It is also recorded in the Ethernet services report ([“Generating Ethernet Reports” on page 493](#)).



## Service Activation

---

PSM supports the Metro Ethernet Forum (MEF) paradigm for activating Layer 2 Ethernet services in the network. As part of service activation, you define the service and you select the endpoints (and in some cases, the internal NNIs) that make up the service.



**NOTE:** Unless otherwise specified, all references to UNI include UNI LAG, all references to NNI include NNI LAG, and all references to ENNI include ENNI LAG.

An endpoint can be one of the following:

- An Ethernet **UNI**, which is an Ethernet user-to-network interface.
- An Ethernet **ENNI**, which is an external Ethernet network-to-network interface.
- An Ethernet **NNI**, which can be an internal or external Ethernet network-to-network interface. An external NNI is an endpoint, but an internal NNI is not. If PSM detects (via LLDP discovery) that the NNI is connected to Juniper Networks equipment, PSM considers that the NNI is internal. Otherwise, PSM considers the NNI is external, and treats it as an endpoint. An NNI that is determined to be external is similar to an ENNI. To avoid confusion, it is best to use ENNIs for external NNIs where possible. For those network elements that do not support ENNI functionality, PSM continues to support the ability to treat the regular NNI as an external endpoint where applicable.



**NOTE:** ENNI is supported on BT17000 Series network elements starting in Release 13.2 only. ENNI is not supported on any other network elements.

Before using PSM for service activation, you need to configure the packetVX cards on the appropriate network elements, and create the virtual switches that represent those cards. You should also create the necessary internal NNIs, but you do not need to create the endpoints as you have the option of creating endpoints in PSM when you activate the service. You can create internal NNIs in PSM as well, but if you create the internal NNIs beforehand, PSM will be able to query the network and use the discovered LLDP topology to automatically select the appropriate internal NNIs as you add endpoints to the service. The ability to automatically select the internal NNIs is called the **Auto-Provision NNIs** feature.



**NOTE:** For the Auto-Provision NNIs feature to work properly, you must create all internal NNIs and bring up their links beforehand. In this situation, all NNIs that you create as part of service activation are external endpoint NNIs.

*Creating* a UNI, NNI, or ENNI refers to the initial configuration needed to transform an unprovisioned port to a UNI, NNI, or ENNI port.

Selecting a UNI, NNI, or ENNI refers to choosing that UNI, NNI, or ENNI port to be part of the service. When you select a UNI, NNI, or ENNI and you activate the service, PSM performs the necessary configuration to include that port in the service.



**NOTE:** In PSM, if you use the **Provision As ...** feature, you can create and select a UNI, NNI, or ENNI in a single step.

Not all internal NNIs need to be selected manually. If the network is running GVRP, then the network can select the internal NNIs automatically after the service is activated. In other situations, PSM can automatically select and configure the internal NNIs that are needed for the service. This is shown in the following table:

Network Composition	NNI Selection
The domain contains only BT17000 Series network elements.	You do not need to manually select the internal NNIs. The BT17000 Series network elements use GVRP to select and configure the required internal NNIs. For more information on GVRP, see <a href="#">“GVRP - GARP VLAN Registration Protocol” on page 421</a> .
The domain contains one or more BT1700 Series network elements or one or more BT1800 Series network elements.	<p>If all network elements in the domain are running the following minimum levels of software:</p> <ul style="list-style-type: none"> <li>• BT17000 Series - Release 10.3 or higher</li> <li>• BT1700 Series - Release 1.5 or higher</li> <li>• BT1718E - Any release</li> <li>• BT1800 Series - Release 1.1 or higher</li> </ul> <p>then you can use the <b>Auto-Provision NNIs</b> feature to instruct PSM to automatically select the required internal NNIs.</p> <p><b>NOTE:</b> PSM uses topology information gathered from LLDP to select the required NNIs. Only those NNIs that cannot be configured using GVRP are selected.</p> <p>Otherwise, you must manually select some or all of the internal NNIs that make up the service. For more information on which internal NNIs you need to select, see <a href="#">“Mixed Networks - BT17000 Series with BT1700 Series or BT1800 Series Elements” on page 422</a>.</p>

- [Service Types on page 346](#)
- [Auto-provisioning NNIs on page 347](#)
- [Activating an Ethernet Service on page 348](#)
- [Example: Activating an EVPLINE Service on page 364](#)
- [Example: Activating an Ethernet Service on a Multi-chassis LAG on page 377](#)
- [Example: Activating EVPLAN and EVPLINE Services Using Service Maps for Flow Redirection on page 381](#)

## Service Types



**NOTE:** Unless otherwise specified, all references to UNI include UNI LAG, all references to NNI include NNI LAG, and all references to ENNI include ENNI LAG.

The service types supported are listed in the table below. The **Service Type** selected in the **Service Attributes** panel determines how UNIs can be used, and should be based on the UNIs you have or expect to have in the service. The service type cannot be changed once the service is activated. If the service does not and will not include any UNIs, then you can set the service type to any value.

*Table 40: Service Types*

Service type	Description
EPLINE (Ethernet Private Line)	Used to replace TDM private lines.  A port-based service with a point-to-point EVC (Ethernet Virtual Connection) between dedicated UNIs (that is, only a single EVC per UNI).  User can select a maximum of two endpoints.
EVPLINE (Ethernet Virtual Private Line)	Used to replace Frame Relay or ATM services.  A multiplexed service with a point-to-point EVC between service-multiplexed endpoints (that is, multiple EVCs per endpoint).  User can select a maximum of two endpoints.  Allows a single physical connection to the attached equipment with multiple virtual connections.
EPLAN (Ethernet Private LAN)	Used to support transparent LAN services and multipoint Layer 2 VPNs.  A port-based service with a multipoint-to-multipoint EVC across dedicated endpoints (that is, only a single EVC per endpoint).  User can select more than two UNIs.
EVPLAN (Ethernet Virtual Private LAN)	Used to support transparent LAN services and multipoint Layer 2 VPNs.  A multiplexed service with a multipoint-to-multipoint EVC across service-multiplexed endpoints (that is, multiple EVCs per endpoint).  User can select more than two endpoints.

Table 40: Service Types (continued)

Service type	Description
EPTREE (Ethernet Private TREE)	<p>Used to support a multipoint service consisting of leaf endpoints and root endpoints. Leaf endpoints and root endpoints can send and receive packets from (other) root endpoints, but leaf endpoints cannot send and receive packets from other leaf endpoints.</p> <p>A port-based service with a rooted-multipoint EVC across dedicated endpoints (that is, only a single EVC per endpoint).</p> <p>User can select more than two endpoints.</p> <p>This service type is only supported on BTI7000 Series network elements.</p>
EVPTRREE (Ethernet Virtual Private TREE)	<p>Used to support a multipoint service consisting of leaf endpoints and root endpoints. Leaf endpoints and root endpoints can send and receive packets from (other) root endpoints, but leaf endpoints cannot send and receive packets from other leaf endpoints.</p> <p>A port-based service at the leaf nodes and a multiplexed service at the root node, using a rooted-multipoint EVC across endpoints (that is, only a single EVC at the leaf endpoint, and multiple EVCs at the root endpoint).</p> <p>User can select more than two endpoints.</p> <p>This service type is only supported on BTI7000 Series network elements.</p>

See the *BTI7000 Series packetVX Solutions Guide* for more details on Ethernet services and Ethernet VCs.

## Auto-provisioning NNIs



**NOTE:** Unless otherwise specified, all references to UNI include UNI LAG, all references to NNI include NNI LAG, and all references to ENNI include ENNI LAG.

PSM has the capability of selecting the necessary internal NNIs to add to the service. Internal NNIs are the NNIs that connect the service endpoints together.

You should only choose this option if all network elements in the domain are running the following minimum levels of software:

- BTI7000 Series - Release 10.3 or higher
- BTI700 Series - Release 1.5 or higher
- BTI718E - Any release
- BTI800 Series - Release 1.1 or higher

Additionally, all the required internal NNIs must already exist and their links brought up, and LLDP enabled.

When this option is selected, PSM uses topology information gathered from LLDP to select and configure those required internal NNIs that do not have GVRP enabled. If PSM determines that GVRP is enabled on a particular NNI, it will let GVRP configure that NNI.

PSM selects internal NNIs differently depending on whether the required NNI is part of an ERPS ring or not. If the NNI is part of an ERPS ring, then PSM has sufficient information to determine whether the NNI should be selected or not. If the NNI is not part of an ERPS ring, then PSM uses a more liberal set of selection criteria and might select more internal NNIs than is necessary. In such a case, you can manually delete the unnecessary NNIs from the service.

As an alternative, you can force PSM to select a single path through non-ERPS nodes when Auto-Provision NNIs is enabled. See the *proNX Service Manager Installation and Administration Guide* for details.

## Activating an Ethernet Service

Use this procedure to configure and activate an Ethernet service.

### Prerequisites:

- All the necessary packetVX cards and virtual switches have been configured.
- ERPS rings (or MSTP) have been configured, as applicable. This prevents routing loops when multiple paths exist through the network.



**NOTE:** Unless otherwise specified, all references to UNI include UNI LAG, all references to NNI include NNI LAG, and all references to ENNI include ENNI LAG.

Additionally:

If you want to ...	Prerequisite	Notes
Select all UNIs, NNIs, and ENNIs manually during service activation.	There is no additional prerequisite.	<p>When you activate a service, you manually select (and/or create) all the UNIs, NNIs, and ENNIs that make up that service.</p> <p><b>NOTE:</b> After you activate, GVRP, if enabled, might cause other NNIs to be selected as well, but this is performed outside of PSM.</p>



If you want to ...	Prerequisite	Notes
<p>Select endpoints manually and let the network select internal NNIs using GVRP.</p>	<p>Enable GVRP on BT17000 Series network elements where possible.</p>	<p>In a network that only contains BT17000 Series network elements, GVRP can be used to propagate VLAN membership information to all the NNIs, making it unnecessary to select and configure each internal NNI individually from PSM. Just select the endpoints and let GVRP configure the required internal NNIs (outside of PSM). PSM automatically discovers and displays the internal NNIs as soon as you select the service endpoints.</p> <p>If the internal NNIs are down or not yet created, GVRP will not be able to configure the required internal NNIs. You can activate the service but the service will be disconnected. Once the internal NNIs have been created and/or their links brought up, the path through the network will be established as VLAN membership information propagates to all the internal NNIs through GVRP.</p> <p>In a mixed network that contains BT17000 Series, BT1700 Series, and/or BT1800 Series network elements, you might need to manually select internal NNIs because not all of these devices support GVRP. See <a href="#">"Activating Services Over Combinations Of BT17000 Series packetVX and BT1700 Series or BT1800 Series Networks"</a> on page 424</p>
<p>Select endpoints manually and let the network select internal NNIs using GVRP, and let PSM select internal NNIs using the <b>Auto-Provision NNIs</b> option.</p>	<p>Ensure all network elements in the domain are at the following minimum levels of software:</p> <ul style="list-style-type: none"> <li>• BT17000 Series - Release 10.3 or higher</li> <li>• BT1700 Series - Release 1.5 or higher</li> <li>• BT1718E - Any release</li> <li>• BT1800 Series - Release 1.1 or higher</li> </ul> <p>Enable LLDP on all network elements in the domain.</p> <p>Create all the required internal NNI ports and bring their links up.</p> <p>Enable GVRP on BT17000 Series network elements.</p>	<p>This lets GVRP configure the required internal NNIs where possible. If GVRP is not enabled or not supported, then PSM uses topological information gathered by the NEs through LLDP, and automatically selects the necessary internal NNIs. PSM only selects those internal NNIs that cannot be configured using GVRP.</p>

The general service activation workflow is as follows:

1. Create the Ethernet service and set the service-wide attributes.
2. Select ports to be added to the service.
3. Set the port-based attributes (optional).
4. Set the advanced switch-based and the advanced port-based attributes (optional).
5. Activate the service.

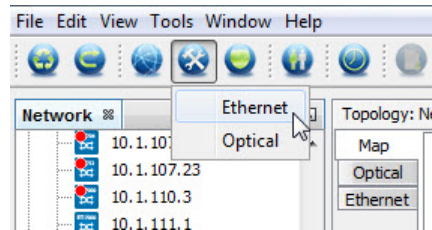


.....

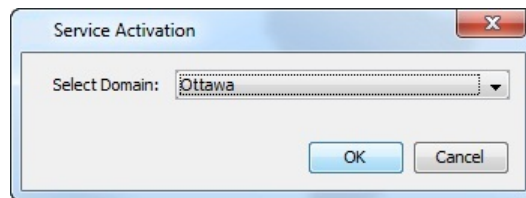
**NOTE:** ENNI is supported on BT17000 Series network elements starting in Release 13.2 only. ENNI is not supported on any other network elements.

.....

1. Create the Ethernet service and set the service-wide attributes.
  - a. Click the **Service Activation** button on the toolbar and choose **Ethernet** from the drop-down menu.

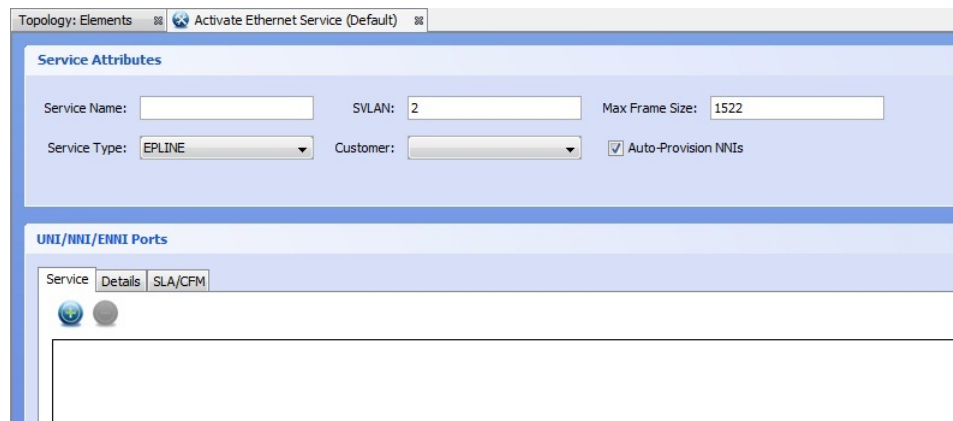


- b. If you have multiple domains, a **Service Activation** pop-up dialog box is displayed, as shown.



From the **Select Domain** drop-down menu, select a domain in which to create the service. Each domain has its own S-VLAN ID namespace, allowing you to re-use S-VLAN IDs across domains. Click **OK**.

- c. The **Activate Ethernet Service** window appears, as shown.



In the Service Attributes pane of the Activate Ethernet Service window, enter the required information as listed in the following table.

**Table 41: Fields in the Service Attributes Pane**

Field	Description	Required field?
Service Name	User-defined name that identifies the service. Must be unique to the domain.	Yes

Table 41: Fields in the Service Attributes Pane (continued)

Field	Description	Required field?
SVLAN	<p>Auto-populated with the next available value. Must be unique to the domain. A value of -1 is shown if there are no SVLAN identifiers available.</p> <p>The auto-populated value can be overridden.</p>	Yes
Max Frame Size	<p>The maximum frame size (in bytes) for the Ethernet service. Applicable to UNI ports on BTI7000 Series NEs only.</p> <p>Default: 1522</p> <p>For BTI7000 Series NEs, this value is used at each UNI port in the service, and supersedes (but must not be greater than) the "Max Frame Size" setting configured on those ports. If this value is greater than the "Max Frame Size" configured on any port in the service, an error message appears.</p> <p>For BTI700 Series and BTI800 Series NEs, this value is ignored. The "Max Frame Size" configured on each port is used instead.</p>	Yes
Service Type	<p>See <a href="#">"Service Types" on page 346</a>.</p> <p>Default: EPLINE</p> <p><b>NOTE:</b> The BTI700 Series network element does not make a distinction between E(V)PLINE and E(V)PLAN service types. Consequently, PSM might display a service type of an existing BTI700 Series service as E(V)PLAN regardless of how it was originally configured.</p> <p><b>NOTE:</b> EPTREE and EVPTRREE services are supported on BTI7000 Series NEs only.</p>	Yes
Customer	User-defined. See <a href="#">"Adding a Customer" on page 454</a> .	Optional
Auto-Provision NNIs	<p>Specify whether you want PSM to select internal NNIs automatically. This check box is selected by default. See <a href="#">"Auto-provisioning NNIs" on page 347</a>.</p> <p>If you do not select this option, you will need to manually select the required internal NNIs in a mixed network. For more information on mixed networks, see <a href="#">"Mixed Networks - BTI7000 Series with BTI700 Series or BTI800 Series Elements" on page 422</a>.</p>	Optional

2. Select ports to be added to the service.

These ports can be endpoints and/or internal NNIs. You must always select the endpoints.

Depending on configuration, you might need to select internal NNIs. The rules for internal NNI selection are as follows:

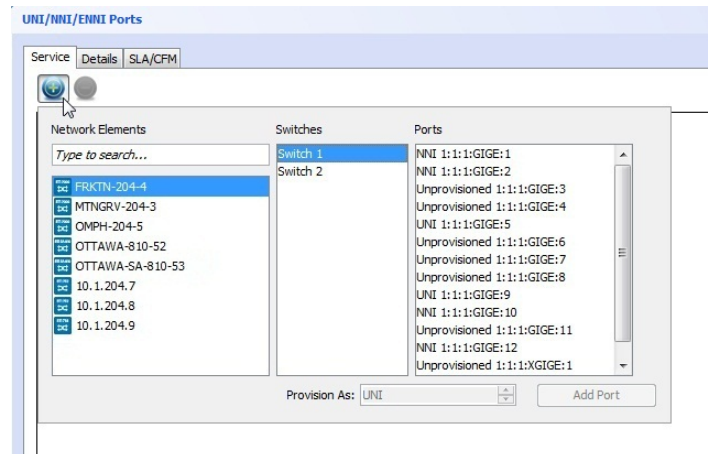
- You must not select internal NNIs if **Auto-Provision NNIs** is enabled.

- You must select internal NNIs if **Auto-Provision NNIs** is disabled and GVRP is disabled on the NNI ports being selected. GVRP is configured on the NNI port using the proNX 900 or the CLI directly.
- If **Auto-Provision NNIs** is disabled and GVRP is enabled on the NNI ports being selected, you can select internal NNIs but there is generally no added benefit to doing so. GVRP will select the appropriate internal NNIs for you.



**NOTE:** When you select an NNI port, you do not make a distinction between an endpoint NNI and an internal NNI. PSM makes that determination automatically based on topology. If PSM detects (via LLDP discovery) that the NNI is connected to Juniper Networks equipment, PSM considers that the NNI is internal. Otherwise, PSM considers the NNI is external (endpoint).

- In the Service tab of the UNI/NNI/ENNI Ports panel, click on the icon. The following dialog appears.



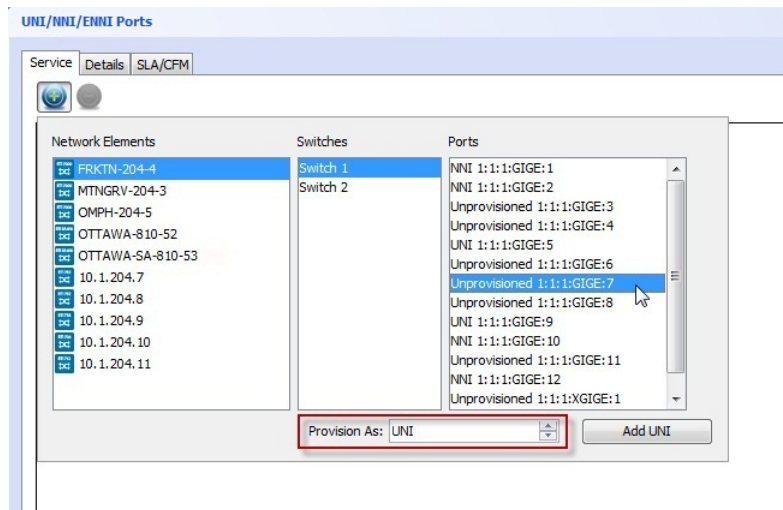
This dialog lets you specify UNI/NNI/ENNI ports to include in the service. These ports are MEF interface ports on network elements within the selected domain. Selecting an NE from the list auto-populates the switch members and ports that are available for the Service Type chosen in the Service Attributes pane.

- Select a network element, card and port. The port can be UNI or UNI LAG, NNI or NNI LAG, ENNI or ENNI LAG, or Unprovisioned. You can multi-select ports by using the **<ctrl>** or **<shift>** keys, but you cannot multi-select a mix of provisioned and unprovisioned ports. You will need to add these separately.



**NOTE:** If you did not select **Auto-Provision NNIs**, you might have to add a number of internal NNIs to the service in order for traffic to be carried through the network. See [“Routing Considerations in Mixed Networks” on page 421](#).

If you select an unprovisioned port in the Ports field, the **Provision As** field is activated, allowing you to provision it as a **UNI** or **UNI LAG**, **NNI** or **NNI LAG**, **ENNI** or **ENNI LAG**.



If you use the **Provision As** option to create a UNI LAG, an NNI LAG, or an ENNI LAG, then all ports you multi-select will be added to the LAG.

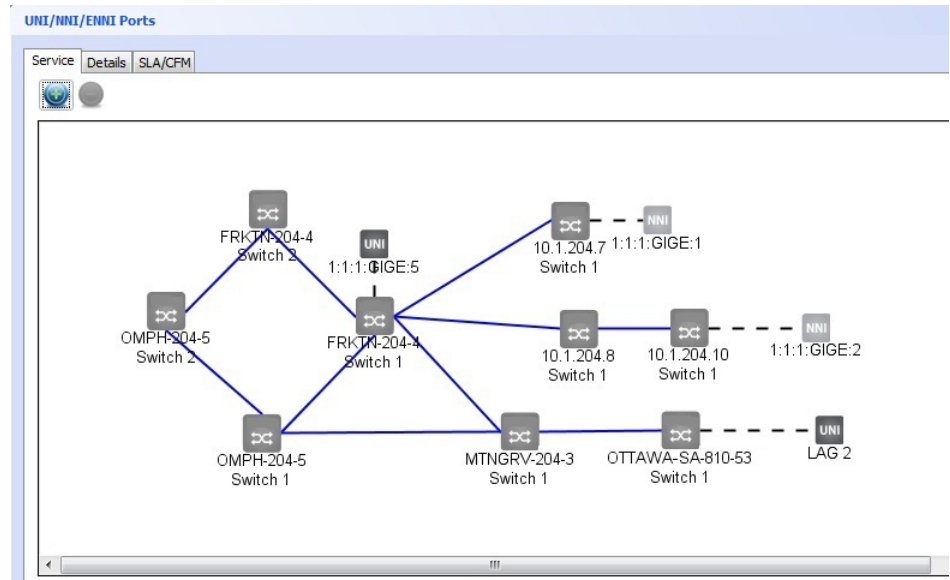


**NOTE:** If you use the **Provision As** field to create a new NNI port on a BTI700 Series network element, you cannot use the proNX 900 to reconfigure any of the settings on that port. If you want to be able to use the proNX 900 to reconfigure the settings on that port, you must create the NNI port using the proNX 900 instead of using the **Provision As** option.

- c. Click **Add UNI** or **Add UNI LAG**, **Add NNI** or **Add NNI LAG**, or **Add ENNI** or **Add ENNI LAG** depending on the type of port chosen.

PSM adds the port and any auto-selected internal NNI ports required. Additionally, if the port that you are adding is a multi-chassis LAG member, PSM automatically adds all members of that multi-chassis LAG to the service. See [“Example: Activating an Ethernet Service on a Multi-chassis LAG”](#) on page 377 for a service activation example involving a multi-chassis LAG.

- d. After you have finished adding ports, click on the **Service** tab to view the added ports.



**NOTE:** PSM displays a warning message if it cannot find all the internal NNIs necessary for the service. This can occur if an internal NNI port is down, for example. In this situation, you can still activate the service but the service might not work.

- e. To view the added ports, click on the **Details** tab.

The Details window displays the added ports, showing the containing NE, switch, and LAG (if applicable). PSM displays the ports you manually specified, and the internal NNI ports that PSM has selected through the **Auto-Provision NNIs** feature.

UNI/ENNI Port	VLAN Mappings	Ingress Service Profile	Egress Service Profile	TPID	Max Frame	Media Rate	Advanced Se...
FRKTN-204-4							
Switch 1							
UNI 1:1:1:GIGE:5	Click to add...			[Not Applicable]	1522	Auto	Click to edit...
NNI 1:1:1:GIGE:10				0x88a8	9600	Auto	Click to edit...
NNI 1:1:1:GIGE:12				0x88a8	9600	Auto	Click to edit...
MTNGRV-204-3							
Switch 1							
NNI 1:1:1:GIGE:11				0x88a8	9600	Auto	Click to edit...
OTTAWA-SA-810-53							
Switch 1							
UNI LAG 2	Click to add...						Click to edit...
1:1:1:GIGE:4				[Not Applicable]	9600	Auto	Click to edit...
NNI 1:1:1:GIGE:2				0x88a8	9600	Auto	Click to edit...
10.1.204.7							
Switch 1							
NNI 1:1:1:GIGE:1				0x88a8	9600	Auto	Click to edit...

- f. To filter your view, click the **All**, **Endpoints**, or **NNI** tabs to view all ports, view only UNI and ENNI ports, or view only NNI ports (both internal and endpoint) respectively.
- g. To edit the list of ports, proceed as follows:
- To remove a port from the service, right-click the port or LAG entry and select **Remove Port**, or select the port or LAG entry and click

- If you remove an auto-selected NNI port from the list, a **Revert NNIs** option appears. This option allows you to add the NNI back to the list.



**NOTE:** Reverting only adds back the auto-provisioned NNIs to this list. Any change you previously made to the NNI port, such as changing the service profiles, remain in effect and are not reverted.

- If you remove a UNI or ENNI port, all internal NNI ports that have been auto-selected due to that UNI or ENNI port are also removed.
- To add members to a LAG, right-click the LAG entry and select **Add LAG Member(s)**.
- To remove a member from a LAG, right-click the LAG member and select **Remove LAG Member**.
- To add more ports, repeat 2.



**NOTE:** By adding or removing internal NNIs, you have full control over what NNIs (auto-selected or otherwise) are included in the service. In some situations, it might be necessary for you to manually delete internal NNIs in this manner. For more information, see [“Auto-provisioning NNIs” on page 347](#).



**NOTE:** Any internal NNIs that will be added due to GVRP are not shown, as this is performed outside of PSM.

3. Set the port-based attributes (optional).
  - a. Click on the **Details** tab.
  - b. Set the port-based attributes by clicking in the appropriate box.



Table 42: Port-based Attributes

Attribute	Description	Range	Default
VLAN Mappings	<p>For a UNI port, this specifies the customer VLAN ID(s) that map to the service, and only applies to virtual services:</p> <ul style="list-style-type: none"> <li>For the Virtual Single service type, specify a single VLAN ID.</li> <li>For the Virtual Multiple service type, specify one or more VLAN IDs as a comma-separated list (e.g. 2000, 2200) or a range (e.g. 2000-2100) or both.</li> <li>For the Virtual Untagged service type, PSM populates this field with the C-PVID that has been set for the port.</li> </ul> <p><b>NOTE:</b> If CVLAN Translation is enabled, only one customer VLAN ID mapping can be specified.</p> <p>For an ENNI port, this specifies the external VLAN ID that maps to the service. Only one VLAN ID can be specified. This field is mandatory.</p> <p>This field is not applicable to NNI ports.</p>	<p>UNI: 1 to 4094</p> <p>ENNI: 2 to 4094</p>	None
Ingress Service Profile	<p>This is the service or bandwidth policy to apply at the ingress. Select the available policies using the drop-down list or click on the ellipsis to see more details. See <a href="#">“Managing Profile Templates” on page 428</a> for more information on how to create profiles.</p> <p><b>NOTE:</b> Service policies are not supported on the BT1805, BT1821, and BT1822.</p>	Not applicable	None
Egress Service Profile	<p>This is the service or bandwidth policy to apply at the egress. Select the available policies using the drop-down list or click on the ellipsis to see more details. See <a href="#">“Managing Profile Templates” on page 428</a> for more information on how to create profiles.</p> <p><b>NOTE:</b> Service policies are not supported on the BT1805, BT1821, and BT1822.</p> <p><b>NOTE:</b> This field is not supported on NNI ports on BT1800 Series network elements.</p>	Not applicable	None
TPID	<p>This shows the outer TPID used at the NNI or ENNI for a stacked Ethernet frame. This field cannot be changed.</p> <p>This field is not applicable to UNI ports.</p>	Not applicable	0x88a8

Table 42: Port-based Attributes (continued)

Attribute	Description	Range	Default
Max Frame	<p>This is the maximum frame size (in bytes) for the port.</p> <p>For UNI ports on BTI7000 Series NEs, this value is not used. The "Max Frame Size" defined for the service is used instead. However, the service "Max Frame Size" must still be less than or equal to this value.</p> <p>For UNI ports on BTI700 Series and BTI800 Series NEs, this value is used instead of the service "Max Frame Size".</p> <p>For NNI ports, this value is always used.</p> <p>If the "Max Frame Size" is already set for this port on the NE, and if the value is not within the valid range, PSM will set the "Max Frame Size" on the port to the default value.</p>	<p>UNI: 1522 to 9600</p> <p>NNI, ENNI: 1526 to 9600</p>	<p>UNI: 1522</p> <p>NNI, ENNI: 9600</p>
Media Rate	This specifies the Ethernet mode and media rate.	<p>Auto</p> <p>Full 10 Mb/s</p> <p>Half 10 Mb/s</p> <p>Full 100 Mb/s</p> <p>Half 100 Mb/s</p> <p>Full 1000 Mb/s</p> <p>Half 1000 Mb/s</p>	Auto
<b>EPTREE and EVPTREE services (BTI7000 Series only)</b>			
Forwarding	<p>This indicates whether the UNI or ENNI port is a root node or a leaf node. There can be multiple root and leaf nodes. If all nodes are root nodes, the resulting service is a LAN.</p> <p>This field is not applicable for NNI ports.</p>	Normal (root) or Leaf	Normal

## 4. Set the advanced switch and port attributes.



**NOTE:** Not all attributes are supported on every device.

- a. To configure advanced switch attributes, click the ellipsis in the Advanced Settings column for the switch entry.

Configure the switch attributes according to the following table.

**Table 43: Advanced Switch Attributes**

Attributes	Range of Values	Applicable to:			Description
		BTI700	BTI800	BTI7000	
Service Settings (switch)					
CVLAN Translation	On or Off	BTI712	Yes	Yes	Allows the customer VLAN ID to be remapped for all ports on the switch with virtual services.
		BTI718			This attribute has the opposite meaning of the MEF CE-VLAN ID Preservation attribute.
		BTI718E			
SLA Measurement Profile	Provisioned profiles	No	No	Yes	Applies to UNI ports. This attribute can only be set after the service has been activated and MEPs have been created.
Control Frame Profile	Provisioned profiles	No	Yes	No	Sets the L2CP EVC profile.
					Read/write for BTI805, BTI821, BTI822.
					Read-only for BTI810.

When you are finished configuring the advanced switch settings, click **OK**.

- b. To configure advanced port attributes for a regular (non-LAG) port, click the ellipsis in the Advanced Settings column for the port entry.

**Table 44: Advanced Port Attributes**

Attributes	Range of Values	Applicable to:			Description
		BTI700	BTI800	BTI7000	
Service					
E-FPSD	On or Off	No	Yes	Yes	Applies to optical UNI ports for EPLINE services.  For BTI800 Series equipment, this attribute can only be set after the service has been activated and MEPs have been created.
TPID Action	None, Aware, Blind	No	No	Yes	Applies to UNI ports for EPLINE and EPLAN services.

Table 44: Advanced Port Attributes (continued)

Attributes	Range of Values	Applicable to:			Description
		BTI700	BTI800	BTI7000	
Service Map Profile	Provisioned templates and service map profiles	BTI712 BTI718	No	Yes	List of provisioned templates and service map profiles. Applies to UNI ports with virtual services.
Service Map Sequence	1-100, default 50	BTI712 BTI718	No	Yes	The sequence number of the service map. A service map with a lower sequence is evaluated first. Applies to UNI ports with virtual services.
<b>Layer 1</b>					
Wavelength	Copper SFP, 850nm to 1560.61nm	No	No	Yes	The wavelength of the transceiver in nm, or a copper SFP or port. This attribute can only be changed if you are creating the port as part of this service activation. If the port already exists, and you are including it as part of this service activation, you cannot change its value.
Circuit ID	1 to 32 alphanumeric characters	No	No	Yes	The circuit identifier of the port.
Description	String	No	Yes	Yes	User-defined description for the circuit ID.
<b>Layer 2</b>					
Service Type	Private Virtual Single Virtual Multiple Virtual Untagged	BTI718E	Yes	Yes	<p>The UNI service type:</p> <ul style="list-style-type: none"> <li>Private - service multiplexing is off, bundling is on, all-to-one bundling is on</li> <li>Virtual Single - service multiplexing is on, bundling is off, all-to-one bundling is off</li> <li>Virtual Multiple - service multiplexing is on, bundling is on, all-to-one bundling is off</li> <li>Virtual Untagged - a special setting to support the situation where the local UNI is untagged and the remote UNI is tagged</li> </ul> <p><b>NOTE:</b> This is not the same attribute as the Ethernet service type in <a href="#">“Service Types” on page 346</a>.</p>
C-PVID	1 to 4094, default is unselected	BTI718E	Yes	Yes	Specifies the customer's default VLAN ID. This attribute is required on UNI ports running a virtual untagged service, but is optional for other service types.

Table 44: Advanced Port Attributes (continued)

Attributes	Range of Values	Applicable to:			Description
		BTI700	BTI800	BTI7000	
Control Frame Profile	Provisioned profiles	No	Yes	Yes	<p>Sets the L2CP UNI profile. See the documentation for the respective devices for details. Applies to UNI ports.</p> <p>Read/write for BTI805, BTI821, BTI822, and BTI7000 equipment.</p> <p>Read-only for BTI810.</p>
MSTP Enabled	On or Off	No	No	Yes	Select to enable MSTP. Applies to UNI ports.
CCM Enabled	On or Off	No	No	Yes	Select to enable CCMs. Applies to UNI ports.
SVLAN Translation	<p>On or Off, default is Off.</p> <p>If On, specify the external SVLAN ID from 2 to 4094.</p>	No	No	Yes	<p>Specify the external SVLAN ID. This SVLAN ID is mapped to the internal SVLAN ID from <a href="#">Table 41 on page 351</a>. Applies to NNI ports only.</p> <p><b>NOTE:</b> To specify the external VLAN mapping for ENNI ports, see <a href="#">Table 42 on page 357</a></p> <p>This attribute can only be configured when you first add the NNI to the service. You cannot change the configuration after the NNI has been added to the service. To change the configuration after the NNI has been added, you must first remove the NNI and then add it back to the service.</p> <p>This mapping is 1:1. You cannot specify an external SVLAN ID that is mapped to another service on this same port.</p> <p>If SVLAN Translation is enabled, untagged frames will be discarded on ingress.</p> <p>SVLAN translation cannot co-exist with GVRP and MSTP. If SVLAN translation is enabled on an NNI that has GVRP and/or MSTP also enabled, PSM will automatically disable GVRP and/or MSTP. When the last SVLAN translation is removed from the NNI, PSM will automatically enable GVRP and/or MSTP if either or both were originally enabled.</p>

When you are finished configuring the advanced port settings, click **OK**.

- c. To configure port-based attributes for a LAG port, click the ellipsis in the Advanced Settings column for the LAG port entry.

Table 45: Advanced LAG Port Attributes

Attributes	Range of Values	Applicable to:			Description
		BTI700	BTI800	BTI7000	
Service					
Same asTable 44 on page 359.					
Layer 2					
Same as Table 44 on page 359.					
LAG					
Distribution Method	Source MAC  Destination MAC  Source and Destination MAC  Source IP  Destination IP  Source and Destination IP  Source Port  Destination Port	Yes	Yes	Yes	The LAG distribution method.
LACP Mode	BTI7000: Active, Passive, On  BTI718E: LACP, Static	BTI718E	No	Yes	The LACP mode. This sets the LACP mode for all members of the LAG. A setting of Active (LACP) means that the port will initiate LACP negotiation. A setting of Passive means that the port will not initiate LACP negotiation but will respond to it. A setting of On (Static) means that the port will neither initiate nor respond to LACP negotiation.
Max Links	1-8	Yes	No	Yes	The maximum number of links permitted in the LAG.
Min Links	1-8	BTI718E	No	No	The minimum number of links that must be up before the LAG is considered up.

When you are finished configuring the advanced LAG port settings, click **OK**.

- d. To configure port-based attributes for a LAG member, click the ellipsis in the Advanced Settings column for the LAG member entry.

**Table 46: Advanced LAG Member Attributes**

Attributes	Range of Values	Applicable to:			Description
		BTI700	BTI800	BTI7000	

#### Layer 1

Same as [Table 44 on page 359](#).

#### LAG Member

LACP Port Priority	0-65535	Yes	No	Yes	The LACP port priority.
LACP Wait Time	0-10 seconds	No	No	Yes	The LACP wait time.
LACP Mode	Active, Passive, On	No	No	Yes	The LACP mode. This sets the LACP mode for individual members of the LAG.
LACP Timeout	Long, Short	No	No	Yes	The LACP timeout period.

When you are finished configuring the advanced LAG member settings, click **OK**.

5. Click **Activate**. The service is activated.

For information about error messages, see [“Service Activation Error Messages” on page 549](#).

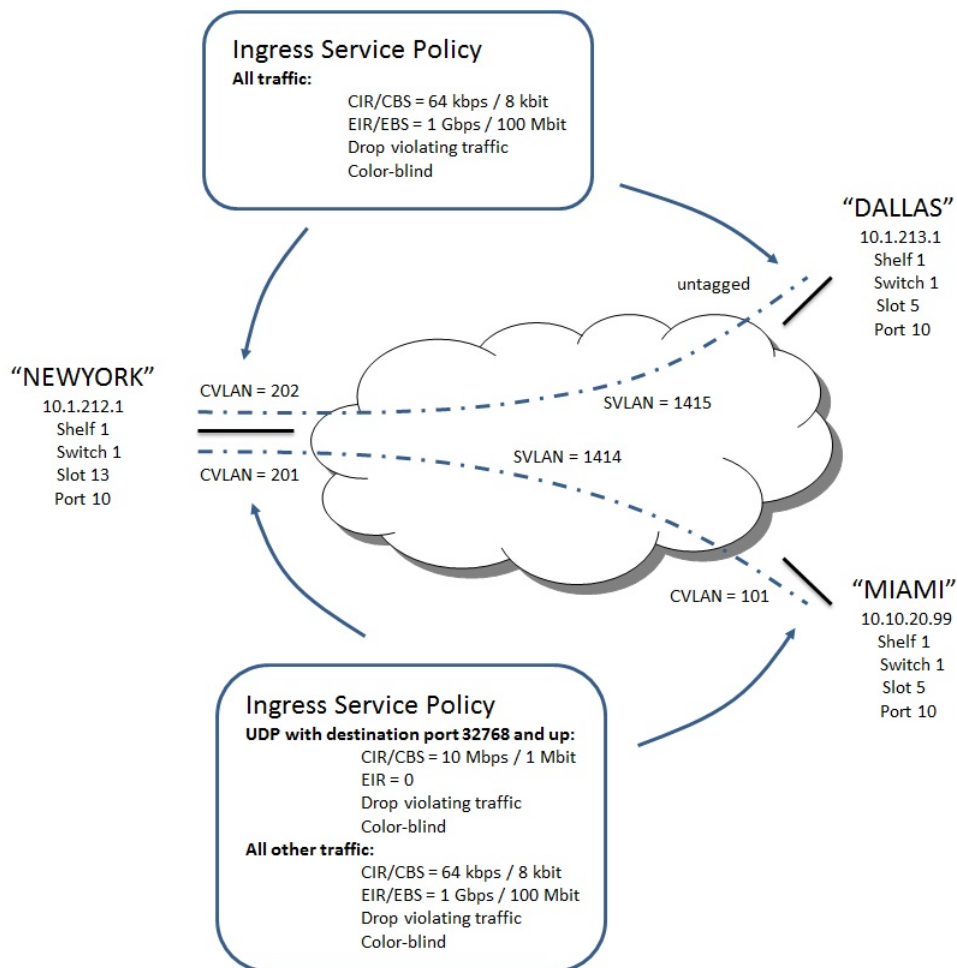


**NOTE:** You must wait for the activation tasks to complete before performing any other operation on the NEs affected by this activation.

## Example: Activating an EVPLINE Service

This is an example of how to use PSM to activate two different types of EVPLINE services. The first service, between **NEWYORK** and **MIAMI**, requires CVLAN translation and no bundling. The second service, between **NEWYORK** and **DALLAS**, requires connectivity between a tagged and an untagged interface, also with no bundling. This is shown in [Figure 78 on page 364](#) along with the desired service policies.

Figure 78: Example: EVPLINE Services



**NOTE:** Before configuring the service, ensure that the PVX cards, virtual switches, and the NNIs have all been created on the appropriate network elements. For information on how to do this, refer to the *BT17000 SeriespacketVX Solutions Guide*.

This example is divided into two parts, setting up the EVPLINE service between **NEWYORK** and **MIAMI** with CVLAN translation, and setting up the service between **NEWYORK** and **DALLAS** with the virtual untagged option.



## Part 1: Setting Up the EVPLINE Service with CVLAN Translation

The service between **NEWYORK** (10.1.212.1:1-1-13-10) and **MIAMI** (10.10.20.99:1-1-5-10) requires CVLAN translation and no bundling. CVLAN ID **201** is mapped to the service at the **NEWYORK** UNI and CVLAN ID **101** is mapped to the service at the **MIAMI** UNI. The UNI ports are initially unprovisioned in this example.

1. On the PSM Client, click the **Service Activation** button on the toolbar, as shown.

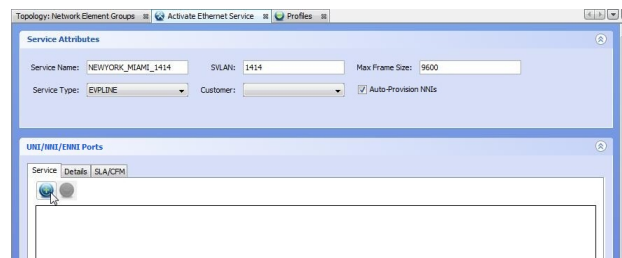


Choose **Ethernet** from the pulldown menu.

The Activate Service panel is displayed.



2. Enter the service attributes and click on the plus sign to start adding interfaces.



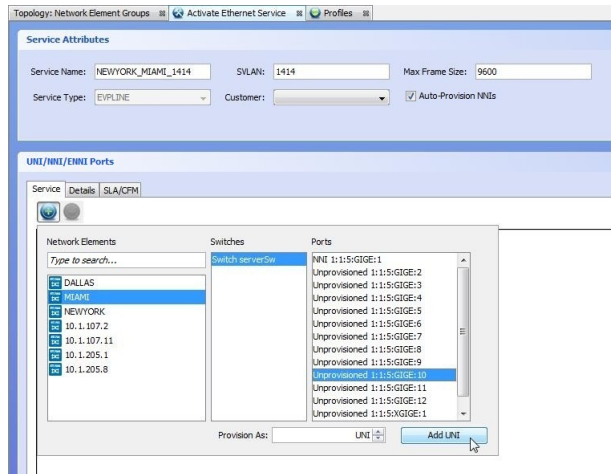
3. Add the **NEWYORK** UNI to the service by highlighting the "Unprovisioned 1:1:13:GIGE:10" port and selecting **Provision As:UNI**.



**NOTE:** The switches and ports only appear in this menu if they have been properly configured on the NE. See the *BT17000 Series packetVX Solutions Guide* for information on how to add and configure a switch.

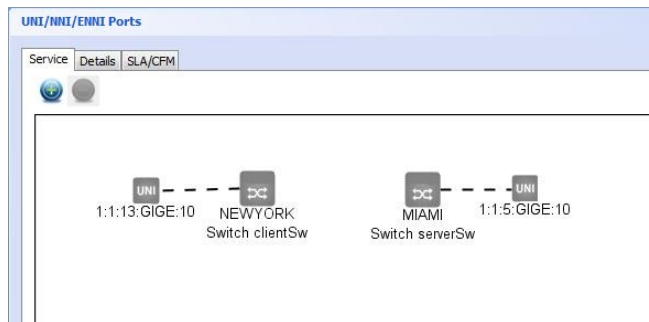
When you are done, click **Add UNI**.

4. Add the **MIAMI** UNI to the service by highlighting the "Unprovisioned 1:1:5:GIGE:10" port and selecting **Provision As:UNI**.



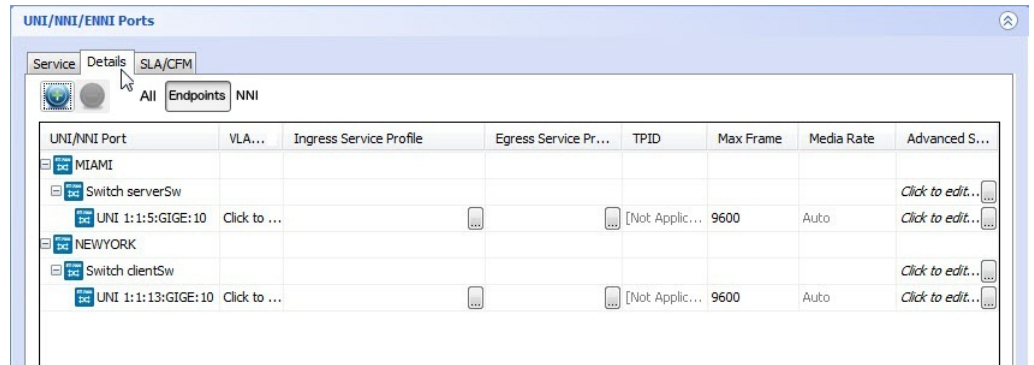
When you are done, click **Add UNI**.

The result is the following topology.

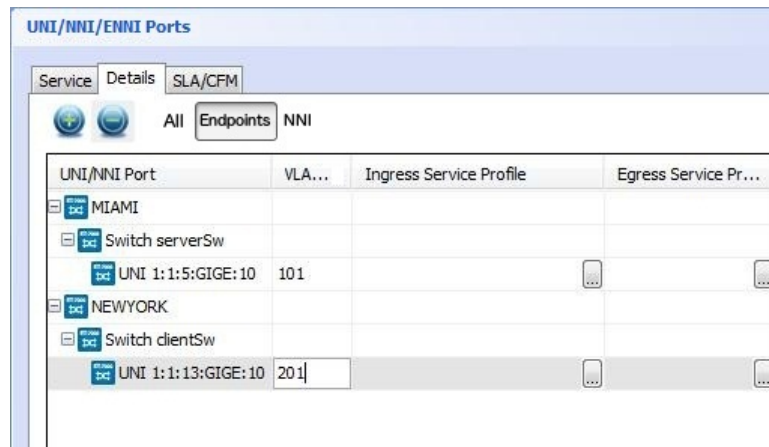


**NOTE:** The NNIs do not need to be explicitly added if the network elements are running GVRP. When working with network elements that do not support GVRP such as the BT1700 Series or BT1800 Series devices, you will need to add the appropriate NNIs to the service or use the Auto-Provision NNIs feature.

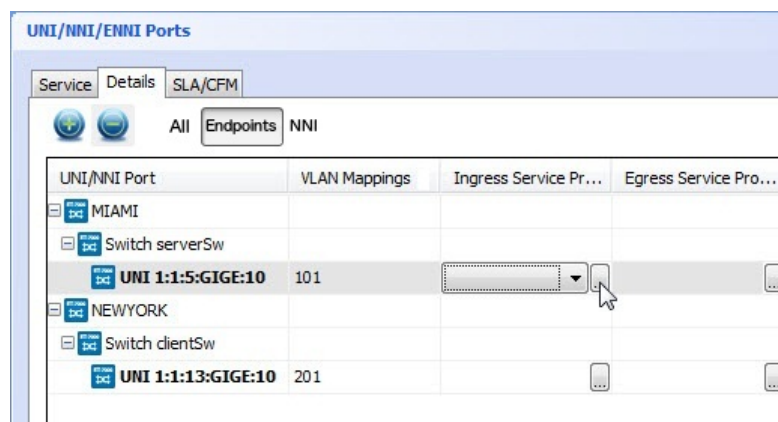
5. Select the **Details** tab in the UNI/NNI Ports pane to enter more detailed information for each UNI.



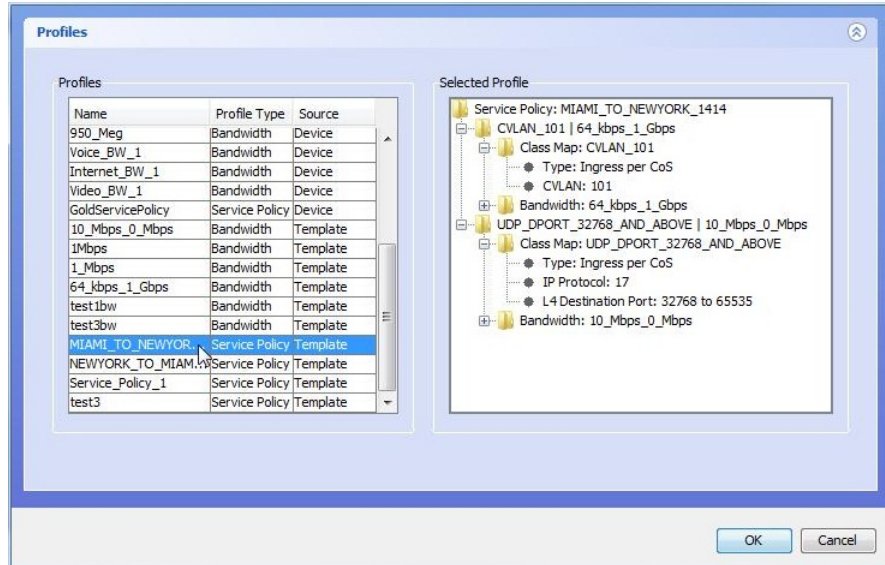
6. Set the CVLAN mappings by clicking in the box and entering the desired CVLAN values for each UNI. In this example, the **MIAMI** UNI maps CVLAN ID **101** to the service, and the **NEWYORK** UNI maps CVLAN ID **201** to the service.



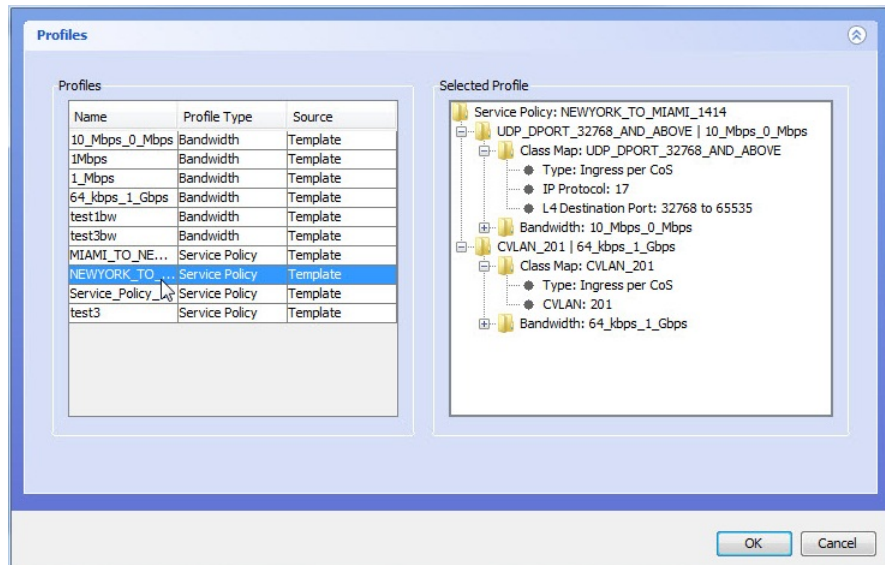
7. Click on the pulldown menu or the ellipsis in the Ingress Service Profile column for the **MIAMI** UNI.



8. Select the desired ingress service profile by highlighting it and clicking **OK**. When a profile is highlighted, the profile details are displayed in the Selected Profile pane. In this example, the desired policy has already been defined.



9. Repeat for the **NEWYORK UNI**.



10. Open the Advanced Settings menu for the **MIAMI UNI** by clicking on the ellipsis.

UNI/NNI Port	VLA...	Ingress Service Profile	Egress Service Pr...	TPID	Max Frame	Media Rate	Advanced S...
MIAMI							
Switch serverSw							Click to edit...
UNI 1:1:5:GIGE:10	101	MIAMI_TO_NEWYORK_1414...	[Not Applic...	9600	Auto		Click to edit...
NEWYORK							
Switch clientSw							Click to edit...
UNI 1:1:13:GIGE:1	201	NEWYORK_TO_MIAMI_1414...	[Not Applic...	9600	Auto		Click to edit...

11. Select the service type from the pulldown menu and click **OK**.

In this example, the Service Type is **Virtual Single**, meaning that service multiplexing is on, bundling is off and all-to-1 bundling is off. Leave the C-PVID unchecked.

**Advanced Settings**

Service

Service Map Profile: [Dropdown] [Ellipsis]

Service Map Sequence: 50

Layer 2

Service Type: [Virtual Multiple] [Dropdown]

Control Frame Profile: [Virtual Single] [Dropdown]

MSTP Enabled: [Virtual Multiple] [Dropdown]

C-PVID: ☐ [Disabled]

Layer 1

Circuit ID: [Text Box]

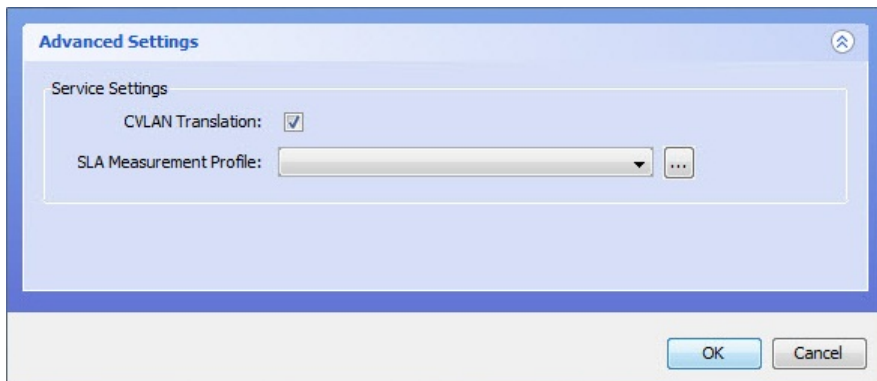
Description: [Text Box]

OK Cancel

12. Open the Advanced Settings menu for the **MIAMI** switch by clicking on the ellipsis.

UNI/NNI Port	VLA...	Ingress Service Profile	Egress Service Pr...	TPID	Max Frame	Media Rate	Advanced S...
MIAMI							
Switch serverSw							Click to edit...
UNI 1:1:5:GIGE:10	101	MIAMI_TO_NEWYORK_1414...	[Not Applic...	9600	Auto		Click to edit...
NEWYORK							Click to edit...
Switch clientSw							Click to edit...
UNI 1:1:13:GIGE:1	201	NEWYORK_TO_MIAMI_1414...	[Not Applic...	9600	Auto		Click to edit...

13. Select **CVLAN Translation** and click **OK**. This attribute has the opposite meaning of the Metro Ethernet Forum CE-VLAN ID Preservation attribute. In other words, **CVLAN Translation = yes** is equivalent to **CE-VLAN ID Preservation = no**.



14. Repeat steps 10 through 13 for the **NEWYORK** UNI.

15. Click **Activate**.

It is good practice to check whether the activate completes successfully. Open the Tasks panel to check.

Tasks			
Task Id	Description	Type	State
4266609	NEWYORK_MIAMI_1414	Ethernet Service Creation	FINISHED

For information about error messages, see [“Service Activation Error Messages”](#) on page 549

## Part 2: Setting Up the EVPLINE Service with the Virtual Untagged Option

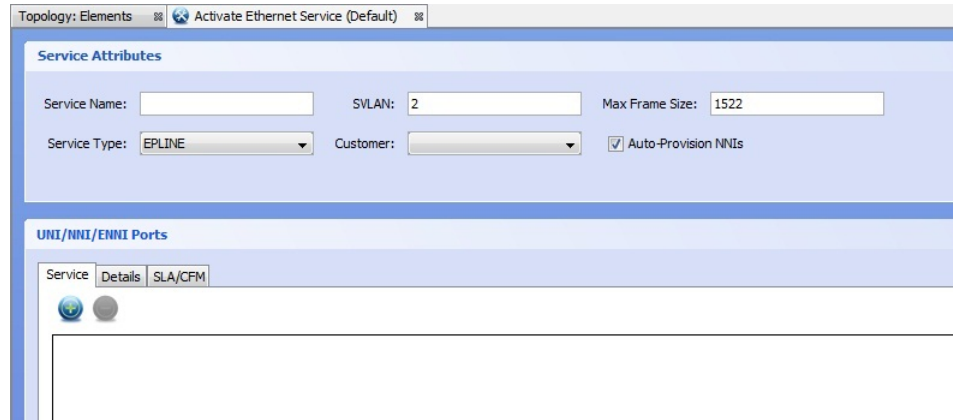
The service between **NEWYORK** (10.1.212.1:1-1-13-10) and **DALLAS** (10.1.213.1:1-1-5-10) requires connectivity between a tagged and an untagged interface. CVLAN ID **202** is mapped to the service at the NEWYORK UNI, while the DALLAS UNI is an untagged interface. In this example, the **NEWYORK** UNI port has already been provisioned but the DALLAS UNI port is unprovisioned.

1. On the PSM Client, click the **Service Activation** button on the toolbar, as shown.

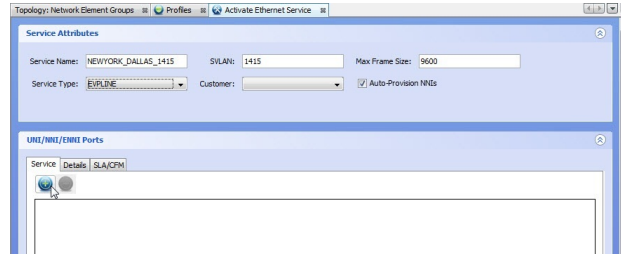


Choose **Ethernet** from the pulldown menu.

The Activate Service window is displayed.



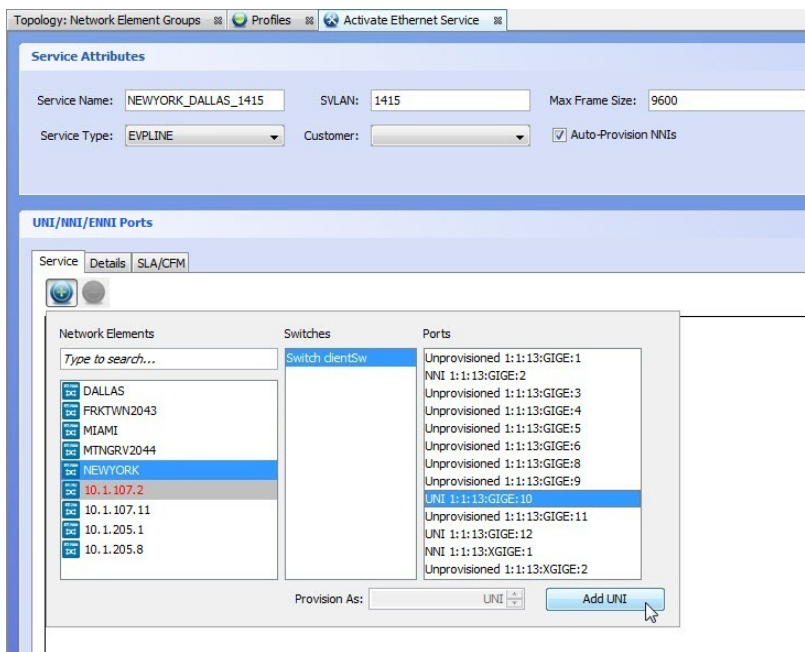
2. Enter the service attributes and click on the plus sign to start adding interfaces.



3. Add the **NEWYORK** UNI to the service by highlighting the "UNI 1:1:13:GIGE:10" port.

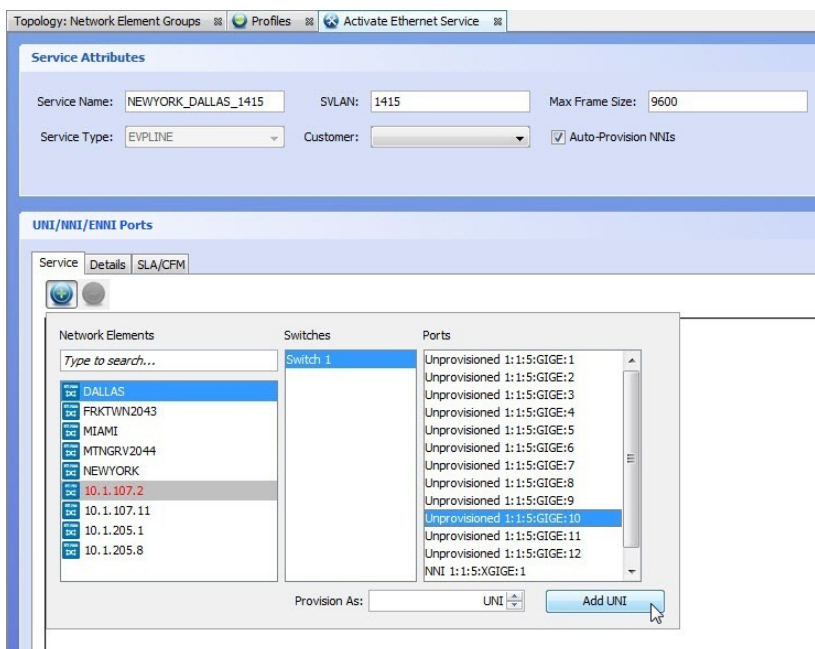


**NOTE:** The switches and ports only appear in this menu if they have been properly configured on the NE. See the *BT17000 Series packetVX Solutions Guide* for information on how to add and configure a switch.



When you are done, click **Add UNI**.

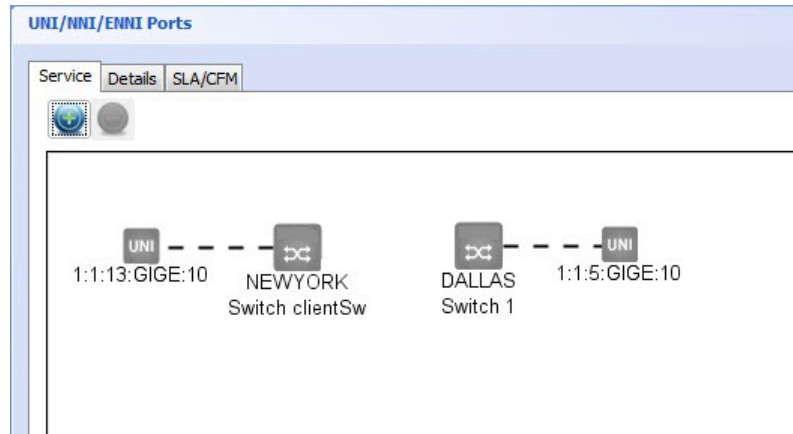
4. Add the **DALLAS** UNI to the service by highlighting the "Unprovisioned 1:1:5:GIGE:10" port and selecting **Provision As:UNI**.



When you are done, click **Add UNI**.

The result is the following topology.



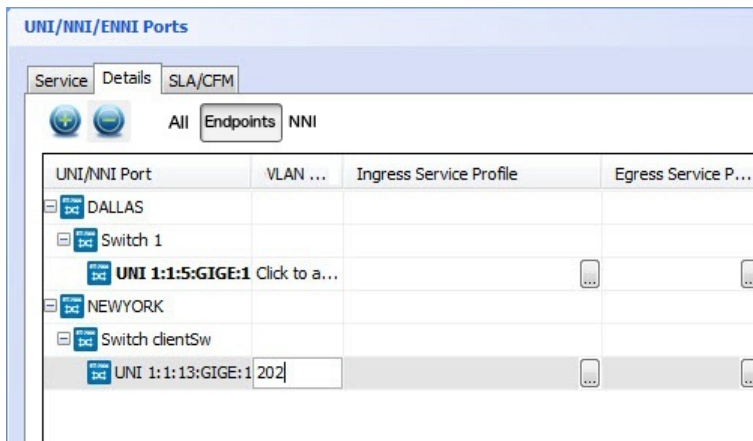


**NOTE:** The NNIs do not need to be explicitly added if the network elements are running GVRP. When working with network elements that do not support GVRP such as the BT1700 Series or BT1800 Series devices, you will need to add the appropriate NNIs to the service or use the Auto-Provision NNIs feature.

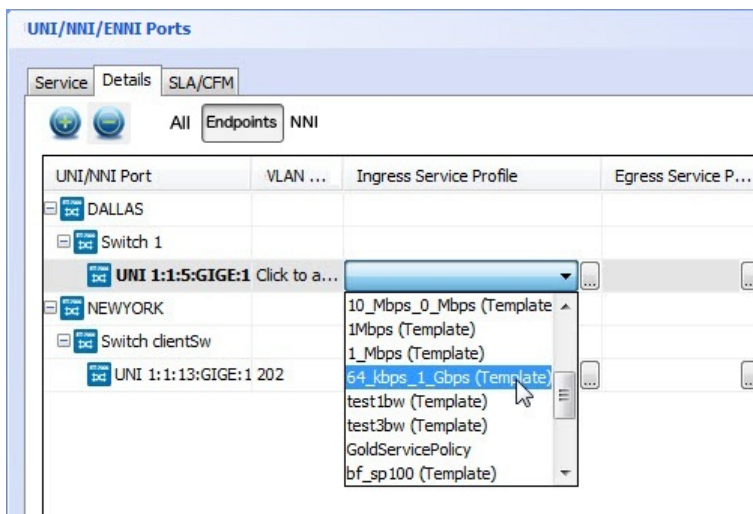
5. Select the Details tab in the UNI/NNI Ports pane to enter more detailed information for each UNI.

UNI/NNI Port	VLAN ...	Ingress Service Profile	Egress Service P...	TPID	Max Frame	Media Rate	Advanced S...
DALLAS							
Switch 1							Click to edit...
UNI 1:1:5:GIGE:1	Click to a...			[Not Applic...	9600	Auto	Click to edit...
NEWYORK							
Switch clientSw							Click to edit...
UNI 1:1:13:GIGE:1	Click to a...			[Not Applic...	9600	Auto	Click to edit...

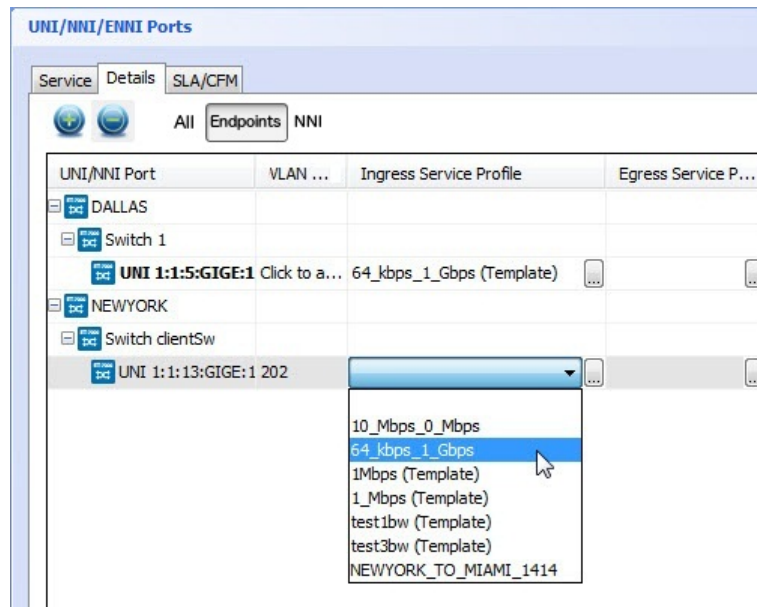
6. Set the CVLAN mappings by clicking in the box and entering the desired CVLAN values for each UNI. In this example, the **NEWYORK** UNI maps CVLAN ID 202 to the service while the **DALLAS** UNI has no mapping.



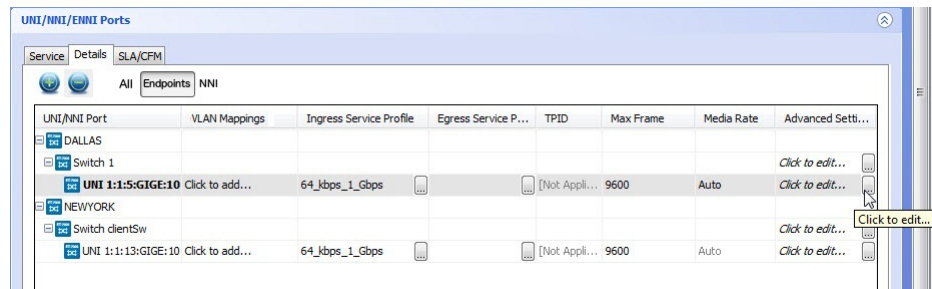
- Click on the pulldown menu or the ellipsis in the Ingress Service Profile column for the **DALLAS** UNI. Select the desired bandwidth profile. In this example, the desired bandwidth profile has already been defined.



- Repeat for the **NEWYORK** UNI.



9. Open the Advanced Settings menu for the **DALLAS** UNI by clicking on the ellipsis.



10. Select the service type from the pulldown menu and click **OK**.

The Service Type should be **Virtual Untagged**, with C-PVID set to the value used at the remote endpoint, in this case, **202**. Ingress traffic at the **DALLAS** site will be automatically tagged with this value, while egress traffic will automatically have this tag stripped.

The **Advanced Settings** dialog box is shown. It contains the following fields:

- Service**
  - Service Map Profile: [Dropdown]
  - Service Map Sequence: 50
- Layer 2**
  - Service Type: Virtual Multiple (dropdown menu is open showing options: Private, Virtual Single, Virtual Multiple, Virtual Untagged)
  - Control Frame Profile: [Dropdown]
  - MSTP Enabled: [Checkbox]
  - SVLAN Translation: [Checkbox]
  - C-PVID: [Checked] 202
- Layer 1**
  - Circuit ID: [Text Field]
  - Description: [Text Field]

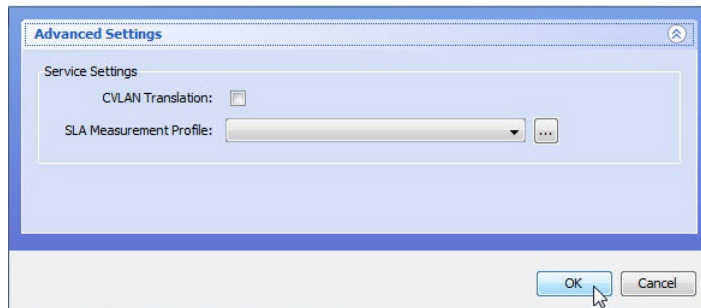
Buttons: OK, Cancel

11. Open the Advanced Settings menu for the **DALLAS** switch by clicking on the ellipsis.

The **UNI/NNI/ENNI Ports** table is shown. It has columns: UNI/NNI Port, VLAN Mappings, Ingress Service Profile, Egress Service P..., TPID, Max Frame, Media Rate, and Advanced Setti... (truncated).

UNI/NNI Port	VLAN Mappings	Ingress Service Profile	Egress Service P...	TPID	Max Frame	Media Rate	Advanced Setti...
DALLAS							
Switch 1							
UNI 1:1:5:GIGE:10	Click to add...	64_kbps_1_Gbps		[Not Appli...]	9600	Auto	Click to edit...
NEWYORK							
Switch clientSw							
UNI 1:1:13:GIGE:10	Click to add...	64_kbps_1_Gbps		[Not Appli...]	9600	Auto	Click to edit...

12. Ensure CVLAN Translation is unchecked and click **OK**. This attribute has the opposite meaning of the Metro Ethernet Forum CE-VLAN ID Preservation attribute. In this example, the **DALLAS** site only expects untagged traffic, so this parameter is not applicable.



13. Modify the Advanced Settings attributes for the **NEWYORK** UNI. Ensure the Service Type is set to **Virtual Single**, C-PVID is unchecked, and CVLAN Translation is unchecked, meaning that CE-VLAN ID preservation is on, service multiplexing is on, bundling is off, and all-to-1 bundling is off.

14. Click **Activate**.

It is good practice to check whether the activate completes successfully. Open the Tasks panel to check.

Tasks			
Task Id	Description	Type	State
4674578	NEWYORK_DALLAS_1415	Ethernet Service Creation	FINISHED

For information about error messages, see [“Service Activation Error Messages” on page 549](#)

### Example: Activating an Ethernet Service on a Multi-chassis LAG

This is an example of how to activate an Ethernet service on a multi-chassis LAG UNI. A multi-chassis LAG UNI has member links that terminate on two different network elements. If one link or network element fails, the service continues to operate over the other link. Service activation for a multi-chassis LAG UNI is very similar to service activation on a regular UNI.

This example focuses on details that are specific to multi-chassis LAG service activation.

1. Select **Tools >Service Activation >Ethernet**.

The **Activate Ethernet Service** panel is displayed.



**NOTE:** If multiple domains exist, you will need to select the domain first.

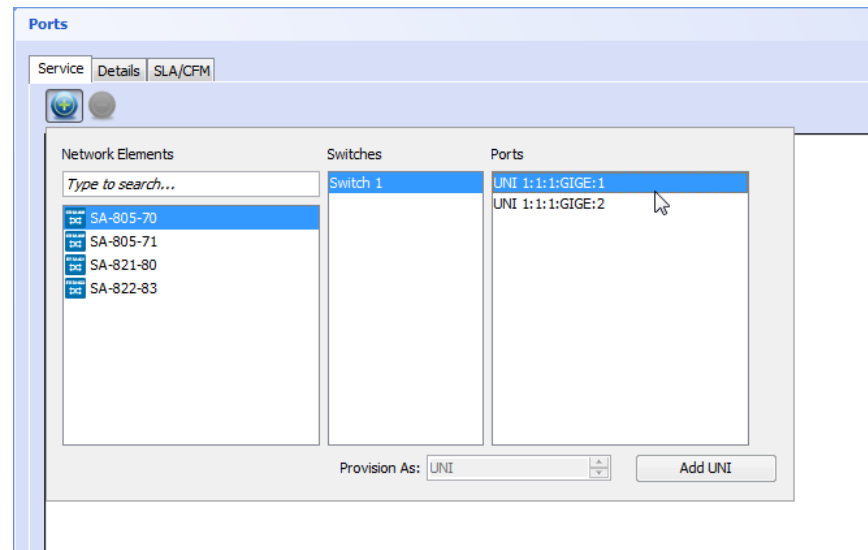
2. Enter the service attributes and click on the plus symbol to start adding UNI ports.
  - a. Select a multi-chassis LAG port and click **Add UNI LAG**.

You can select any member of the multi-chassis LAG as the UNI endpoint. When you select a multi-chassis LAG member, PSM automatically adds all members of that same multi-chassis LAG to the service.

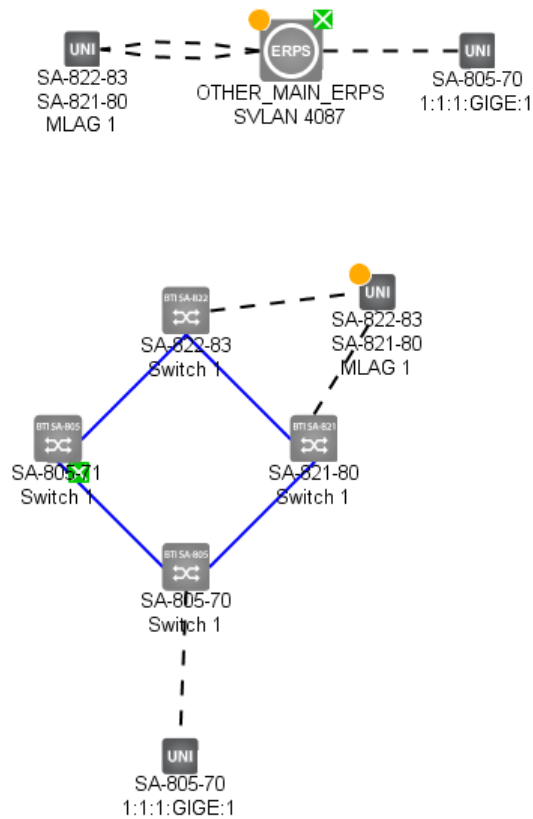
You can distinguish between different multi-chassis LAGs by the MLAG index. For example, to select MLAG 1, simply select a member belonging to MLAG 1.

- b. Add the other UNI endpoint as you normally do.

For example:



The result is the following topology.



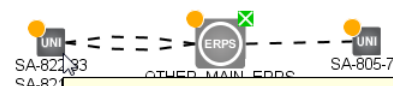
3. Select the **Details** tab to enter more detailed information for each UNI.

Only parameters for the active multi-chassis LAG member can be configured. PSM automatically copies the parameters from the active member to the non-active members. You cannot change the parameters for the non-active members directly. In the figure below, the active multi-chassis LAG member is on SA-821-80, and the standby multi-chassis LAG member is on SA-822-83.

Service Details SLA/CFM				
All Endpoints NNI				
UNI/NNI Port	VLAN Mappings	Ingress Service Profile	Egress Service Profile	TPID
SA-805-70				
Switch 1				
UNI 1:1:1:GIGE:1	Click to add...			[Not Applicab
SA-821-80				
Switch 1				
UNI LAG 3 (MLAG 1)	Click to add...			[Not Applicab
1:1:1:GIGE:7				
SA-822-83				
Switch 1				
UNI LAG 3 (MLAG 1)				[Not Applicab
1:1:1:GIGE:7				

#### 4. Click **Activate**.

The PSM server sends the activation request to the network element. You can monitor the status of the request through the **View > Server > Tasks** window. The changes are shown in PSM a short while after the task completes successfully.

	
<b>SA-822-83</b> <b>Port</b> UNI LAG 3 (MLAG 1) MAC Address: 00:14:d0:60:02:12 <b>Layer 1</b> Description: MC-LAG-7 <b>Layer 2</b> State: Down (Disabled) L2CP: uni-evpl <b>LAG</b> Members: 1:1:1:GIGE:7 Max Links: 8 <b>MLAG</b> Mode: Active/Standby, Non-Revertive State: Standby (Standby) <b>CFM</b> MEP: 4626 <b>Service</b> CVLAN Mapping(s): 100-105 Ingress Profile: bwg1 <b>Alarms:</b> Cr Ma Mi Ack 0 1 0 0	<b>SA-821-80</b> <b>Port</b> UNI LAG 3 (MLAG 1) MAC Address: 00:14:d0:60:01:fd <b>Layer 1</b> Description: MC-LAG-7 <b>Layer 2</b> State: Up (Enabled) L2CP: uni-evpl <b>LAG</b> Members: 1:1:1:GIGE:7 Max Links: 8 <b>MLAG</b> Mode: Active/Standby, Non-Revertive State: Active (Active) <b>CFM</b> MEP: 4626 Remote MEPs: 4115 <b>Service</b> CVLAN Mapping(s): 100-105 Ingress Profile: bwg1 <b>Alarms:</b> Cr Ma Mi Ack 0 2 0 0

For information about error messages, see [“Service Activation Error Messages” on page 549](#)



## Example: Activating EVPLAN and EVPLINE Services Using Service Maps for Flow Redirection

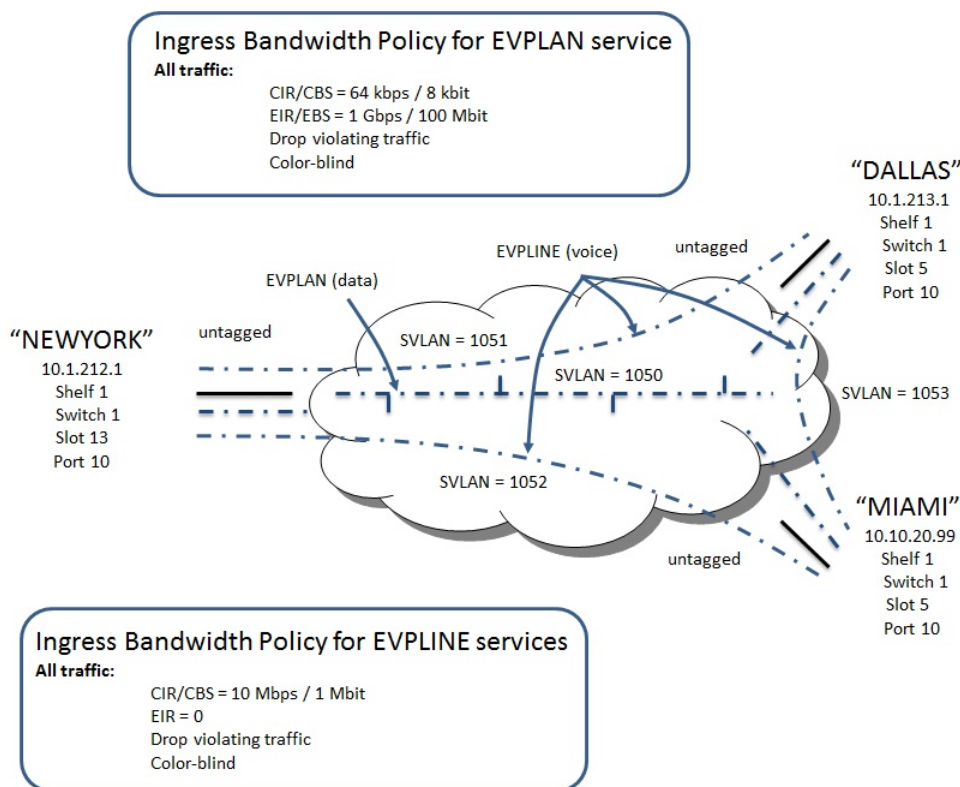
This is an example of how to use PSM to activate two different types of services for three endpoints. The first is a typical multipoint-to-multipoint EVPLAN service for regular data connectivity and the second is a set of separate EVPLINE point-to-point services for voice connections. This models a corporate network where regular intranet traffic between sites use the EVPLAN service, while the lower latency, more stringent quality-of-service site-to-site voice traffic uses a special EVPLINE service. The assumption is that the network provider has set up low latency pathways for the EVPLINE traffic, perhaps with little or no CIR oversubscription on any of the network segments that comprise the path.



**NOTE:** Although the interfaces are untagged, the services are still considered virtual since more than one service is provided at each UNI. Therefore the services are EVPLINE and EVPLAN rather than EPLINE and EPLAN.

Figure 79 on page 382 shows the desired network configuration along with the bandwidth policies.

Figure 79: Example: EVPLINE and EVPLAN Services



**NOTE:** Before configuring the service, ensure that the PVX cards, virtual switches, and the NNIs have all been created on the appropriate network elements. For information on how to do this, refer to the *BT17000 Series packetVX Solutions Guide*.

This example is divided into three parts: setting up the service maps, setting up the EVPLINE services, and setting up the EVPLAN service. The service maps are used to classify voice traffic for the EVPLINE services. Data traffic for the EVPLAN service do not require classification. Instead, CVLAN ID mapping and C-PVIDs are used to map data traffic to the EVPLAN service.

To keep this example short, some details covered in previous examples are omitted.

### Part 1: Setting Up the Service Maps

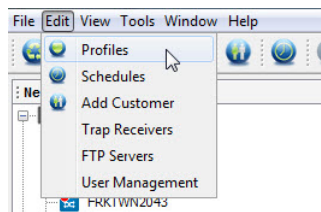
A service map must be created at each site to classify ingress packets for the voice service. In this example, voice traffic needs to be diverted to the EVPLINE service while all other traffic remains on the EVPLAN service. This is performed using a combination of class maps and service maps. A class map is a specific filter used to classify traffic, such as matching a destination port number. A service map is a collection of class maps, or in other words, a collection of filters. A match is declared in the service map if the ingress packet matches any of the filters specified in the collection of class maps.



**NOTE:** The terminology used by PSM differs slightly from that used by the CLI. Specifically, the CLI expands the notion of service policy to include service maps, while PSM treats the service map as distinct from service policy. The general configuration approach, however, remains the same.

In this example, all ingress SIP, RTP, and RTCP packets are considered to be voice traffic. The approach is therefore to create class maps to identify each of these protocols, and then group these class maps together into a service map that maps these packets to the EVPLINE service. The remaining traffic will be mapped to the EVPLAN service using CVLAN mapping.

1. Open the Profiles panel.

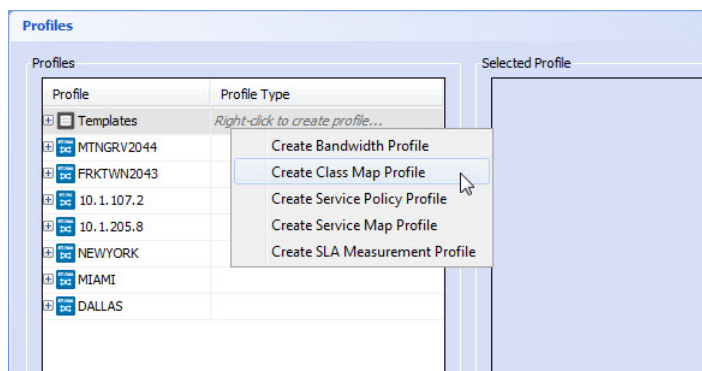


2. Create class map profiles to identify SIP, RTP, and RTCP traffic destined for **NEWYORK**.

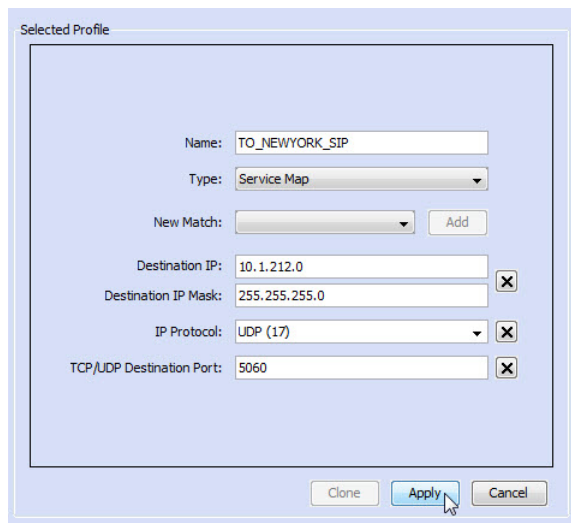


**NOTE:** The port numbers used below are for illustration purposes only. Actual port numbers might differ and might likely include a range.

- a. Right-click and select **Create Class Map Profile**.



- b. In the Selected Profile pane, enter the criteria for determining SIP traffic destined for the **NEWYORK** site. This is UDP traffic heading to the **10.1.212.x** subnet with a destination port of **5060**. Click **Apply**.



- c. Repeat to create a class map for RTP traffic destined for the **NEWYORK** site. This is UDP traffic heading to the **10.1.212.x** subnet with a destination port of **5004**. Click **Apply**.

Selected Profile

Name: TO\_NEWYORK\_RTP

Type: Service Map

New Match:  Add

Destination IP: 10.1.212.0

Destination IP Mask: 255.255.255.0

IP Protocol: UDP (17)

TCP/UDP Destination Port: 5004

Clone Apply Cancel

- d. Repeat to create a class map for RTCP traffic destined for the **NEWYORK** site. This is UDP traffic heading to the 10.1.212.x subnet with a destination port of **5005**. Click **Apply**.

Selected Profile

Name: TO\_NEWYORK\_RTCP

Type: Service Map

New Match:  Add

Destination IP: 10.1.212.0

Destination IP Mask: 255.255.255.0

IP Protocol: UDP (17)

TCP/UDP Destination Port: 5005

Clone Apply Cancel

This results in three class maps, classifying SIP, RTP, and RTCP traffic destined for **NEWYORK**.

3. Repeat to create class maps for SIP, RTP, and RTCP traffic destined the **MIAMI** site.

Selected Profile

Name: TO\_MIAMI\_SIP

Type: Service Map

New Match:

Destination IP: 10.10.20.0

Destination IP Mask: 255.255.255.0

IP Protocol: UDP (17)

TCP/UDP Destination Port: 5060

Clone Apply Cancel

Selected Profile

Name: TO\_MIAMI\_RTP

Type: Service Map

New Match:

Destination IP: 10.10.20.0

Destination IP Mask: 255.255.255.0

IP Protocol: UDP (17)

TCP/UDP Destination Port: 5004

Clone Apply Cancel

Selected Profile

Name:

Type:

New Match:

Destination IP:

Destination IP Mask:

IP Protocol:

TCP/UDP Destination Port:

4. Repeat to create class maps for SIP, RTP, and RTCP traffic destined for the **DALLAS** site.

Selected Profile

Name:

Type:

New Match:

Destination IP:

Destination IP Mask:

IP Protocol:

TCP/UDP Destination Port:

Selected Profile

Name: TO\_DALLAS RTP

Type: Service Map

New Match:  Add

Destination IP: 10.1.213.0

Destination IP Mask: 255.255.255.0

IP Protocol: UDP (17)

TCP/UDP Destination Port: 5004

Clone Apply Cancel

Selected Profile

Name: TO\_DALLAS RTCP

Type: Service Map

New Match:  Add

Destination IP: 10.1.213.0

Destination IP Mask: 255.255.255.0

IP Protocol: UDP (17)

TCP/UDP Destination Port: 5005

Clone Apply Cancel

5. Group the class maps by creating a service map profile to identify voice traffic destined for the **NEWYORK** site.
  - a. Right-click and select **Create Service Map Profile**.

Profiles

Profile	Profile Type
Templates	
MTNGRV2044	
FRKTWN2043	
10.1.107.2	
10.1.205.8	
NEWYORK	
MIAMI	
DALLAS	

Selected Profile

Create Bandwidth Profile  
Create Class Map Profile  
Create Service Policy Profile  
Create Service Map Profile  
Create SLA Measurement Profile



- b. In the Selected Profile pane, add the three **TO\_NEWYORK\_xxx** class maps created in the previous step. Click **Apply**.

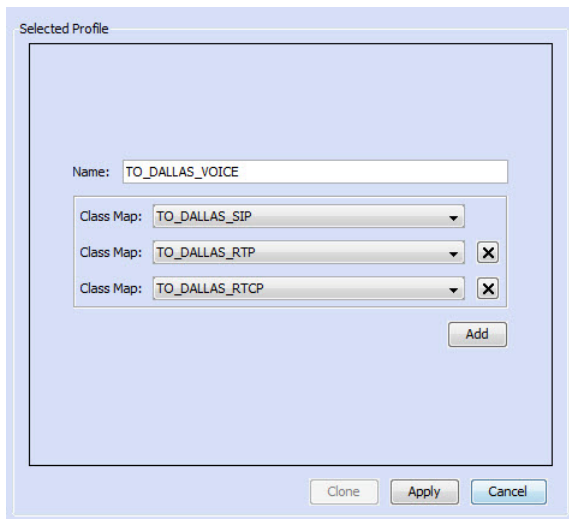
The screenshot shows the 'Selected Profile' configuration window. The 'Name' field is set to 'TO\_NEWYORK\_VOICE'. Below it, there are three 'Class Map' dropdown menus, each with a corresponding 'X' button to the right. The first dropdown is set to 'TO\_NEWYORK\_SIP', the second to 'TO\_NEWYORK\_RTP', and the third to 'TO\_NEWYORK\_RTCP'. An 'Add' button is located below the third dropdown. At the bottom of the window, there are three buttons: 'Clone', 'Apply' (highlighted with a mouse cursor), and 'Cancel'.

The result is a service map that identifies voice traffic destined for **NEWYORK**.

6. Repeat to create the service map for voice traffic destined for the **MIAMI** site.

The screenshot shows the 'Selected Profile' configuration window. The 'Name' field is set to 'TO\_MIAMI\_VOICE'. Below it, there are three 'Class Map' dropdown menus, each with a corresponding 'X' button to the right. The first dropdown is set to 'TO\_MIAMI\_SIP', the second to 'TO\_MIAMI\_RTP', and the third to 'TO\_MIAMI\_RTCP'. An 'Add' button is located below the third dropdown. At the bottom of the window, there are three buttons: 'Clone', 'Apply', and 'Cancel'.

7. Repeat to create the service map for voice traffic destined for the **DALLAS** site.

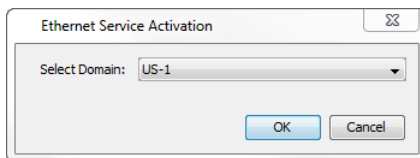


The required service maps have now been created.

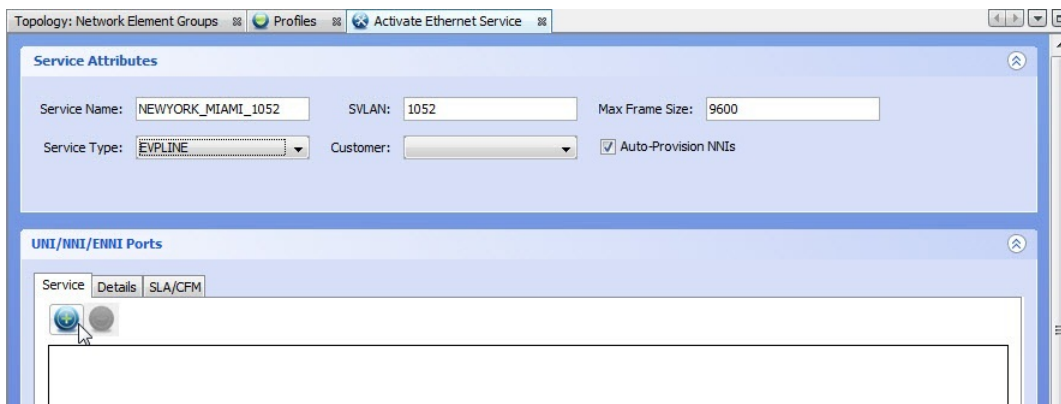
## Part 2: Setting Up the EVPLINE Services

All three EVPLINE services are identical.

1. Create the **NEWYORK** to **MIAMI** EVPLINE service.
  - a. On the PSM Client, click the **Service Activation** button on the toolbar and choose **Ethernet**.
  - b. If you have defined multiple Ethernet domains, a dialog appears allowing you to select the Ethernet domain in which you want to create this service. Use the pulldown menu to select the desired domain and click **OK**.



- c. Enter the service attributes and click on the plus sign to start adding interfaces.



- d. Add the **NEWYORK** UNI on "1:1:13:GIGE:10" and the **MIAMI** UNI on "1:1:5:GIGE:10".

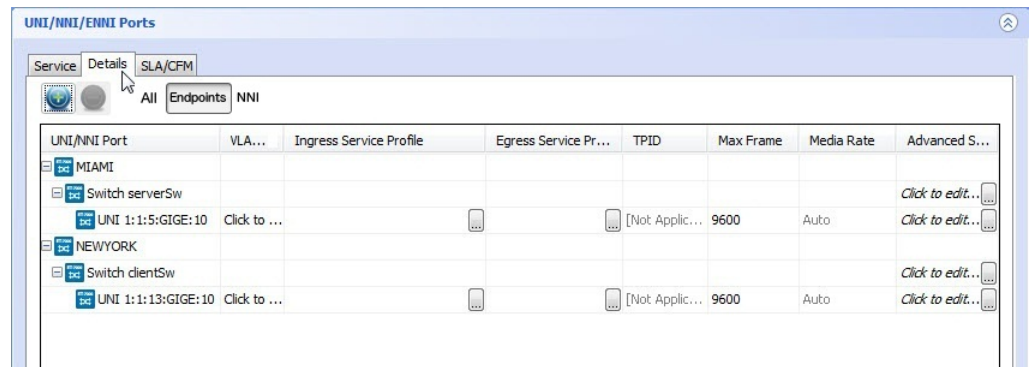


**NOTE:** The switches and ports only appear in the Add UNI menu if they have been properly configured on the NE. See the *BT17000 Series packetVX Solutions Guide* for information on how to add and configure a switch.



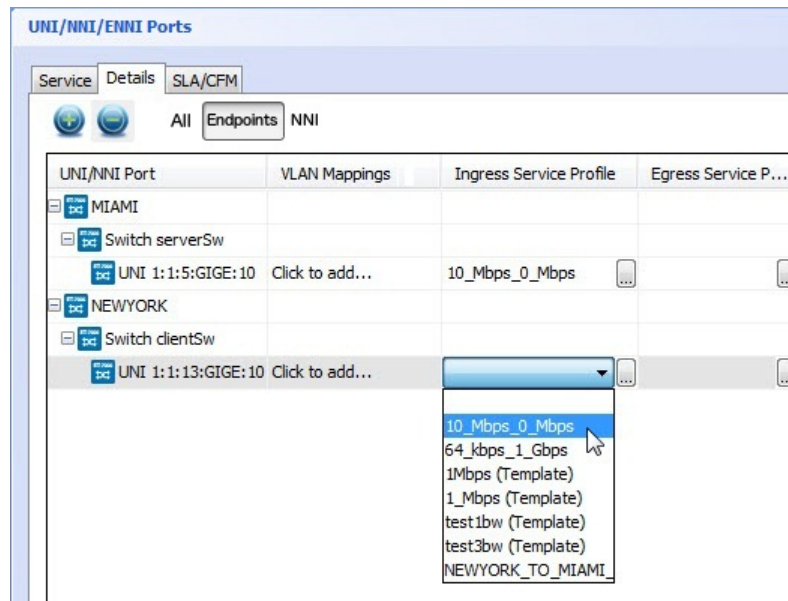
**NOTE:** The NNIs do not need to be explicitly added if the network elements are running GVRP. When working with network elements that do not support GVRP such as the BT1700 Series or BT1800 Series devices, you will need to add the appropriate NNIs to the service or use the Auto-Provision NNIs feature.

- e. Click the Details tab in the UNI/NNI Ports pane to enter more detailed information for each UNI.

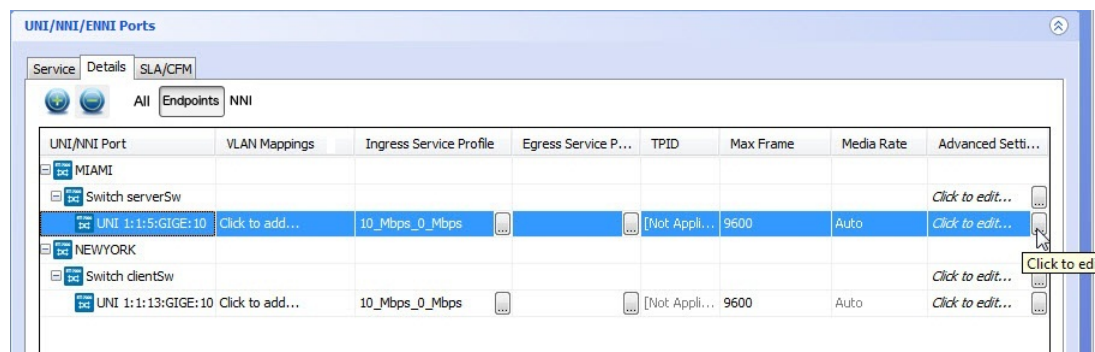


There is no need to specify any CVLAN mappings since the interfaces are untagged.

- f. Select the ingress service profile for both sites by clicking on the pulldown menu or the ellipsis.



g. Open the Advanced Settings menu for the **MIAMI** UNI by clicking on the ellipsis.



h. Select the service map from the pulldown menu and click **OK**.

**Advanced Settings**

Service

Service Map Profile: **TO\_NEWYORK\_VOICE (Template)** ...

Service Map Sequence: **50**

Layer 2

Service Type: **Virtual Multiple** C-PVID: ☐ [Disabled]

Layer 1

Wavelength: **850.00 nm**

Circuit ID:

Description:

OK Cancel

The Service Type is not applicable. Ensure the C-PVID is unchecked. The Service Map sequence is also not applicable.

- i. Open the Advanced Settings menu for the **MIAMI** switch by clicking on the ellipsis.

**UNI/NNI/ENNI Ports**

Service Details SLA/CFM

All Endpoints NNI

UNI/NNI Port	VLAN Mappings	Ingress Service Profile	Egress Service P...	TPID	Max Frame	Media Rate	Advanced Setti...
MIAMI							
Switch serverSw							Click to edit...
UNI 1:1:5:GIGE:10	Click to add...	10_Mbps_0_Mbps		[Not Appli...	9600	Auto	Click to edit...
NEWYORK							
Switch clientSw							Click to edit...
UNI 1:1:13:GIGE:10	Click to add...	10_Mbps_0_Mbps		[Not Appli...	9600	Auto	Click to edit...

- j. Ensure CVLAN Translation is unchecked and click **OK**.

**Advanced Settings**

Service Settings

CVLAN Translation: ☐

SLA Measurement Profile:  ...

OK Cancel

- k. Repeat substeps **f** through **i** for the **NEWYORK** UNI but select the **TO\_MIAMI\_VOICE** service map.

The image shows a screenshot of the 'Advanced Settings' dialog box in the proNX Service Manager. The dialog is titled 'Advanced Settings' and has a close button in the top right corner. It is divided into three main sections: 'Service', 'Layer 2', and 'Layer 1'. In the 'Service' section, 'Service Map Profile' is set to 'TO\_MIAMI\_VOICE (Template)' and 'Service Map Sequence' is '50'. In the 'Layer 2' section, 'Service Type' is 'Virtual Multiple' and 'C-PVID' is 'Disabled'. In the 'Layer 1' section, 'Wavelength' is '850.00 nm', and there are empty text boxes for 'Circuit ID' and 'Description'. At the bottom right, there are 'OK' and 'Cancel' buttons.

I. Click **Activate**.

It is good practice to check whether the activate completes successfully. Open the Tasks panel to check that the task has finished.

For information about error messages, see [“Service Activation Error Messages” on page 549](#)

2. Repeat for the **NEWYORK** to **DALLAS** EVPLINE service, with the following differences:

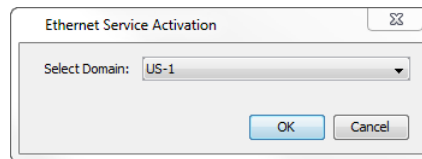
- Service Name - **NEWYORK\_DALLAS\_1051**
- SVLAN - **1051**
- UNI ports - **NEWYORK** UNI on "1:1:13:GIGE:10" and **DALLAS** UNI on "1:1:5:GIGE:10"
- Service Map - **TO\_DALLAS\_VOICE** service map at the **NEWYORK** UNI and **TO\_NEWYORK\_VOICE** service map at the **DALLAS** UNI.

3. Repeat for the **DALLAS** to **MIAMI** EVPLINE service, with the following differences:

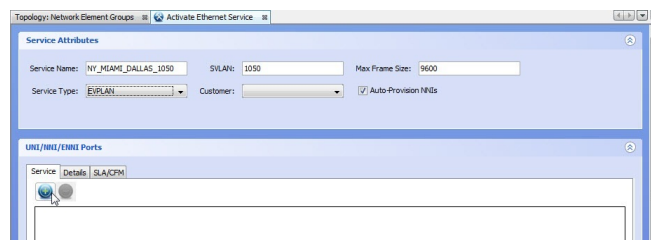
- Service Name - **DALLAS\_MIAMI\_1053**
- SVLAN - **1053**
- UNI ports - **DALLAS** UNI on "1:1:5:GIGE:10" and **MIAMI** UNI on "1:1:5:GIGE:10"
- Service Map - **TO\_DALLAS\_VOICE** service map at the **MIAMI** UNI and **TO\_MIAMI\_VOICE** service map at the **DALLAS** UNI.

## Setting Up the EVPLAN Service

1. On the PSM Client, click the **Service Activation** button on the toolbar and choose **Ethernet**.
2. If you have defined multiple Ethernet domains, a dialog appears allowing you to select the Ethernet domain in which you want to create this service. Use the pulldown menu to select the desired domain and click **OK**.



3. Enter the service attributes and click on the plus sign to start adding interfaces.



4. Add the **NEWYORK** UNI on "1:1:13:GIGE:10", the **MIAMI** UNI on "1:1:5:GIGE:10", and the **DALLAS** UNI on "1:1:5:GIGE:10".

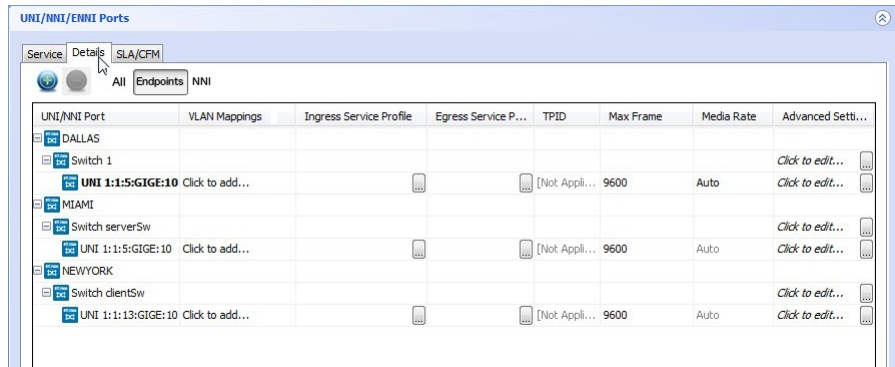


**NOTE:** The switches and ports only appear in the Add UNI menu if they have been properly configured on the NE. See the *BT17000 Series packetVX Solutions Guide* for information on how to add and configure a switch.

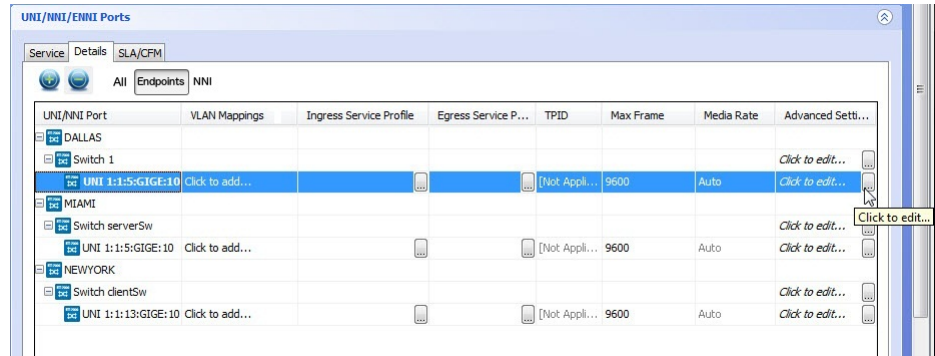


**NOTE:** The NNIs do not need to be explicitly added if the network elements are running GVRP. When working with network elements that do not support GVRP such as the BT1700 Series or BT1800 Series devices, you will need to add the appropriate NNIs to the service or use the Auto-Provision NNIs feature.

5. Click the Details tab in the UNI/NNI Ports pane to enter more detailed information for each UNI.



6. Configure the Advanced settings for each UNI.
  - a. Open the Advanced Settings menu for the each UNI by clicking on the ellipsis.



- b. Set the C-PVID to an arbitrary value and click **OK**. For simplicity, set the C-PVID to the same value for all three UNIs.



**Advanced Settings**

Service

Service Map Profile:  ...

Service Map Sequence: 50

Layer 2

Service Type: Virtual Multiple C-PVID: ☒ 2001

Control Frame Profile: DEFAULT\_UNI\_PROFILE

MSTP Enabled: ☒ CCM Enabled: ☒

SVLAN Translation: ☐

Layer 1

Circuit ID:

Description:

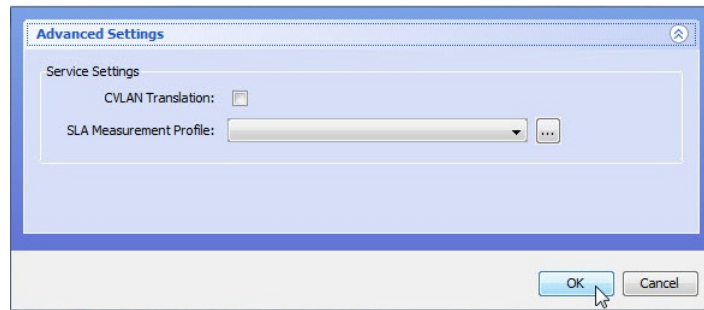
OK Cancel

By setting the C-PVID value, all untagged traffic arriving at the UNI will be treated as if it contained a CVLAN ID equal to the C-PVID value. This value can then be used in the CVLAN mapping table. The Service Type is not applicable. The Service Map sequence is also not applicable.

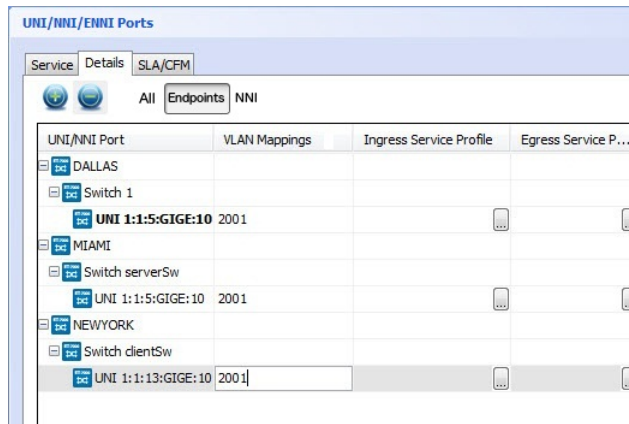
7. Configure the Advanced Settings attributes for each switch.
  - a. Open the Advanced Settings menu for each switch by clicking on the ellipsis.

UNI/NNI Port	VLAN Mappings	Ingress Service Profile	Egress Service P...	TPID	Max Frame	Media Rate	Advanced Setti...
DALLAS							
Switch 1							Click to edit...
UNI 1:1:5:GIGE:10	Click to add...			[Not Appli...]	9600	Auto	Click to edit...
MIAMI							
Switch serverSw							Click to edit...
UNI 1:1:5:GIGE:10	Click to add...			[Not Appli...]	9600	Auto	Click to edit...
NEWYORK							
Switch clientSw							Click to edit...
UNI 1:1:13:GIGE:10	Click to add...			[Not Appli...]	9600	Auto	Click to edit...

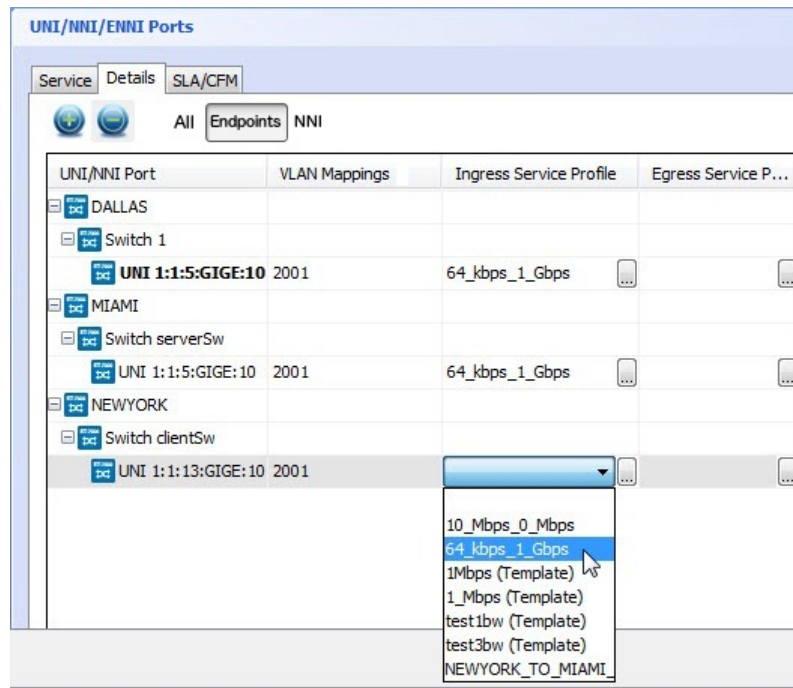
- b. Ensure CVLAN Translation is unchecked and click **OK**.



8. Set the CVLAN mapping for each UNI, using the C-PVID value configured earlier.



9. Select the ingress service profile by clicking on the pulldown menu or the ellipsis.



10. Click **Activate**.

It is good practice to check whether the activate completes successfully. Open the Tasks panel to check that the task has finished.

For information about error messages, see [“Service Activation Error Messages” on page 549](#)

## Modifying a Service

PSM allows users to modify existing Ethernet Services in the network by editing, adding and removing ports.

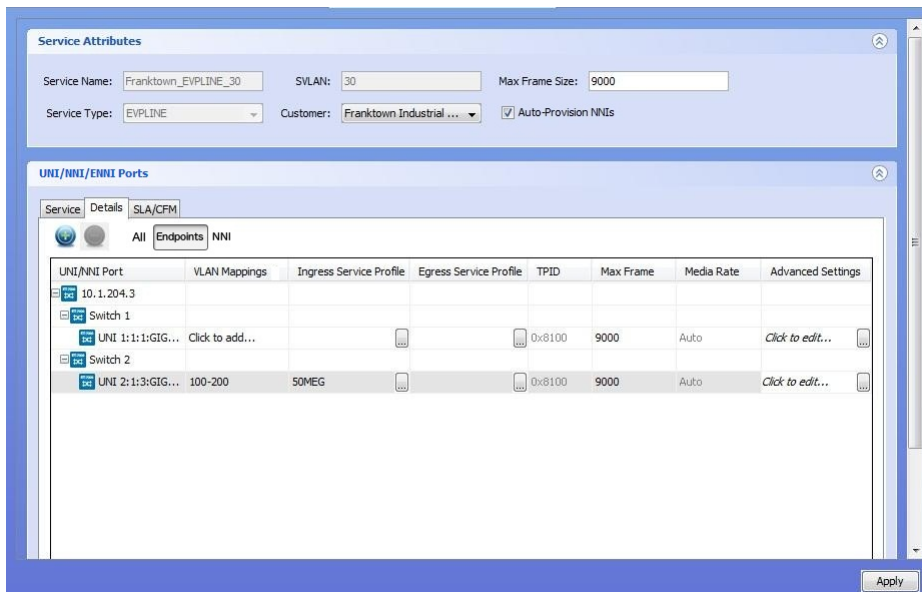
- [Modifying a Port in a Service on page 399](#)
- [Adding a Port to a Service on page 400](#)
- [Removing a Port from a Service on page 401](#)

### Modifying a Port in a Service



**CAUTION:** Modifying a port in a service might affect the service or the data traffic running on the service.


1. Double-click a service in the Network tree.  
The **Ethernet Service Activation** window for that service appears.
2. Select the **Details** tab to display the port settings.
3. Click the port you want to modify, and then click the ellipsis in the Advanced settings column. The text in the editable fields is black; fields that cannot be changed are grey.

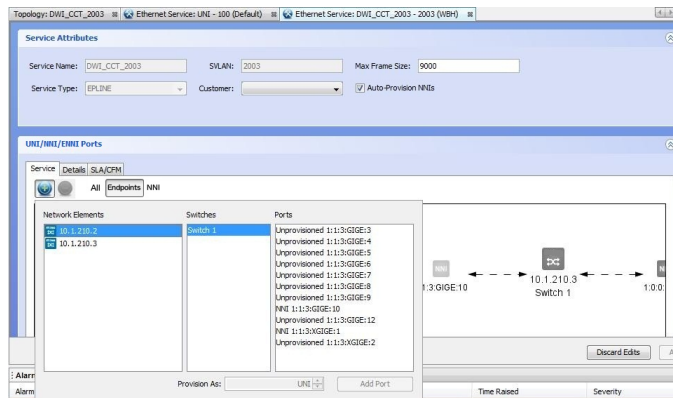


**NOTE:** For multi-chassis LAGs, you can only modify the active LAG member. PSM automatically copies the modifications to the non-active LAG members.

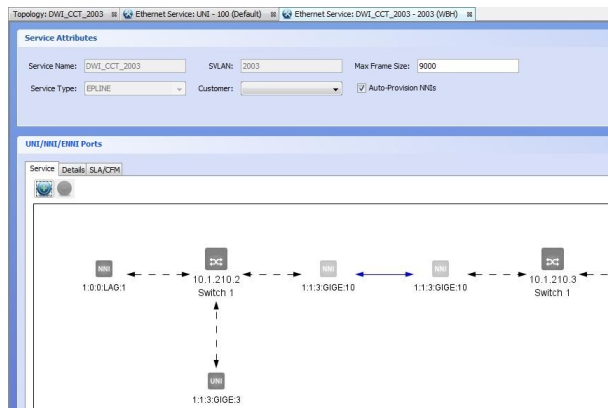
4. To implement the port modifications, click **Apply**. The port is changed.

## Adding a Port to a Service

1. Double-click a service in the Network tree.  
The **Ethernet Service Activation** window for that service appears.
2. In the Service tab of the UNI/NNI/ENNI Ports panel, click the  icon.
3. Select the network element where the port is to be added, then select a switch from the Switch Members list. This populates the ports panel with a list of ports that can be added to the selected service, as shown below.



4. Select the port or group of ports to be added to the service.
5. Click **Add UNI** or **Add UNI LAG**, **Add NNI** or **Add NNI LAG**, or **Add ENNI** or **Add ENNI LAG** depending on the type of port chosen.
6. Click **Apply**. The port or group of ports is added as shown below.



## Removing a Port from a Service



**CAUTION:** Removing a port from a service might affect the service or the data traffic running on the service.

1. Double-click a service in the Network tree.  
The **Ethernet Service Activation** window for that service appears.
2. In the **UNI/NNI/ENNI Ports** section, remove a port using one of the following options:
  - a. In the **Details** tab, select the port from the list and click the subtract button to remove the port, or right-click the port and click **Remove Port(s)**.

- b. In the **Service** tab, select the port icon and click the subtract button to remove the port.



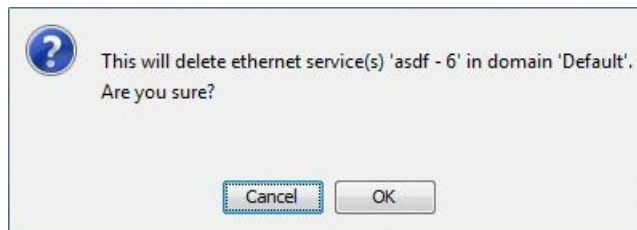
**NOTE:** When you remove one member of a multi-chassis LAG from a service, PSM automatically removes all other members of that multi-chassis LAG from the service.

3. To implement the port removal, click **Apply**. The port is removed.

---

## Deleting a Service

1. To delete a service, right-click on the service in the tree view and choose **Delete**.  
An information window opens asking for confirmation.



2. Click **OK**.

The service is deleted from the network elements and the proNX Service Manager server.

The NE data stored in the proNX Service Manager server is automatically updated after the deletion completes when it re-discovers the affected nodes.

---

## Adding SLA/CFM to a Service

Use this procedure to add SLA/CFM to UNI ports in an Ethernet service.

### CFM provisioning

In an Ethernet network consisting only of BT17000 Series network elements, Y.1731 setup is performed automatically by the NEs. You do not need to use PSM to configure CFM.

In a mixed Ethernet network consisting of BT17000 Series, BT1700 Series, and/or BT1800 Series network elements, or in an Ethernet network consisting of non-Juniper Networks network elements, Y.1731 setup is partially performed by the NEs. You can use PSM to complete the CFM provisioning.

In all cases, you cannot use PSM to change the settings for the Local MEG and MEP, but you can use PSM to manually add and/or remove remote MEPs. Manually adding and/or removing remote MEPs is required when interworking with non-Juniper Networks network

elements. Where applicable, PSM automatically sets the MEG name, MEG level, and MEP IDs for each MEP provisioned on a UNI.

There is a single MEP per switch in the BTI7000 Series and BTI700 Series equipment, and a single MEP per port in the BTI800 Series equipment. The single MEP per switch limits you to having only one UNI on the switch belonging to an SLA pair. See [Table 47 on page 403](#).



**NOTE:** There is a limit to the number of MEPs and MIPs supported on a BTI810 network element. See the *BTI800 Series Technical Product Guide* for details. A single MIP counts as 2 towards that limit.

When a UNI is removed from a service, the corresponding MEP is automatically removed. When an NNI is removed from a service, the corresponding MIP is removed. When a service is deleted, the MEG is automatically removed.

#### SLA provisioning

SLA provisioning is performed by specifying SLA Initiator/Responder pairs in the SLA/CFM tab in the Ethernet Service Activation screen. [Table 47 on page 403](#) shows the constraints when configuring SLAs on different endpoints.

**Table 47: SLA Provisioning Constraints**

NE Type	Notes
BTI7000 Series	<p>A UNI port can be configured as either an initiator or a responder.</p> <p>A UNI port can be the initiator for up to 4 responder ports.</p> <p>Only one UNI port per switch can be configured on an SLA pair.</p> <p>A UNI port that is an initiator cannot be a responder for the same remote port, but it can be a responder for another remote port.</p>
BTI700 Series excluding the BTI718E	<p>A UNI port can only be configured as a responder, not an initiator.</p> <p>Only one UNI port per switch can be configured on an SLA pair.</p>
BTI718E	<p>A UNI port can be configured as either an initiator or a responder.</p> <p>A UNI port can be the initiator for multiple responders.</p> <p>Only one UNI port per switch can be configured on an SLA pair.</p> <p>A UNI port that is an initiator cannot be a responder for the same remote port, but it can be a responder for another remote port.</p>

Table 47: SLA Provisioning Constraints (continued)

NE Type	Notes
BTI800 Series	<p>A UNI port can be configured as either an initiator or a responder.</p> <p>A UNI port can be the initiator for only one responder port.</p> <p>Multiple UNI ports per switch can be configured for SLA pairs.</p> <p>A UNI port that is an initiator can only be a responder for the same remote port. It cannot be a responder for another remote port.</p> <p>For the BTI805, BTI821, and BTI822, when you add one SLA pair, a second SLA pair is automatically added in the opposite direction between the same two endpoints.</p> <p><b>NOTE:</b> If you plan to use the link trace and loopback capabilities on a BTI810, you should enable automatic MIP creation. For information on how to do this, see the <i>proNX Service Manager Installation and Administration Guide</i>. By default, automatic MIP creation is disabled for the BTI810.</p>

PSM reports an error in the SLA/CFM dialog for the following reasons:

- Only one end of the SLA pair has been provisioned (one initiator or one responder).
- Mismatched MEPs (a MEP ID that does not exist has been paired with a MEP ID on the service).



**NOTE:** The SLA Measurement Profile is provisionable in the Advanced Settings of each Switch in the Details tab of the activation view. You can select either an existing profile or a template, and you are able to view the profile's contents.



1. Open the Service Attributes window for an Ethernet service, and then click the **SLA/CFM** tab.

The screenshot shows the 'UNL/NE Ports' configuration window with the 'SLA/CFM' tab selected. The 'SLA Details' section is currently empty. The 'CFM Details' section contains a table with the following data:

MEP A NE	MEP A Port (MEP ID)	MEP A Level	MEP A Remote State	MEP Z NE	MEP Z Port (MEP ID)	MEP Z Level	MEP Z Rem...	Crosscheck
Miami	UNE 1:1:5:GIGE:10 (4112)	4	Ok	NewYork	UNE 1:1:1:GIGE:10 (	4	Ok	min

Below the table, there is an 'Auto-Configure CFM' button and a 'MEG Name' input field. At the bottom right, there is an 'Add Remote MEP' button.

PSM automatically populates the CFM Details table with the MEPs on the BT17000 Series NEs.

2. Optionally, set the **MEG Name**.

The MEG Name can be up to 6 characters long. By default, it is the SVLAN ID prefixed by one or more "v"s (padded up to 6 characters).

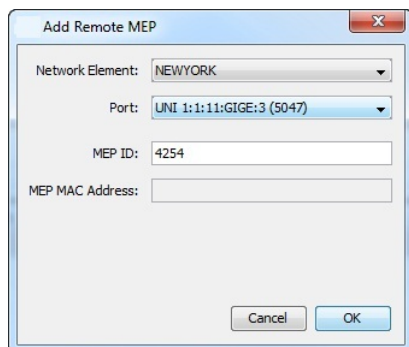
3. Click **Auto-Configure CFM** to add MEPs on BT1700 Series and BT1800 Series devices. PSM responds with a dialog box detailing the MEPs that it has added. Click **OK** to close the dialog box.

Clicking **Auto-Configure CFM** configures CFM for BT1700 Series and BT1800 Series devices. Once clicked, the system goes through the service and automatically adds MEPs, Remote MEPs, and MIPs to the service. If the **Activate** or **Apply** button is then clicked, the MEPs/MIPs are provisioned on the devices.

If the service includes BT17000 Series UNIs, then this step also adds Remote MEPs to and from the BT17000 Series UNIs so that CFM is properly configured on all equipment. If a service is modified, then clicking the **Auto-Configure CFM** button adds the proper CFM to whatever has been modified.

When the configuration is complete, a list of the entities added is displayed in the CFM Details table.

4. To manually add Remote MEPs to the CFM Details table, click **Add Remote MEP** and specify the remote **MEP ID**.



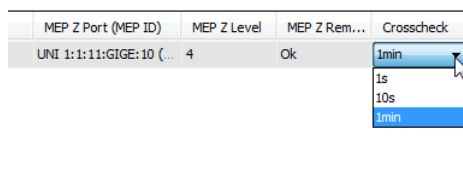
The 'Add Remote MEP' dialog box contains the following fields:

- Network Element: NEWYORK (dropdown)
- Port: UNI 1:1:11:GIGE:3 (5047) (dropdown)
- MEP ID: 4254 (text input)
- MEP MAC Address: (empty text input)
- Buttons: Cancel, OK

Use the pop-up dialog box to configure the remote MEP. MEPs on BTI700 Series and BTI800 Series devices require that the MAC address of the device be entered manually. Once you are finished configuring the remote MEP, click **OK**.

The Remote MEP is added to the CFM Details table. Repeat this step to add further MEPs.

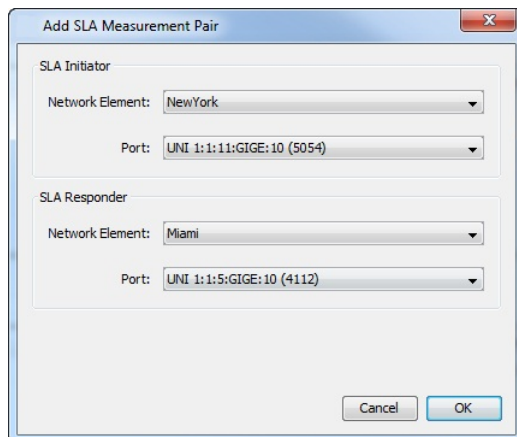
- To change the CCM interval, select the new interval in the Crosscheck dropdown menu.



MEP Z Port (MEP ID)	MEP Z Level	MEP Z Rem...	Crosscheck
UNI 1:1:11:GIGE:10 (...)	4	Ok	1min

The Crosscheck dropdown menu is open, showing options: 1min, 1s, 10s, 1min.

- To add SLA pairs to the service, click **Add SLA Pair** and specify the initiator and responder.



The 'Add SLA Measurement Pair' dialog box contains the following fields:

- SLA Initiator**
  - Network Element: NewYork (dropdown)
  - Port: UNI 1:1:11:GIGE:10 (5054) (dropdown)
- SLA Responder**
  - Network Element: Miami (dropdown)
  - Port: UNI 1:1:5:GIGE:10 (4112) (dropdown)
- Buttons: Cancel, OK

Use the pop-up dialog box to configure the SLA pair.

Once you are finished configuring the SLA pair, click **OK**. The SLA pair is added to the SLA Details table. Repeat this step to add further SLA pairs.

UNI/NNI Ports

Service Details SLA/CFM

Initiator NE	Initiator Port (MEP ID)	State	SVLAN Priority	Responder NE	Responder Port (MEP ID)
NewYork	UNI 1:1:11:GIGE:10 (5054)	Enabled	0	Miami	UNI 1:1:5:GIGE:10 (4112)

Delete SLA Pair Add SLA Pair

CFM Details

MEP A NE	MEP A Port (MEP ID)	MEP A Level	MEP A Remote State	MEP Z NE	MEP Z Port (MEP ID)	MEP Z Level	MEP Z Remote State	Crosscheck
Miami	UNI 1:1:5:GIGE:10 (4112)	4	Ok	NewYork	UNI 1:1:11:GIGE:10 ...	4	Ok	Imin

Auto-Configure CFM Add Remote MEP

7. To change the SVLAN priority of the SLA pair, select the new priority from the SVLAN Priority dropdown menu.

SVLAN Priority	Responder NE
0	Miami

0  
1  
2  
3  
4  
5  
6  
7

8. To enable or disable the SLA pair, select the new state from the State dropdown menu.

State	SVLAN Priority
Enabled	0

Enabled  
Disabled

9. When you are done adding SLAs/CFMs to the service, click **Activate** to activate a new service or **Apply** to apply changes to an existing service.



**NOTE:** When you perform a CFM update on a pre-1.5 release BT1700 Series device, you must manually rediscover the device in order for the update to be reflected in PSM.

This procedure is complete.

## Running a Y.1731 Link Trace

Use this procedure to run a Y.1731 link trace from one UNI to another UNI.

### Prerequisites:

- MEPs and MIPs have been configured for the service.

A Y.1731 link trace request at the local MEP causes a Link Trace Message (LTM) to be sent to the remote MEP. All MIPs between the local and remote MEPs respond to the LTM with a Link Trace Reply (LTR). PSM uses information from the LTRs to display the path between the two endpoints.

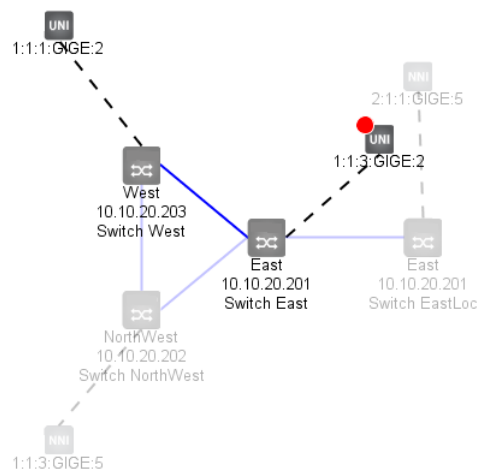
- In the Network tree view, click on the Ethernet service where you want to run the link trace.

The Ethernet service appears in the **Topology** window.

- Right-click the UNI port that you want to be the initiator, select **CFM Tests > Linktrace to**, and pick the responder port from the drop down list. If you want the responder port to be shown with its IP address in this list, see [“Setting Device Display Options” on page 274](#).

The initiator UNI port must be on a BT17000 Series, a BT1800 Series, or a BT1718E device. The responder UNI port can be a port on any compliant device.

After the link trace is finished, the path between the two UNIs is highlighted.



**NOTE:** The link trace might take some time to complete. You can watch its progress in the View > Server > Tasks window.

3. To clear the highlighting of the path, right-click the background in the **Topology** window and select **Clear Highlighting**.

## Running a Y.1731 Loopback

Use this procedure to run a Y.1731 loopback from one UNI to another UNI.

### Prerequisites:

- MEPs and MIPs have been configured for the service.

A Y.1731 loopback request at the local MEP causes a Loopback Message (LBM) to be sent to the remote MEP. The remote MEP responds to the LBM with a Loopback Reply (LBR). Unlike link trace messages, only the target MEP responds to the LBM.

1. In the Network tree view, click on the Ethernet service where you want to perform the loopback.

The Ethernet service appears in the **Topology** window.

2. Right-click the UNI port that you want to be the initiator, select **CFM Tests > Loopback to**, and pick the responder port and then the number of LBMs to send. If you want the responder port to be shown with its IP address in this list, see [“Setting Device Display Options” on page 274](#).

The initiator UNI port must be on a BTI7000 Series, a BTI800 Series, or a BTI718E device. The responder UNI port can be a port on any compliant device.

When a loopback is initiated on a BTI7000 Series or a BTI800 Series network element, a window appears showing the ongoing results of the loopback. When a loopback is initiated on a BTI718E device, the window only appears after the loopback test has completed. In all cases, the window stays open for a period of time after the test has finished.

MEP - Number of LBMs Tx   Remote MEP - Number of LBRs Rx	
5443 - 0	4851 - 0
5443 - 4	4851 - 4
5443 - 5	4851 - 5
5443 - 6	4851 - 6
5443 - 7	4851 - 8
5443 - 9	4851 - 9

The window shows the number of LBMs transmitted by the initiator and the number of LBRs received from the responder. For the BTI7000 Series network elements, the counts are reset to 0 each time a loopback test is run. For the BTI800 Series and BTI718E devices, the counts are not reset, and represent the loopback counts from the time the service was started.

## Running an RFC 2544 Benchmarking Test

Use this procedure to run an RFC 2544 benchmarking test on the BT1805, BT1821, or BT1822 devices.

The tests specified in RFC 2544 are useful to determine whether an Ethernet service complies with service level agreements. These tests apply to EPLINE and EVPLINE services only.

1. Right-click a service in the Network tree and select **RFC 2544 >Run Tests**.

The **Rfc 2544** dialog appears.

The screenshot shows the 'Rfc 2544' dialog box with the 'General' tab selected. The 'Throughput', 'Frame Loss Ratio', and 'Latency' checkboxes are all checked. The 'Endpoint' is set to a dropdown menu. The 'Frame Size' fields are set to 64, 128, 256, 512, 1024, and 1518. The 'Cos Type' is set to 'EPU' and 'Cos Level' is empty. The 'Run' button is highlighted.

2. Select the test parameters as follows:

- **Throughput**— This is always selected. The other tests require the throughput test to be enabled. The throughput test measures the maximum rate that can be processed within the specified **Acceptable Loss** constraint.
- **Frame Loss Ratio**— Select to run the frame loss ratio test. This test measures the frame loss ratios for different ingress traffic rates.
- **Latency**— Select to run the Latency test.
- **Endpoint**— Select the endpoint of the circuit where the test is to be initiated.
- **Frame Size 1** through **Frame Size 6**— Select the six different frame sizes to use for the test(s).

- **Cos Type**— Select the class of service type from the pulldown menu. Select **EPU** (EVC per UNI) if you want to use the EVC class of service. Select **MANUAL** if you want to manually specify the class of service.
  - **Cos Level**— Select the class of service level if the **Cos Type** is set to **MANUAL**.
3. Select the **Details** tab to configure the detailed test settings.

The screenshot shows the 'Rfc 2544' configuration window with the 'Details' tab selected. The window is divided into three sections: THROUGHPUT, FRAME LOSS RATIO, and LATENCY. Each section has an 'Oper-Way' dropdown menu set to 'DUAL\_EN...', a 'Duration' field set to '5', and an 'S. Trial' field set to '1'. The THROUGHPUT section also has a 'Max. Rate' field set to '1000', a 'Max. Trial Times' field set to '5', and an 'Acceptable Loss' field set to '0'. The FRAME LOSS RATIO section has a 'Granularity' field set to '1'. The LATENCY section has a 'Background Traffic' checkbox that is unchecked. At the bottom of the window are 'Cancel' and 'Run' buttons.

4. Select the throughput test parameters as follows:
- **Oper-Way**— Select **DUAL\_ENDED** to generate test traffic from both ends, or **LOOPBACK** to loop back the test traffic at the remote end.
  - **Max. Trial Times**— Specify the maximum number of trials to run. The minimum value for this parameter is 5.
  - **Acceptable Loss**— Specify the percentage of frames that can be lost (and the outcome still considered to be acceptable). If this is set to 0, the throughput test measures the maximum rate that can be processed with no loss of frames.
  - **Max. Rate**— Specify the starting traffic rate (Mbps) for the test.
  - **Duration**— Specify the duration of the test in seconds.
  - **S. Trial**— Specify the number of successive trials that must be successful before the test at the current frame size is stopped. A trial is successful if the number of lost frames is within the **Acceptable Loss** constraint.
5. Select the frame loss ratio test parameters as follows:

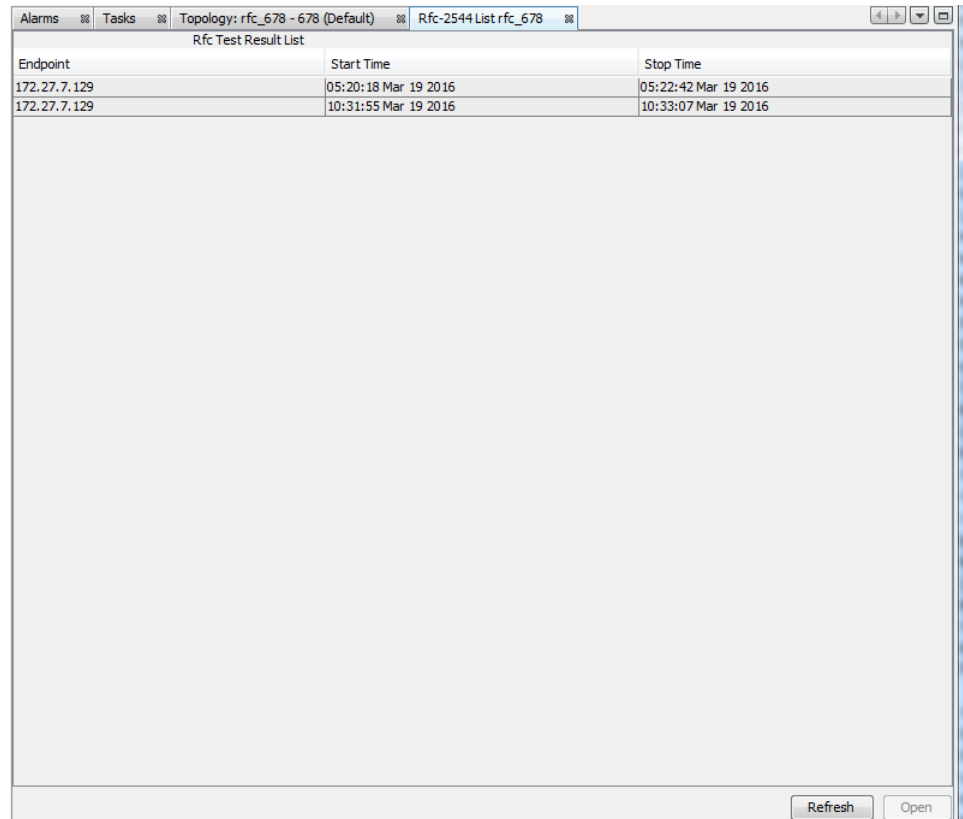
- **Oper-Way**— Select **DUAL\_ENDED** to generate test traffic from both ends, or **SINGLE\_ENDED** to generate test traffic from one end, or **LOOPBACK** to loop back the test traffic at the remote end.
  - **Granularity**— Specify the percentage of the maximum frame rate to step down for each successive trial. The maximum frame rate is the frame rate that achieves 100% link utilization for the frame size being used. The rate is stepped down from the maximum frame rate successively if frame loss occurs.
  - **Duration**— Specify the duration of the test in seconds.
  - **S. Trial**— Specify the number of successive trials that have no lost frames before the test at the current frame size is stopped.
6. Select the latency test parameters as follows:
    - **Oper-Way**— Select **DUAL\_ENDED** to generate test traffic from both ends, or **LOOPBACK** to loop back the test traffic at the remote end.
    - **Duration**— Specify the duration of the test in seconds.
  7. Select **Background Traffic** to enable background traffic in the latency tests.
  8. Click **Run**.

You can monitor the status of the test through the **View > Server > Tasks** window.
  9. View the test results when the test is finished.



- a. Right click the service in the Network tree and select **RFC 2544 >Show Results**.

This command retrieves the most recent, completed RFC 2544 tests from the NE and lists them in the **Rfc Test Result List**.



Endpoint	Start Time	Stop Time
172.27.7.129	05:20:18 Mar 19 2016	05:22:42 Mar 19 2016
172.27.7.129	10:31:55 Mar 19 2016	10:33:07 Mar 19 2016



**NOTE:** Once PSM retrieves the test results, it stores them in its local database and makes them available for display (even if the test results are subsequently deleted from the NE).

- b. Select the test you want to view and click **Open**.

A new tab opens showing the test that you have selected.

- c. Click the chevron in the upper right corner to view the test results.

The test results are organized as shown in the following figure:



d. To see the results of a specific test, click the associated chevron.

For example, these are the results of the throughput test:

Throughput Results					
Direction [ FE --> NE ]					
Frame Size	S. Trials	Traffic Load	Tx Count	Loss Count	Loss Ratio (%)
64	1	1000	7408468	0	0
128	1	1000	4181981	0	0
256	1	1000	2249747	0	0
512	1	1000	1170851	0	0
1024	1	1000	597641	0	0
1518	1	1000	405717	0	0
Direction [ NE --> FE ]					
Frame Size	S. Trials	Traffic Load	Tx Count	Loss Count	Loss Ratio (%)
64	1	1000	7396529	0	0
128	1	1000	4208895	0	0
256	1	1000	2256370	0	0
512	1	1000	1171562	0	0
1024	1	1000	597539	0	0
1518	1	1000	405729	0	0

10. To export the test data to an Excel file, click **Export** and save the file.

## Ethernet Ring Protection Switching (ERPS)

ERPS is a ring protection scheme for Ethernet networks, and is supported on BT17000 Series, BT1800 Series, and BT1700 Series equipment.

The network operator creates the ERPS service directly on the network element using either the proNX 900 or the CLI, and can use PSM to view the service graphically. PSM automatically discovers and displays ERPS services in the network but does not currently support creating ERPS services.


- [Visualizing an ERPS Service on page 414](#)
- [Viewing the ERPS Services Table on page 418](#)
- [Adding VLANs to an ERPS Ring on page 419](#)

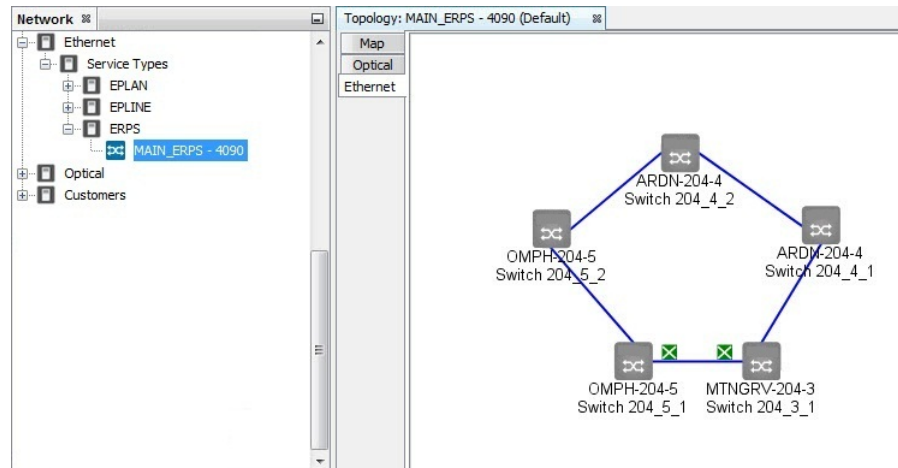
### Visualizing an ERPS Service

Use this procedure to view the ERPS service and its states.

Under normal (non-failure) conditions, the ERPS service blocks the RPL link to prevent looping of traffic for the Ethernet services it is protecting. On link failure, the ERPS service enables the blocked port to allow traffic from those Ethernet services to continue to flow.

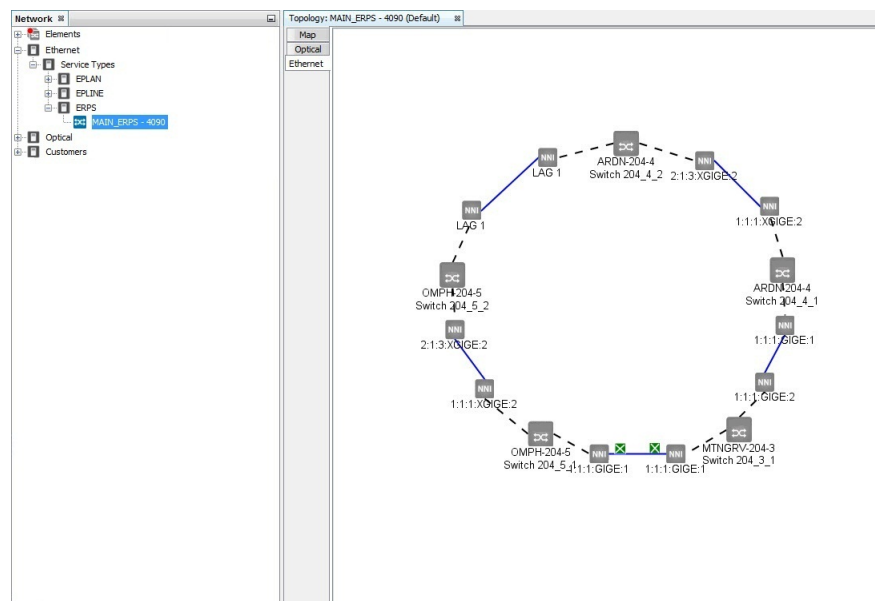
1. In the **Network** tree view, select the desired ERPS service.

The ERPS service view opens in the main map window. If PSM is configured to show the ERPS link icons ([“Setting Service Display Options” on page 275](#)), a green  is displayed to indicate the RPL link being blocked.



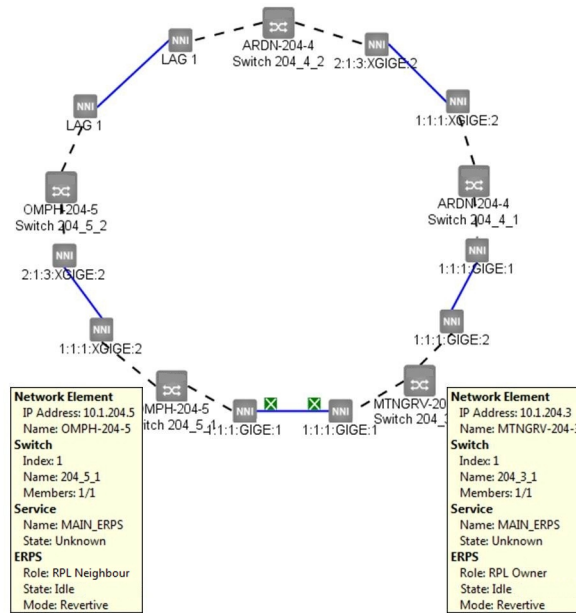
2. Right click the service view and select **Show Connected Ports**.

The ERPS service view is expanded to show the ports.



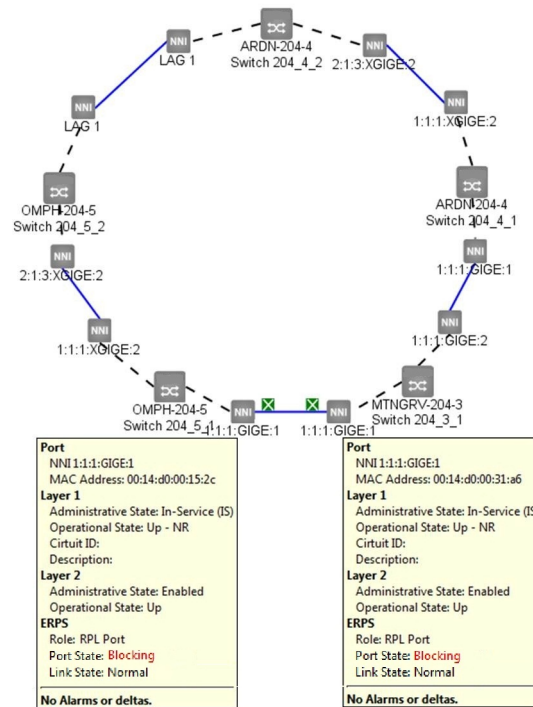
3. Hover over the network elements to see information on the ERPS service.

For the purposes of illustration, the mouse-over information for two network elements is shown simultaneously.





4. Hover over the NNI ports to see ERPS information for the NNI ports.

For the purposes of illustration, the mouse-over information for two NNI ports are shown simultaneously.

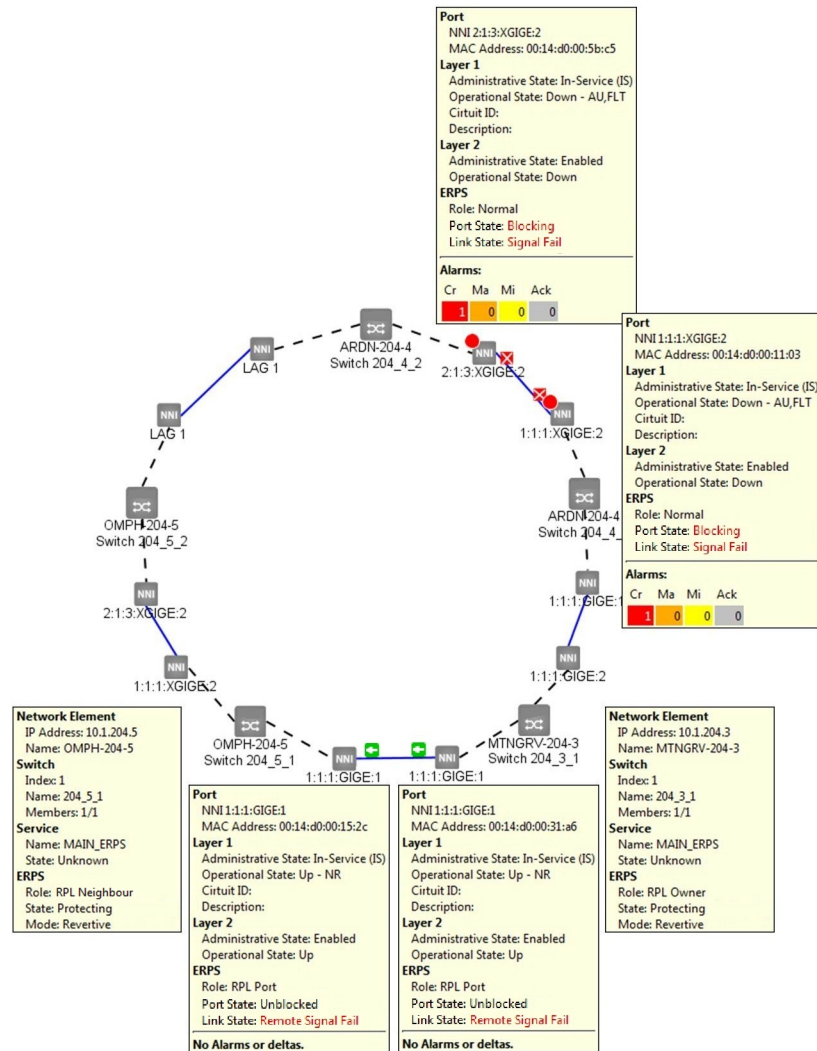


**NOTE:** The same ERPS state information can be viewed from the **Details** tab in the UNI/NNI Ports pane of the Ethernet Service Activation window. Simply double-click on an existing ERPS service in the Network tree view and select the **Details** tab.

### Effect Of Link Failure on ERPS States

If a link goes down, the RPL port becomes unblocked and the ERPS states change to show that it is in protecting mode. If PSM is configured to show the ERPS link icons ("Setting Service Display Options" on page 275), a red  is displayed to indicate the failed link, and a green  is displayed on the RPL link to show that it is passing traffic.

For the purposes of illustration, the mouse-over information for various elements and ports are shown simultaneously.



## Viewing the ERPS Services Table

Use this procedure to view the ERPS services table.

The ERPS services table displays information on all ERPS services running in the network.

### 1. Select **View > Ethernet > ERPS**.

The ERPS services table opens in the main Map window. The table shows the ERPS services in the network along with their port states and other information.

Network Element	Domain	Switch	Service Name	Port	Service State	Port Role
10.1.206.2	Default	2	ERPS_MainRing	NNI 2:1:13:3:GIGe:1	Disable	Normal
10.1.206.2	Default	2	ERPS_MainRing	NNI 2:1:13:3:GIGe:2	Disable	Normal
10.10.20.201	Default	1	ERPS_MainRing	NNI 1:1:3:GIGe:10		
10.10.20.201	Default	1	ERPS_MainRing	NNI 1:1:3:GIGe:9		
10.10.20.201	Default	1	ERPS_MainRing	NNI 1:1:3:GIGe:1		
10.10.20.201	Default	1	ERPS_MainRing	NNI 1:1:3:GIGe:2		
10.10.20.201	Default	2	ERPS_MainRing	NNI 2:1:1:GIGe:10		
10.10.20.202	Default	1	ERPS_MainRing	NNI 1:1:3:GIGe:1		
10.10.20.202	Default	1	ERPS_MainRing	NNI 1:1:3:GIGe:1		
10.10.20.202	Default	1	ERPS_MainRing	NNI 1:1:3:GIGe:2		
10.10.20.203	Default	1	ERPS_MainRing	NNI 1:1:1:GIGe:1		
10.10.20.203	Default	1	ERPS_MainRing	NNI 1:1:1:GIGe:2		
10.1.206.3	Default	2	ERPS_MainRing	NNI 2:1:15:3:GIGe:3	Disable	Normal
10.1.206.3	Default	4	ERPS_MainRing	NNI 4:1:7:3:GIGe:1	Disable	RPL Owner
10.1.206.4	Default	1	ERPS_MainRing	NNI LAG 1		
10.1.206.4	Default	1	ERPS_MainRing	NNI LAG 3		
10.10.20.201	Default	1	ERPS_SubRing	NNI 1:1:3:GIGe:10		

## Adding VLANs to an ERPS Ring

Use this procedure to add VLANs to a node in an ERPS ring.

PSM can be used to add VLAN IDs to a node in an ERPS ring. The typical use case for this procedure is to help with ERPS node insertion. Node insertion refers to breaking the NNI between two adjacent nodes in a ring, and reattaching the same NNI ports to a new node.

When a node is inserted into an ERPS ring, the list of VLANs must be configured on the new node, as follows:

- Associate the list of VLANs to the ERPS ring NNIs on the new node. This is not needed if GVRP is enabled on the ring.
- Add the list of VLANs to the ERPS protected VLAN list on the new node.
- Create the Ethernet services represented by these VLANs on the new node.

This procedure performs the above 3 tasks and runs an audit of the ERPS ring. The audit checks to make sure the existing configuration is consistent across all the nodes, and highlights any inconsistencies that it finds. Although the audit results are purely informational, and do not block the user from proceeding, you should examine the results for potential issues.

Additionally, PSM creates MIPs on the ERPS ring NNIs on the new node if MIPs have been configured on the ERPS ring NNIs on the existing nodes.

The following are the constraints for this procedure:

- This procedure should only be used on non-interconnect nodes. A non-interconnect node is a node that is not simultaneously part of a main ring and a sub-ring.
- This procedure should only be used when there is a single ERPS ring on the physical topology. Running this procedure in a configuration where there are multiple ERPS rings on the same physical ring is not supported.

- This procedure should only be run when a single node is inserted. When inserting multiple nodes in a ring, you should insert and repair one node at a time.



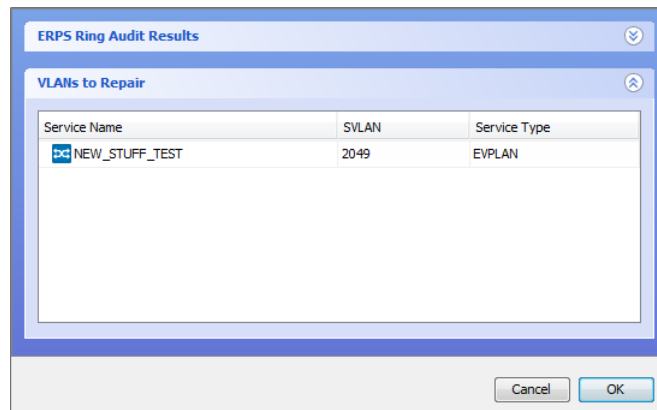
**NOTE:** This procedure supplements the ERPS node insertion procedures on the network elements. Refer to the ERPS node insertion procedures in the respective documentation for the different network elements for more details.

1. Select the desired ERPS service in the tree view.
2. In the Ethernet services topology window, identify the node that you want to add the VLANs to.

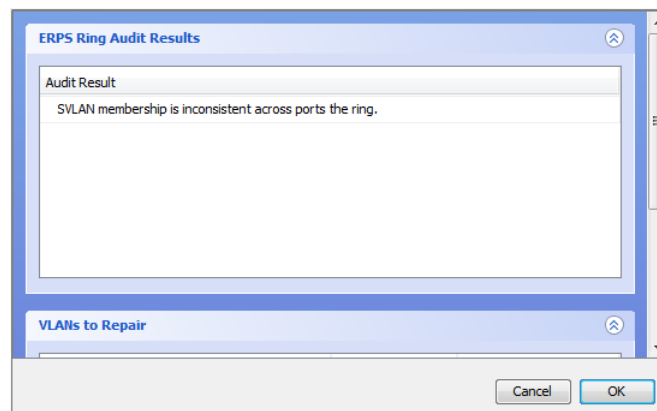
This is typically the newly inserted node.

3. Right click that node and select **Repair VLANs**.

PSM audits the ERPS service, treats the existing nodes as the baseline, and prepares to configure the selected node to be consistent with the baseline. The audit results and the list of VLANs to be added are presented. For example:



Here is an example of an audit that has uncovered underlying issues:







**TIP:** You can use this procedure purely to audit the ERPS ring.

4. Add the VLANs to the selected node.

If the audit shows that the ERPS ring is healthy, select **OK** to add the **VLANs to Repair** list to the selected node.

If the audit shows issues with the existing ERPS ring configuration, select **Cancel**, fix the issues, and repeat 3.



**NOTE:** You are advised, but not required, to fix the audit issues before selecting **OK** to add the VLANs.

Once you click **OK**, PSM associates the list of VLANs to the ERPS ring NNIs on the selected node, adds the list of VLANs to the protected VLAN list for the ERPS service on the selected node, creates the Ethernet services represented by these VLANs, and finally, creates the MIPs as necessary.

## Routing Considerations in Mixed Networks

Depending on the topology of the network, there are certain considerations to take into account when activating services. This section highlights the main concerns and steps required to successfully activate services within different network configurations.

- [GVRP - GARP VLAN Registration Protocol on page 421](#)
- [Mixed Networks - BT17000 Series with BT1700 Series or BT1800 Series Elements on page 422](#)

### GVRP - GARP VLAN Registration Protocol

The Generic Attributes Registration Protocol (GARP) is defined in 802.1D as a means for bridges to distribute information amongst themselves about membership in various *groups*. 802.1D defines GMRP (GARP Multicast Registration Protocol) to distribute multicast group membership. 802.1Q defines GVRP (GARP VLAN Registration Protocol) to distribute information about VLAN membership.

GVRP addresses the problem of determining which inter-bridge links (NNIs) must be members of which VLANs. In a VLAN-bridge, packets in VLAN x can only be transmitted on links that are members of VLAN x. VLAN x subscriber interfaces (UNIs) are manually configured, but it can be cumbersome to define a VLAN member for all VLANs across all NNIs. One fall-back would be to simply define all VLANs on NNIs, but this means that all flooded packets will be flooded everywhere, which is a large waste of bandwidth.

GVRP, in effect, advertises VLAN membership backwards through the network. If a node must receive packets in VLAN x, it sends a registration for VLAN x to all of its neighbors. Each of those neighbors adds the receiving link to VLAN x and then forwards a registration to all of its neighbors.

Using GVRP lets you dynamically route VLAN traffic through the network and create services without specifying the NNI ports needed for the service.

### Mixed Networks - BTI7000 Series with BTI700 Series or BTI800 Series Elements

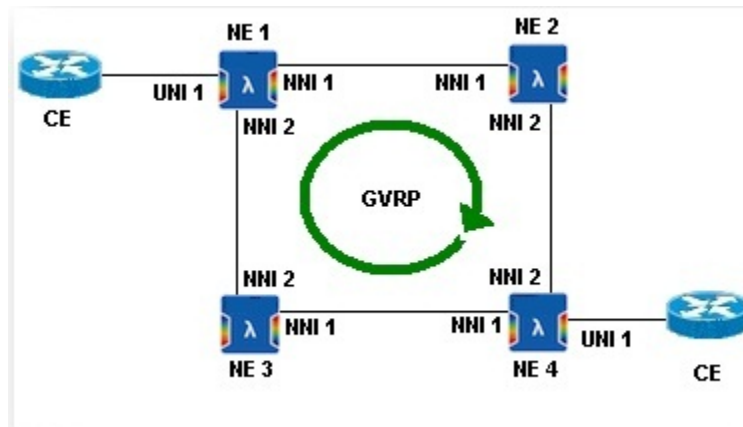
When a network includes BTI7000 Series packetVX and BTI700 Series or BTI800 Series devices, the topology of the network dictates the NNIs that must be explicitly added to successfully activate a service, regardless of the type of Ethernet service selected. The rule of thumb is that all NNIs on BTI700 Series devices must be added, and all NNIs on BTI7000 Series switches that are facing BTI700 Series devices must be added in order for traffic to flow. Some examples follow.



**NOTE:** This section only applies if the Auto-Provision NNIs feature is not selected.

### Creating Services in BTI7000 Series packetVX Only Networks

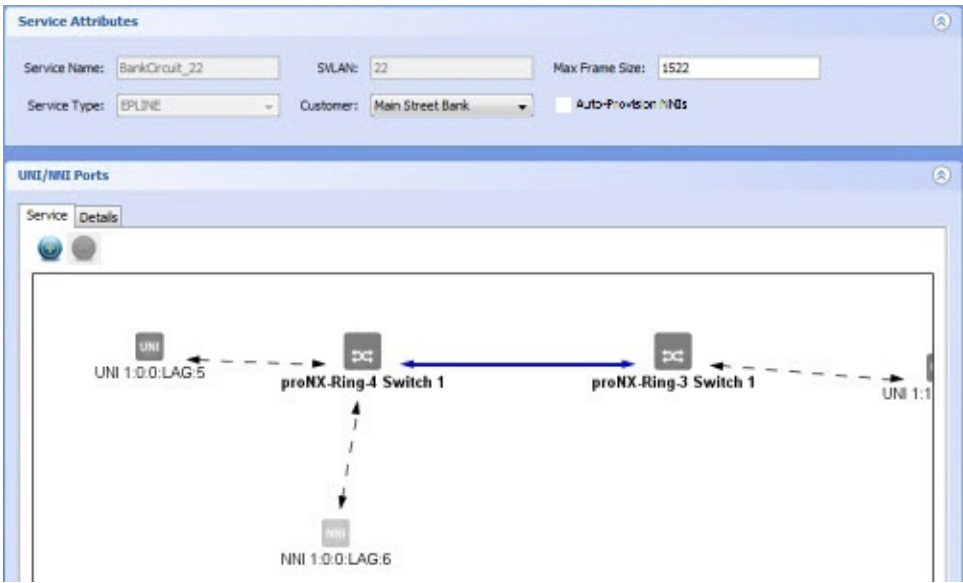
Figure 80: Creating Services in BTI7000 Series packetVX Only Networks



In this case, all network elements are BTI7000 Series packetVX nodes. Only the endpoint UNIs need to be added to the service, as the NNIs will all be GVRP-enabled and the dynamic VLAN creation will automatically route the traffic.

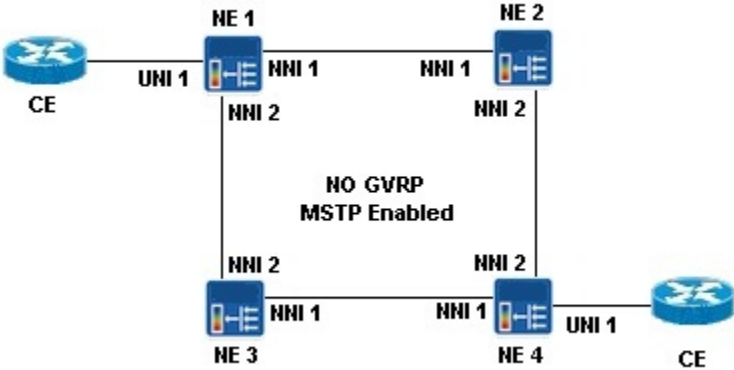
Equipment	Example IP	Example Port
NE 1	172.27.7.106	UNI 1: GIGE 12 on Switch 2
NE 4	172.27.7.110	UNI 1: GIGE 4 on Switch 1

Figure 81: Creating Services in BTI7000 Series packetVX-only Networks



Creating Services Over BTI700 Series And/or BTI800 Series Only Networks

Figure 82: Creating Services Over BTI700 Series And/or BTI800 Series Only Networks



In this case, all network elements are either BTI700 Series or BTI800 Series devices. If the **Auto-Provision NNIs** feature is disabled, you must explicitly add the NNIs that are part of the service. To avoid single points of failure, it is the user's responsibility to add all NNIs that can form possible paths.

Equipment	Example IP	Example Ports
NE 1	172.27.7.101	UNI 1: GIGE 3 on Switch 1 NNI 1: GIGE 15 on Switch 1 NNI 2: GIGE 16 on Switch 1

Equipment	Example IP	Example Ports
NE 2	172.27.7.104	NNI 1: GIGE 15 on Switch 1 NNI 2: GIGE 16 on Switch 1
NE 3	10.1.100.55	NNI 1: GIGE 15 on Switch 1 NNI 2: GIGE 16 on Switch 1
NE 4	10.1.100.56	UNI 1: GIGE 3 on Switch 1 NNI 1: GIGE 15 on Switch 1 NNI 2: GIGE 16 on Switch 1

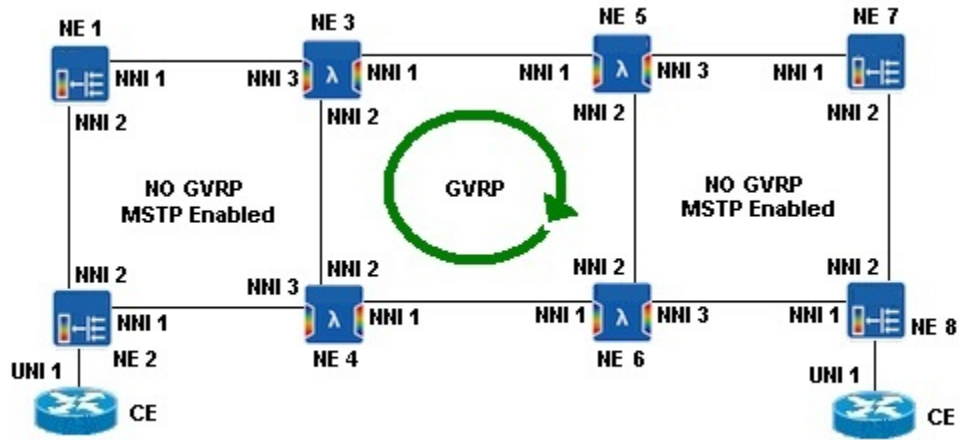
Figure 83: Creating Services Over BT1700 Series And/or BT1800 Series Only Networks

The screenshot displays the Service Manager configuration interface. The top section, 'Service Attributes', includes fields for Service Name (BOA2), SVLAN (12), Max Frame Size (9000), Service Type (EPLINE), and Customer (Syracuse branch). There is an unchecked checkbox for 'Auto-Provision NNIs'. The bottom section, 'UNI/NNI Ports', shows a diagram of the network topology. It features a central switch labeled 'East-712 Switch 1' connected to two NNI ports: 'NNI 1:1:1:GIGE:2' on the left and 'NNI 1:1:1:GIGE:1' on the right. The diagram also includes a 'Service' icon and a 'Details' tab.

#### Activating Services Over Combinations Of BT17000 Series packetVX and BT1700 Series or BT1800 Series Networks

This is a combination of the two previous cases. If the **Auto-Provision NNIs** feature is disabled, you must add all the NNIs that do not face the GVRP ring (see the table below).

Figure 84: Activating Services Over a Combination Of BTI7000 Series packetVX, BTI700 Series, and BTI800 Series Networks



In this example, NE 1 and NE 2 are BTI700 Series devices, NE 3 through NE 6 are BTI7000 Series packetVX devices, and NE 7 and NE 8 are BTI800 Series devices.

Equipment	Example IP	Example Ports
NE 1	172.27.7.101	NNI 1: GIGE 15 on Switch 1 NNI 2: GIGE 16 on Switch 1
NE 2	172.27.7.104	UNI 1: GIGE 3 on Switch 1 NNI 1: GIGE 15 on Switch 1 NNI 2: GIGE 16 on Switch 1
NE 3	172.27.7.105	NNI 3: GIGE 16 on Switch 1
NE 4	172.27.7.106	NNI 3: GIGE 16 on Switch 1
NE 5	10.1.100.54	NNI 3: GIGE 16 on Switch 1
NE 6	10.1.100.52	NNI 3: GIGE 16 on Switch 1
NE 7	10.1.100.55	NNI 1: GIGE 15 on Switch 1 NNI 2: GIGE 16 on Switch 1
NE 8	10.1.100.56	UNI 1: GIGE 3 on Switch 1 NNI 1: GIGE 15 on Switch 1 NNI 2: GIGE 16 on Switch 1

## Managing Profiles

---

- [About Profile Manager on page 426](#)
- [Managing Profile Templates on page 428](#)
- [Bandwidth Profile Templates on page 431](#)
- [Class Map Profile Templates on page 434](#)
- [Service Policy Profile Templates on page 436](#)
- [Service Map Profile Templates on page 438](#)
- [SLA Measurement Profile Templates on page 439](#)

### About Profile Manager

PSM allows users to create or clone profiles that can be used to configure Ethernet services.

The Profile Manager provides an easy way for you to create new profiles, as well as to manage the various profiles already associated with devices in the network. PSM automatically discovers existing profiles in the network, and makes them visible in the Profile Manager, organized by network element.

A profile can exist in the following forms:

- as a profile stored in PSM
- as a profile stored on the network element

A profile that is stored in PSM is called a profile template. You can use the Profile Manager to create profile templates:

- by specifying all parameters explicitly
- by cloning from another profile template
- by cloning from a profile associated with an actual device in the network

Profile templates are stored in PSM and are applied to the specified network elements during a service activation operation. Applying a profile template to a network element causes that profile to be created and stored on the network element using the same name as the template. After service activation, the profile exists both as a template in PSM and as an actual profile on the network element.

You can create, edit, or delete profile templates on PSM. You cannot use PSM to edit or delete profiles discovered on the network elements.



**NOTE:** There is no synchronization between the profile templates defined in PSM and the network. Changes to the templates are not reflected in the network, and changes in the network are not automatically copied back to the respective profile template. Changes in the network, however, are reflected in the discovered profiles for the respective network elements.

---

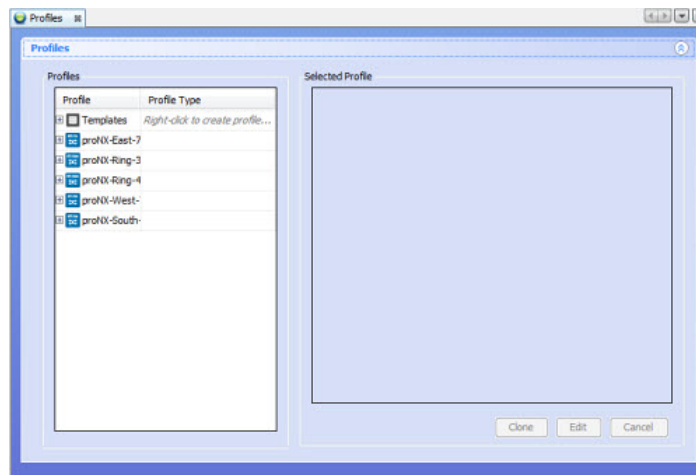


**NOTE:** Profile templates are part of the replicated data set when running with multiple servers. For more information on replicated data, see [“Running Multiple Servers with Server Replication” on page 30](#).

The Profile Manager screen is accessible via the Edit menu item Profiles, or via the toolbar button shown below.



The Profile Manager screen is shown below.



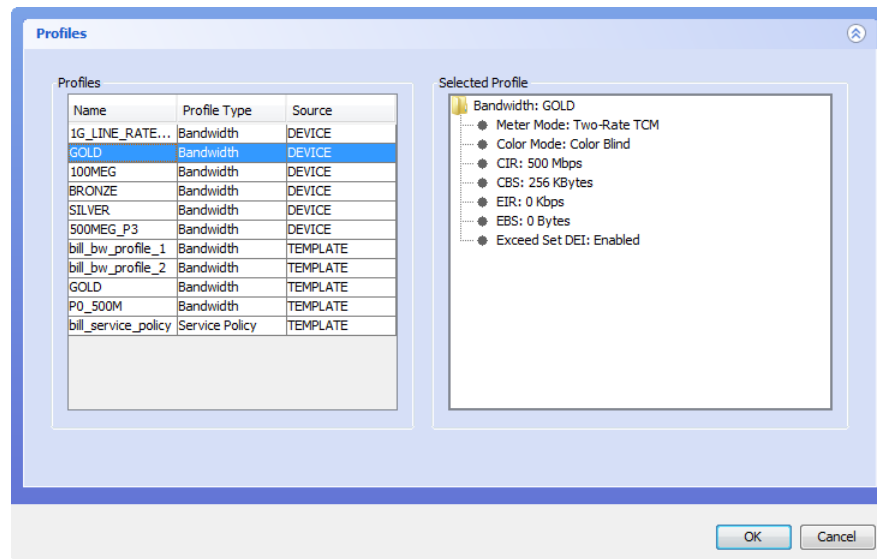
### Selecting a Profile During Service Activation

When you activate an Ethernet service, you have the ability to specify which profile to use on a port. The possible profiles include the list of profile templates in PSM, and the list of profiles discovered on the network element to which the port belongs. If you want to use a profile found on another network element, you must first clone that profile into PSM so that it appears in the list of profile templates.

Note that it is normal for a profile template in PSM and a profile on a device to have the same name. The reason is that when you activate a service and you specify a profile template, PSM creates a profile on the device with the same name as the template.

During service activation, when confronted with a choice between a profile template on PSM and the equivalent profile on the device, you should always select the profile on the device. If you select the profile template instead, you are in effect requesting PSM to create a new profile on the device with the same name as the profile template, which will result in an error because that profile already exists.

For example, in the following profile selection dialog (during service activation), the profile GOLD appears as both a profile template and a profile:



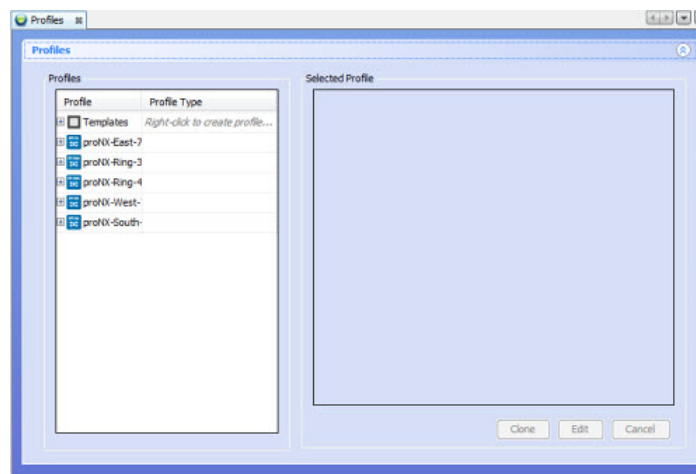
In such situations, you should always select the GOLD profile on the device (i.e. where the Source is DEVICE) rather than the GOLD profile template (i.e. where the Source is TEMPLATE). In fact, PSM will not allow you to select the GOLD profile template because doing so means that you are requesting PSM to create a new GOLD profile on the device, but the GOLD profile already exists on the device.

## Managing Profile Templates

### Creating a Profile Template

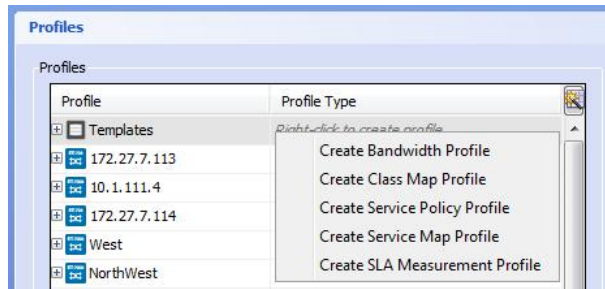
1. From the main menu choose **Edit>Profiles**, or click the **Profile Manager** button in the toolbar.

The Profiles window displays.

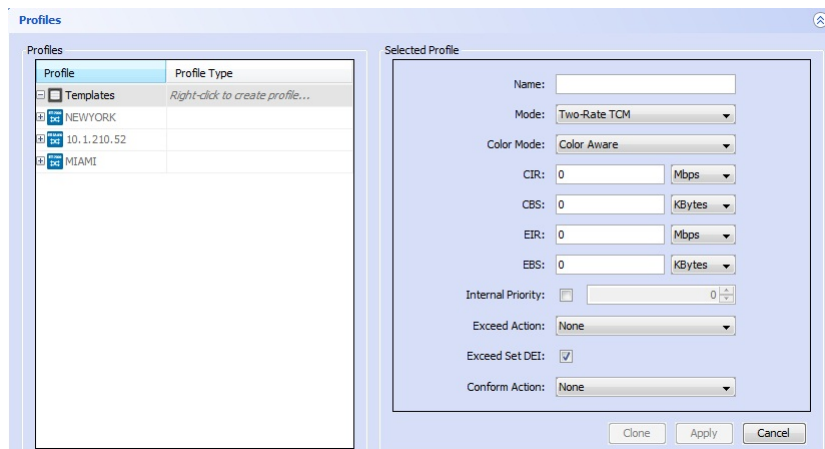


2. In the left panel, right-click on **Templates** and choose a profile type from the pop-up menu, as shown below.





The parameters for the selected profile type display in the right panel. The screen below shows the Bandwidth Profile parameters.



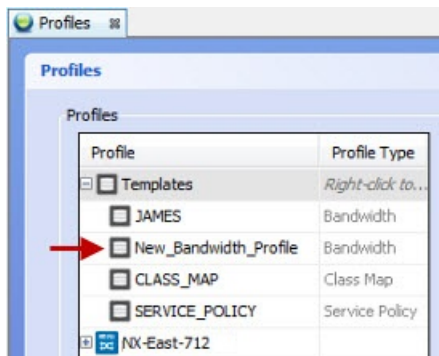
For information on setting parameters for the Bandwidth, Service Policy, Class Map, or Service Map profiles, see:

- [Bandwidth Profile Templates on page 431](#)
- [Class Map Profile Templates on page 434](#)
- [Service Policy Profile Templates on page 436](#)
- [Service Map Profile Templates on page 438](#)

3. Enter a unique name for the profile in the Name field, and set the other parameters using the drop-down menu.

4. Click **Apply**.

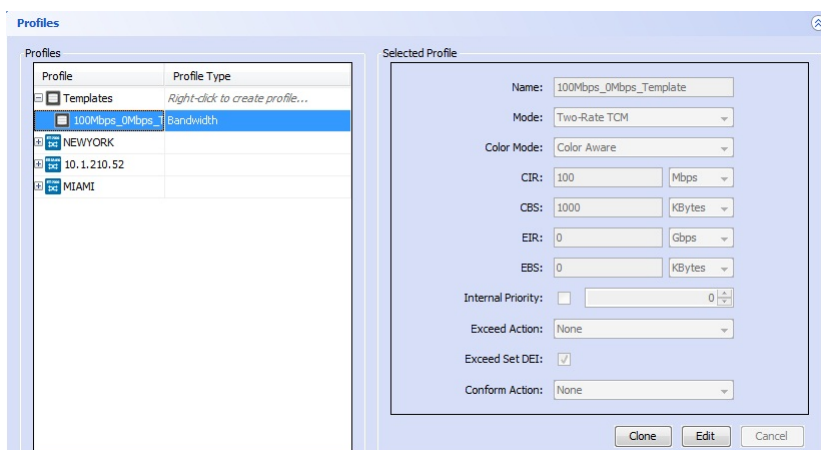
The newly-created profile appears under Templates in the left panel of the Profiles window.



### Editing an Existing Profile Template

Only profile templates can be edited. Auto-discovered profiles from network elements cannot be edited using PSM.

1. From the main menu choose **Edit>Profiles**. The Profiles window displays.
2. Expand the Templates tree and select a profile to edit from the profile Templates list. The profile parameters are displayed in the Selected Profile section on the right side of the screen, as shown below.



3. To enable editing of the attributes, click the **Edit** button.



**NOTE:** The name of the profile template along with some other parameters cannot be changed this way. See [“Creating a Profile Template Through Cloning”](#) on page 431 for this type of operation.

4. Modify the parameters.
5. Click **Apply** to save the changes.

### Creating a Profile Template Through Cloning

---

You can clone from an existing profile (discovered from a network element) or from a profile template. Cloning creates a new template with all the same parameter values as the original. Cloned templates let users deploy proven profiles, thus reducing user input error.

1. From the main menu choose **Edit>Profiles**. The Profiles window is displayed.
2. Expand the profile or profile template list so that the profile or profile template you want to use as the source is displayed.
3. Right-click the profile or profile template that you want to be the source, and choose **Clone** from the pop-up menu.

The profile parameters are displayed in the Selected Profile section on the right panel with the Name field blank.

4. Enter a name, edit the parameters as required, and click the **Apply** button.

The cloned profile template is created and displayed in the expanded profile template list, and the original profile or profile template is left unmodified.

### Deleting a Profile Template

---

Only profile templates can be deleted. Auto-discovered profiles from network elements cannot be deleted using PSM.

1. From the main menu choose **Edit>Profiles**. The Profiles window displays.
2. In the Profiles area, right-click a profile Template from the expanded list, and choose **Delete** from the pop-up menu  
A confirmation dialog displays.
3. Select **OK** to delete profile template, or **Cancel** to keep the profile template.

## Bandwidth Profile Templates

Bandwidth Profiles are used for policing traffic to:

- control the maximum rate of traffic sent or received on an interface.
- partition a network into multiple priority levels or classes of service.

A bandwidth profile is the starting point of any policing function and can be configured for use at the CoS queue, logical interface, or Layer 2 (MAC) level. The figure below shows the parameters for a bandwidth profile.

Figure 85: Bandwidth Profile Template Parameters

There are three modes supported for Bandwidth Profile Templates:

- Two-Rate TCM (TriColor Marker)
- Single-Rate TCM
- CAR

For information about configuring CIR, CBS, EIR and EBS and Quality of Service / Class of Service, see the *BT17000 Series packetVX Solutions Guide*.



**NOTE:** Pre-10.3 BT17000 Series network elements and all BT1700 Series network elements use peak information rate and peak burst size instead of excess information rate and excess burst size. When managing those devices, PSM internally converts the EIR and EBS to the peak information rate and peak burst size. This conversion is performed transparently to the operator. The values shown on PSM continue to be the EIR and EBS, whereas the values shown on the CLI on those devices are the peak information rate and peak burst size.

### TCM Bandwidth Profiles

The Three Color (or Tricolor) Marking (TCM) scheme classifies packets as green, yellow or red based on user-defined rates and burst size values.

1. To create this type of Bandwidth Profile template, click the **New** button and select **Bandwidth** from the popup dialog.
2. In the Selected Profile attributes pane on the right side, select **Two-Rate TCM** or **Single-Rate TCM** from the Mode attribute.

You must provide a name for the profile template a number of rate values along with Color Mode and Action attributes.

3. Click **Apply** to accept the changes, or **Discard** to cancel.

---

### Two-rate TCM

Two-Rate TCM classifies packets based on two rates and two burst sizes. Two-Rate TCM is useful when the peak rate needs to be enforced.

The two rate values are Committed Information Rate (CIR) and Excess Information Rate (EIR).

The two burst size values are Committed Burst Size (CBS) and Excess Burst Size (EBS).

Traffic is marked green, yellow or red based on whether the packets arriving are below the CIR (green), exceed the CIR but not the EIR (yellow), or exceed the EIR (red).

---

### Single-rate TCM

Single-Rate TCM classifies packets based on a single rate and two burst sizes. Single-Rate TCM is useful when only the burst size matters.

The rate value is Committed Information Rate (CIR).

The two burst size values are Committed Burst Size (CBS) and Excess Burst Size (EBS).

Traffic is marked green, yellow or red based on whether the packets arriving are below the CBS (green), exceed the CBS but not the EBS (yellow), or exceed the EBS (red).

---

### CAR Bandwidth Profile Template

Committed Access Rate (CAR) allows you to configure a value above which any traffic is discarded.

To create this type of Bandwidth Profile template, click the New button and select "CAR" from the Mode attribute. Enter a name for the profile template and a CAR value. Click Apply to commit the changes or Discard to cancel.



**NOTE:** This type of Bandwidth Profile can be used only on the BT1700 Series network elements.

---

---

### Color Mode and Actions

The color mode for both Two-Rate and Single-Rate TCM is the same, either Color Aware or Color Blind. Color aware indicates that the existing color of the packet is taken into consideration when applying the bandwidth profile. Color blind indicates that the existing classification is ignored. The color (green or yellow) of a packet can be determined from the DEI bit in the VLAN tag.

Each color has an associated action that can be performed. The Conform Action applies to packets that are colored green and the Exceed Action applies to packets that are colored yellow. Incoming traffic that violates the profile is dropped. The options for assigning actions are as follows:

- **None:** no action is taken
- **Remark DSCP:** Sets the IP DSCP (differentiated service code point) value. The value can be in the range 0-63.

In addition, the Conform Action has the following option:

- **Set ToS from Priority:** Sets the IP type of service field

---

### Setting DEI on Exceed Traffic

Traffic that is classified as yellow can have the DEI bit set in the frame.

To select this option, choose **Exceed Set DEI**.



**NOTE:** This is only applicable for the BT17000 Series network elements.

---

---

### Internal Priority for Bandwidth Profile Templates

The internal priority is the primary determinant of the QoS for the flow. It is a value from 0 to 7 (inclusive) and is used to select the appropriate transmit queue for the packet when a bandwidth profile is used. If the bandwidth profile is assigned to a UNI, all frames received on the UNI will be assigned the indicated internal priority.

See the BT17000 Series documentation for more details.

## Class Map Profile Templates



**NOTE:** Class maps are not supported on the BT1805, BT1821, and BT1822.

---

Class Map Profiles specify the fields of a packet to be matched in order to determine the packets to classify.

Figure 86: Class Map Profile Template

Selected Profile

Name:

Type:

New Match:

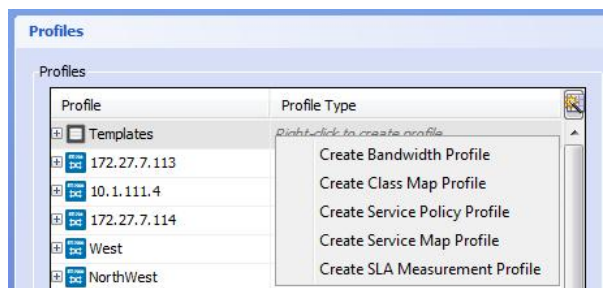
CVLAN:

Source IP:

Source IP Mask:

In Class Map profiles, at least one match criteria must be added. All criteria added to the profile must match in order for a packet to be classified by a particular Class Map Profile.

1. From the main menu choose **Edit>Profiles**. The **Profiles** window is displayed.
2. Right-click beside Templates and choose **Create Class Map Profile**.



Class Map fields are added to the Selected Profile window on the right.

3. Enter a name for the class map in the Name field.
4. From the type drop-down menu, select a class map type:
  - Ingress per Cos
  - Egress per CoS
  - Service Map
5. From the New Match drop-down list, select the criteria to match.
6. Click **Add**.

A new attribute is displayed based on the selection and a value will be required. An X will be displayed next to the attribute allowing the match criteria to be removed if desired.



**NOTE:** The BTI700 Series devices only support the following subset of Match criteria:

- C-VLAN
- C-VLAN Priority
- S-VLAN Priority
- Source MAC
- Destination MAC

Class Map profile templates work in conjunction with Service Policy Profile Templates. See [“Example: Activating EVPLAN and EVPLINE Services Using Service Maps for Flow Redirection”](#) on page 381 for an example on how to configure class maps.

## Service Policy Profile Templates



**NOTE:** Service policies are not supported on the BTI805, BTI821, and BTI822.

Service Policy Profile Templates are used to pair Bandwidth Profiles with Class Map Profiles.



Figure 87: Service Policy Profile Template

Selected Profile

Name:

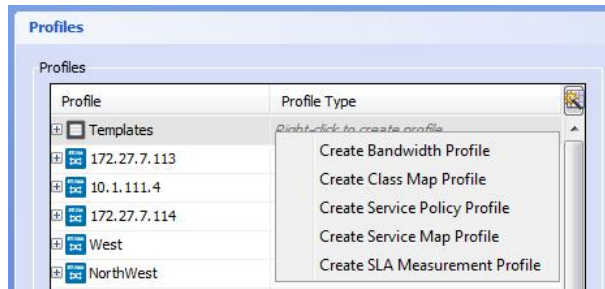
Class Map:	<input type="text" value="CM_Name"/>	Bandwidth:	<input type="text" value="10M_internet"/>
Class Map:	<input type="text" value="CM_Name 1"/>	Bandwidth:	<input type="text" value="20M_internet"/>

Any number of Ingress or Egress Class Map Profiles can be paired with Bandwidth Profiles in a Service Policy Profile provided that:

- all pairings are of the same type, either Ingress or Egress
- a Class Map profile can appear only once in a given Service Policy profile

To create a Service Policy Profile Template:

1. Create at least one Bandwidth Profile Template and one Class Map Profile Template. See [“Bandwidth Profile Templates” on page 431](#) and [“Class Map Profile Templates” on page 434](#).
2. From the main menu choose **Edit>Profiles**. The **Profiles** window is displayed.
3. Right-click beside Templates and choose **Create Service Policy Profile**. The Selected Profile fields display on the right.



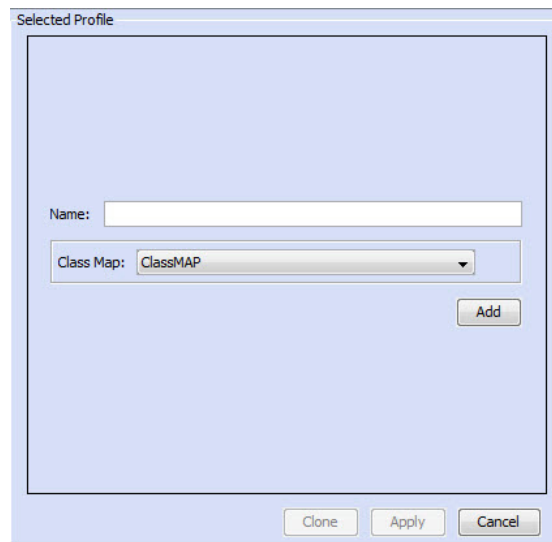
4. In the Name field, enter a unique name for the Service Policy.
5. From the Class Map and Bandwidth drop-down menus select a Class Map/Bandwidth pairing.
6. To add subsequent pairings to the Service Policy Profile, click **Add** and select the desired Class Map(s) and Bandwidth Profile(s).
7. When you are done, click **Apply**.

See [“Example: Activating EVPLAN and EVPLINE Services Using Service Maps for Flow Redirection”](#) on page 381 for an example on how to configure service policies.

## Service Map Profile Templates

Service Map Profile templates are used to associate Class Map Profiles with Service Policies.

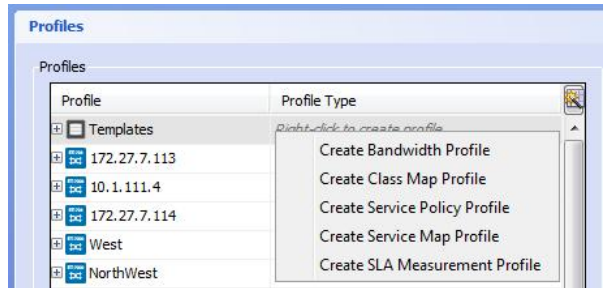
*Figure 88: Service Map Profile Template*



Any number of Class Map Profiles can be specified provided that each Class Map Profile appears only once in a given Service Map Profile.

To create a Service Map Profile Template:

1. Create at least one Class Map Profile Template of type Service Map. See [“Class Map Profile Templates” on page 434](#).
2. From the main menu choose **Edit>Profiles**. The **Profiles** window is displayed.
3. Right-click beside Templates and choose **Create Service Map Profile**. The Service Map Profile window is displayed on the right.



4. In the Name field, enter a unique name for the Service Map Profile.
5. From the Class Map drop-down menu select a Class Map.
6. To add more Class Maps to this Service Map Profile, click **Add** and select the desired Class Map(s).
7. When you are done, click **Apply**.

See [“Example: Activating EVPLAN and EVPLINE Services Using Service Maps for Flow Redirection” on page 381](#) for an example on how to configure service maps.

## SLA Measurement Profile Templates

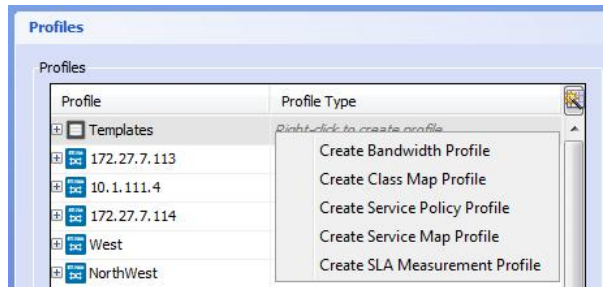
Use this procedure to create Y.1731-based SLA (service level agreement) Measurement Profile Templates which can be assigned to Ethernet services.

*Figure 89: SLA Measurement Profile Template*

 The screenshot shows the 'Selected Profile' configuration window for an SLA Measurement Profile. It contains several input fields and a dropdown menu. The fields are: 'Name' (empty), 'Far-End Loss Ratio' (0.001 %), 'Near-End Loss Ratio' (0.001 %), 'Maximum Delay' (3000 us), 'Average Delay' (2000 us), 'Maximum Delay Variation' (100 us), 'Average Delay Variation' (50 us), and 'Monitor Period' (15 Minutes). At the bottom right, there are three buttons: 'Clone', 'Apply', and 'Cancel'.

To create an SLA Measurement Profile Template:

1. From the main menu choose **Edit>Profiles**. The **Profiles** window is displayed.
2. Right-click beside **Templates** and choose **Create SLA Measurement Profile**. The Selected Profile fields display on the right.



3. In the Name field, enter a unique name for the SLA Measurement Policy.
4. Specify the attributes as desired.
5. When you are done, click **Apply**.

## CHAPTER 13

# Managing Pseudowire Services

- [Introduction on page 441](#)
- [Visualizing a Pseudowire Service on page 441](#)
- [Service Activation on page 444](#)
- [Modifying a Pseudowire Service on page 450](#)
- [Deleting a Pseudowire Service on page 451](#)

## Introduction

---

A pseudowire service provides pseudowire connectivity between pseudowire endpoints. A pseudowire endpoint is a TDM DS1/E1 interface on a pseudowire-capable module.

The incoming bitstream on the TDM interface is encapsulated within Ethernet frames and transported across the network as regular Ethernet traffic. At the egress, the bitstream is extracted from the Ethernet frames and transmitted out the DS1/E1 interface at the far end.

PSM can be used to manage pseudowire services on the BT1810.

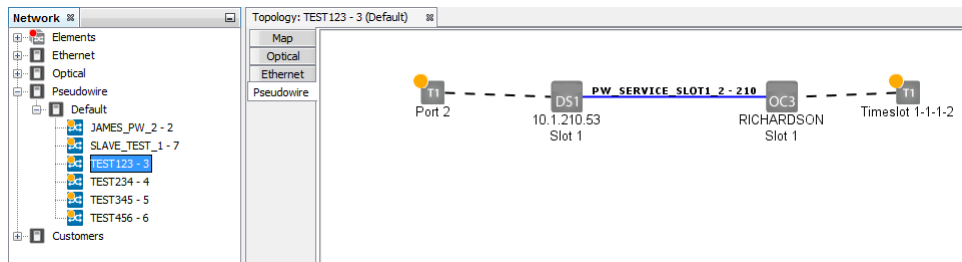
## Visualizing a Pseudowire Service

---

Use some or all of the techniques in this procedure to visualize a pseudowire service.

1. In the Network tree, select the desired pseudowire service.

The selected pseudowire service topology view opens in the main map window.

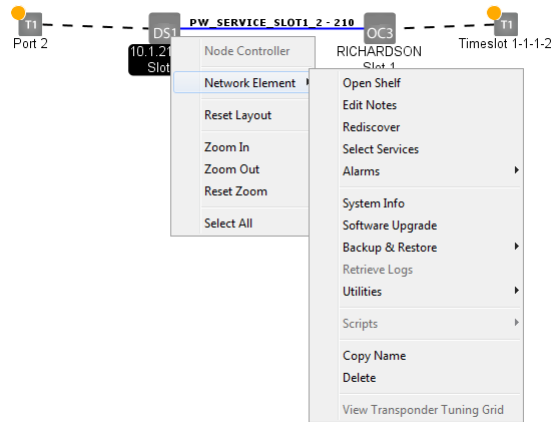


**NOTE:** If this is your first time visualizing this service, you will see the administratively-defined default layout if it exists. If a default layout does not exist for this service, then you will see the layout that PSM automatically generates. See 8.



**NOTE:** If this is your second or subsequent time visualizing this service, you will see the layout that existed when you last exited this service view.

2. To see details on a network element, link, or port, hover over the network element, link, or port.
3. To see the equipment on a network element, double-click the NE.  
The equipment and connections are shown in a zoomed-in view.
4. To change the size of the service view:
  - a. Right-click the background and select **Zoom In** to increase the view size
  - b. Right-click the background and select **Zoom Out** to decrease the view size
  - c. Right-click the background and select **Reset Zoom** to return the view size to its original size
5. Right-click a network element and select **Network Element** to see the regular NE menu options.



6. To move elements in this view, drag elements to the desired location.
7. To move all of the ports and switches in the service, choose **Select All** and drag the service within the window.
8. You can save the current layout as the default, or revert to the default, or revert to the layout that PSM automatically generates.
  - a. To save the current layout as the default layout for this service, right-click the background and select **Save Layout as Default**.



**NOTE:** You must have administrator privileges to execute this command.

Once the current layout is saved as the default, subsequent users who visualize this service will be able to see the current layout.

- b. To reset the current layout to the default, right-click the background and select **Reset Layout to Default**.
  - c. To reset the current layout to the layout that PSM automatically generates, right-click the background and select **Reset Layout**.
9. To save the service screen view as an image:
  - a. Select **Save Service Image**.  
The **Save Service Image** dialog appears.
  - b. Navigate to the desired folder and enter the filename.  
The default file format is png. To save the file in jpg format, enter .jpg at the end of the filename.
  - c. Click **Save**.
10. To select all NEs in the service, click **Select Network Elements**.

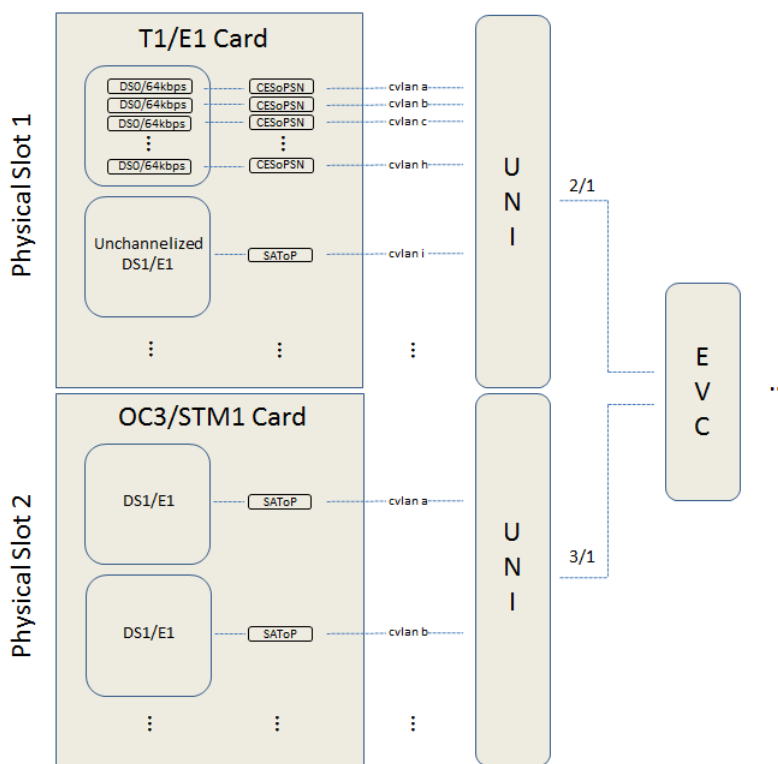
This brings you back to the main Topology Map view and shows all NEs in the service selected.

## Service Activation

PSM supports the Metro Ethernet Forum (MEF) paradigm for activating T1/E1 TDM (pseudowire) services in a BT1810 network. Service activation is performed by first creating a regular Ethernet service and then creating a pseudowire service that uses that Ethernet service.

Figure 90 on page 444 shows the component model for a BT1810 switch with a T1/E1 card residing in slot 1 and an OC3/STM1 card residing in slot 2.

Figure 90: BT1800 Series Component Model



Each card consists of a set of TDM and logical pseudowire interfaces. The pseudowire interfaces are logically connected to the UNI, and are distinguishable from each other through different CVLANs. Each card is automatically associated with its own UNI, with the UNI in logical slot 2 port 1 (2/1) associated with the card in physical slot 1, and the UNI in logical slot 3 port 1 (3/1) associated with the card in physical slot 2. These associations are hardcoded and cannot be changed.

The incoming bitstream on the TDM interface is processed on the card, encapsulated inside an Ethernet frame (with a destination MAC address of the remote TDM card), and passed to the local UNI. From there, the TDM traffic is transported across the network as regular Ethernet traffic.





**NOTE:** When configuring the underlying Ethernet service, you should take into consideration the delay variation requirements for a TDM circuit.

Although a TDM service is point-to-point, the Ethernet service (or EVC) that transports the TDM traffic can be EVPLINE or EVPLAN. If EVPLINE is used, then each TDM service uses its own point-to-point EVC. If EVPLAN is used, then more than one TDM service can share the same EVC. In the previous figure, all TDM services on the switch share a single EVC. Note that each TDM service is still point-to-point. The network routes the Ethernet frames based on the destination MAC address and CVLAN membership, so only the intended destination will receive the traffic.



**TIP:** For convenience, you can share a single EVC across multiple TDM services. In this way, you do not need to create an Ethernet service for each TDM service.

- [Activating a Pseudowire Service on page 445](#)

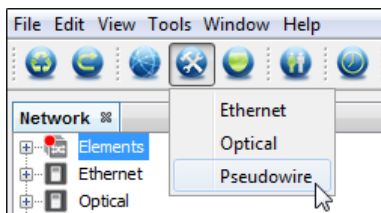
## Activating a Pseudowire Service

Use this procedure to configure and activate a pseudowire service on a BTI800 Series network.

### Prerequisites:

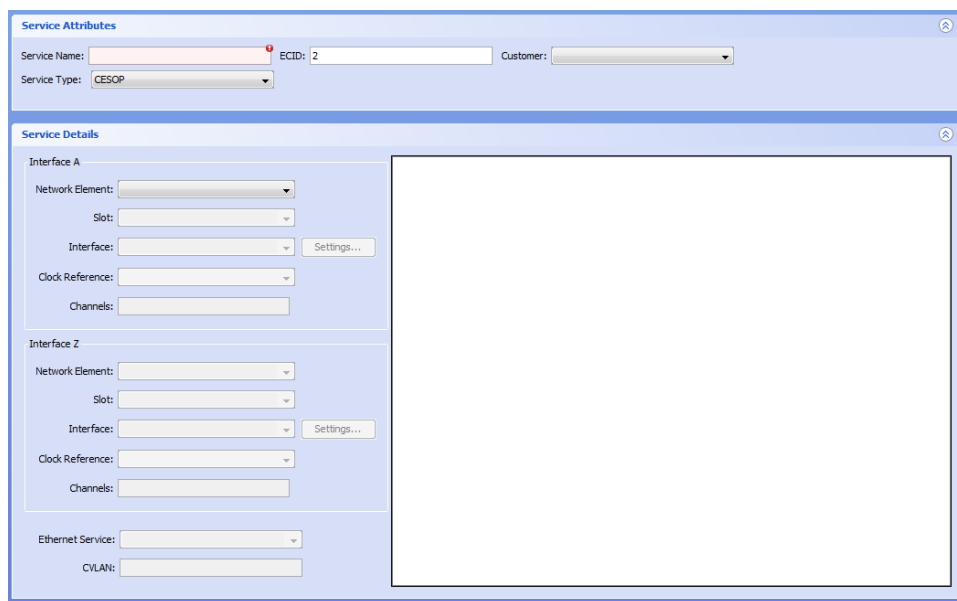
- All the necessary Ethernet NNIs have been configured in the network. If this network includes BTI7000 Series NEs, then all the necessary packetVX cards and virtual switches have been configured.
- The Ethernet service connecting the two TDM endpoints has been configured.
- The TDM endpoint interfaces have been configured.
- ERPS has been configured, as applicable. This prevents routing loops when multiple paths exist through the network.

1. Click the **Service Activation** button on the toolbar and choose **Pseudowire** from the drop-down menu.

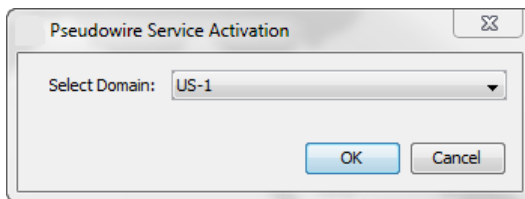


If you have one Ethernet domain only, the **Activate Pseudowire Service** window appears, as shown. Proceed to 3.

*Figure 91: Activate Pseudowire Service (CESOP)*



If you have multiple domains, a **Pseudowire Service Activation** pop-up dialog box is displayed, as shown. Proceed to 2.



2. From the **Select Domain** drop-down menu, select a domain in which to create the service. Click **OK**.


Although you are creating a pseudowire service, you still need to select the Ethernet domain in which you are running the service because you will need to associate the pseudowire service to an Ethernet service later.


3. In the **Service Attributes** pane of the **Activate Pseudowire Service** window, enter the required information as listed in the following table.

*Table 48: Fields in the Service Attributes Pane*

Field	Description	Required field?
Service Name	User-defined name that identifies the service. Must be unique to all pseudowire services in the domain.	Yes
ECID	Emulated circuit identifier. Must be unique to all pseudowire services in the domain.  The auto-populated value can be overridden.	Yes
Customer	User-defined. See <a href="#">“Adding a Customer” on page 454</a> .	Optional
Service Type	The service type can be <b>SATOP</b> or <b>CESOP</b> . By default, the service type is <b>SATOP</b> . When you select <b>CESOP</b> , additional fields are available for configuration.	Yes

4. Configure the **Interface A** endpoint.
  - a. In the **Service Details** pane, use the pulldown menu to select the **Network Element** for the **Interface A** endpoint.  
  
The pulldown menu is populated with all BT1800 Series nodes that have TDM cards inserted.
  - b. Select the **Slot** and **Interface** from the pulldown menus.  
  
The pulldown menus are populated with all possible selections. Only the interfaces (or timeslots) not already in use can be selected. Interfaces or timeslots that are part of an existing service are greyed out.  
  

 **NOTE:** Only ports that have been configured on the device as framed and enabled are selectable for a CESOP service.

 **NOTE:** Entries with an (M) designation can be configured as clock masters. Entries without that designation can only be configured as slaves (or use internal clocking).
  - c. Select the **Clock Reference**.
  - d. For CESOP, specify the **Channels** that make up the service.  
  
You can specify a single channel (e.g. **5**), a range of contiguous channels (e.g. **5-20**), non-contiguous channels (e.g. **5,9**), or a mix (e.g. **3,5-20**). For T1, the available channels are 1 to 24. For E1, the available channels are 1 to 31. A channel cannot belong to more than one service.



**NOTE:** If the Clock Reference is set to Adaptive Master, then you must select one, two, four, or eight channels.



**NOTE:** Channelized services can only be configured for T1/E1 cards.

- e. Configure the TDM and physical interface settings (optional).

Click on the **Settings** tab and set the TDM and physical interface (T1/E1 card only) attributes by clicking in the appropriate box.

**Table 49: TDM Attributes**

Attribute	Description	Range	Default
Customer VLAN Priority	This specifies the priority to assign to the service.	0 to 7	6
PDV (Jitter Buffer)	This specifies the size of the jitter buffer in microseconds.	2000 to 32000	5000
Payload Size	This specifies the payload size of the packetized bitstream in bytes. Both endpoints must have the same payload size.	SATOP: 192, 384, 576, 768, 960  CESOP: Depends on the number of channels. See <a href="#">Table 51 on page 448</a> .	SATOP: 192  CESOP: None.

**Table 50: Physical Interface Attributes (T1/E1 Card Only)**

Attribute	Description	Range	Default
Line Build Out	This specifies the line build out (in feet) for the interface.	0 to 133, 134 to 266, 267 to 399, 400 to 533, 534 to 655 feet	0 to 133
Line Code	This specifies the line coding for the interface.	AMI or B8ZS (T1) or HDB3 (E1)	B8ZS (T1) HDB3 (E1)

**Table 51: CESOP Payload Sizes**

Number of channels	Allowed payload sizes
1	64
2	64,96,128,160,192,224,256
3	96,120,144,168,192,216

Table 51: CESOP Payload Sizes (continued)

Number of channels	Allowed payload sizes
4	64,96,128,160,192,224,256
5	40,80,120,160,200,240,280,320
6	48,96,144,192,240,288,336
7	56,112,168,224,280,336
8	64,128,192,256,320
9	72,144,216,288
10	80,160,240,320
11	88,176,264,352
12	96,192,288
13	104,208,312
14	112,224,336
15	120,240
16	128,256
17	136,272
18	144,288
19	152,403
20	160,320
21	168,336
22	176,352
23	184
24	192
25	200
26	208
27	216

Table 51: CESOP Payload Sizes (continued)

Number of channels	Allowed payload sizes
28	224
29	232
30	240
31	248

- Repeat 4 for **Interface Z**.



**NOTE:** Unlike the BT1800 Series CLI, you do not need to enter the destination MAC address. PSM automatically determines the MAC address at both ends of the service.

- Select the **Ethernet Service** to use from the pulldown menu.

Only the Ethernet services that include the UNIs at both ends are shown.

- Specify the CVLAN to use for the service. This is the CVLAN that exists between the pseudowire endpoint and the Ethernet UNI.

The same CVLAN is used at both endpoints. The value itself is not important but it must be unique at each UNI.

- Click **Activate**. The service is activated.



**NOTE:** You must wait for the activation tasks to complete before performing any other operation on the NEs affected by this activation.

## Modifying a Pseudowire Service



**CAUTION:** Modifying a service might affect the service or the data traffic running on the service.

A stranded or semi-stranded service cannot be modified. A stranded or semi-stranded service refers to a service that has incomplete configuration that results in the absence of end-to-end connectivity.

1. In the Network tree view, expand the Pseudowire branch and double-click the service you want to modify.

The selected service appears in the main panel.

2. To modify the customer associated with this service, select a different customer in the **Customer** pulldown menu in the **Service Attributes** pane.
3. To modify the TDM or physical interface settings, select **Settings...** for **Interface A** or **Interface B** as desired.
4. Make changes to the **Customer VLAN Priority**, the **PDV (Jitter Buffer)**, the **Payload Size**, and/or the physical interface attributes and click **OK**.
5. After making all your changes, click **Apply**.

---

## Deleting a Pseudowire Service

1. To delete a service, right-click on the service in the Network tree view and choose **Delete**.

A dialog opens asking for confirmation.

2. Click **OK**.

The service is deleted, and is subsequently removed from the Network tree view the next time the node updates the proNX Service Manager.





# Managing Customers

- [Introduction on page 453](#)
- [Adding a Customer on page 454](#)
- [Modifying a Customer on page 455](#)
- [Deleting a Customer on page 456](#)

## Introduction

---

PSM allows you to add, modify and delete data about your customers. Customer data includes a company name, company reference, a list of employees specifying who is the primary and maintenance contact, and a notes section.

Customers can be associated with services during service activation. When this association is made, you will be able to see which services belong to which customers, and which alarms affect which customers.



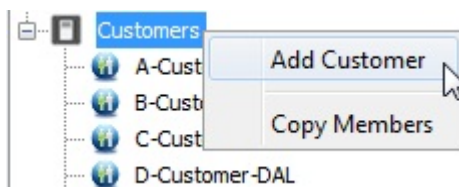
**NOTE:** Customer data and service association are part of the replicated data set when running with multiple servers. For more information on replicated data, see [“Running Multiple Servers with Server Replication” on page 30](#).

## Adding a Customer

1. To add a customer, click the Add Customer icon in the toolbar as shown below.



You can also right-click Customers in the Network tree and choose Add Customer as shown below.

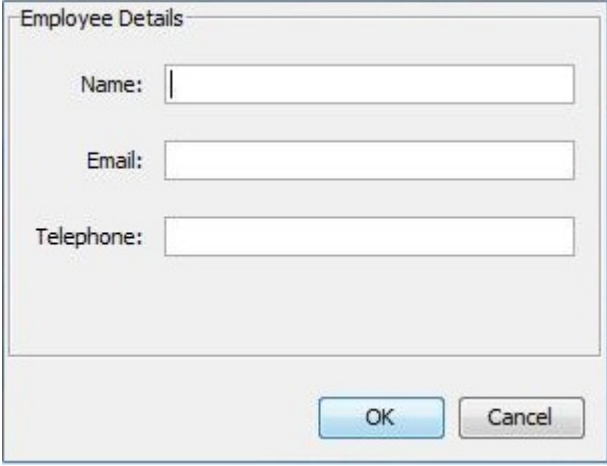


The Customer screen displays.

A screenshot of the 'Customer: <new>' form. The form has a title bar 'Customer: ABC Systems'. Below the title bar is a section 'Customer Details' containing several fields: 'Company Name' (with 'ABC Systems' entered), 'Company Reference' (empty), and a table with columns 'Employees', 'Email', and 'Telephone'. Below the table are 'Add', 'Edit', and 'Delete' buttons. Further down are 'Primary Contact' and 'Maintenance Contact' dropdown menus, and a 'Notes' text area. At the bottom right are 'Discard Edits' and 'Save' buttons.

2. In the Company Name field (required), enter a unique name for the customer.
3. In the Company Reference field (optional), enter additional customer identification information.
4. In the Employees table, click Add.

The Add Employee window displays. Enter a Name, Email and Telephone number, then click OK.

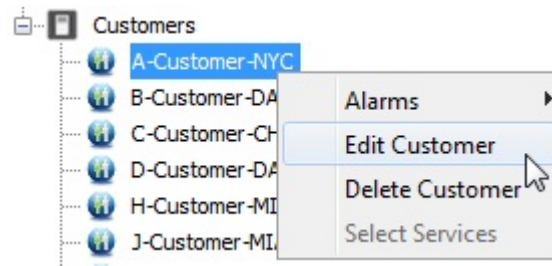
A dialog box titled "Employee Details" with a light gray background. It contains three text input fields: "Name:", "Email:", and "Telephone:". Each field has a small vertical cursor at the beginning. At the bottom right of the dialog box are two buttons: "OK" and "Cancel".

**NOTE:** Entering data in the Employee Details fields is optional; however, it is recommended that at least one field be completed.

5. To edit employee details, select an employee from the Employees window and click Edit. The Edit Employee window displays where you can change data.
6. To delete an employee record, select an employee from the Employees window and click Delete. You are prompted to confirm the deletion.
7. You can also designate employees listed in the Employees window to be a Primary Contact or a Maintenance Contact, and add text in the Notes fields:
  - In the Primary Contact field, choose an employee from the drop-down, or select <none>
  - In the Maintenance Contact field, choose an employee from the drop-down, or select <none>
  - In the Notes field, enter any additional text.
8. Click Save.

## Modifying a Customer

1. In the Customers area of the Network tree view, right-click the customer name and choose Edit Customer from the pop-up menu, as shown below.



The Customer Details screen displays. All fields in can be modified except the Company Name field.

- 
2. To save the changes, click Save. To discard the changes, click Discard Edits.

## Deleting a Customer

---

1. In the Customers area of the Network tree view, right-click the customer name and choose **Delete Customer**.

A confirmation dialog is displayed.

- 
2. Click **OK** to delete the customer or **Cancel** to cancel.

## CHAPTER 15

# Managing Network Element Alarms

- [Supported Network Elements and Devices on page 457](#)
- [Alarm Visualization on page 458](#)
- [Acknowledging, Emailing, and Clearing Alarms on page 469](#)
- [Assigning an Alarm to a User on page 470](#)
- [Viewing Historical Alarms on page 470](#)
- [Viewing Alarms Through an RSS Feed on page 472](#)
- [Sending Traps on the Northbound Interface on page 473](#)

## Supported Network Elements and Devices

---

PSM supports the display and processing of alarms for the following:

- BTI7800 Series network elements
- BTI7000 Series network elements
- BTI800 Series network elements
- BTI700 Series network elements
- MX Series and PTX Series routers
- QFX Series switches

## MX Series, PTX Series, and QFX Series Alarms

Not all MX Series and PTX Series and QFX Series alarms are reported by PSM. PSM reports the following alarms for these devices:

- Chassis alarms
- Link down
- Optical diagnostics (from JUNIPER-DOM-MIB)
- OTN (from JUNIPER-OTN-MIB)

Additionally, severities for chassis alarms are mapped as follows:

Table 52: Alarm Severity Mapping for Chassis Alarms

MX Series, PTX Series, QFX Series chassis alarm severity	PSM alarm severity
Major	Critical
Minor	Major
-	Minor

## Alarm Visualization

PSM displays alarms reported by discovered network elements in the Alarms panel, and provides an alarms summary at the bottom of the window. Alarms are displayed in table format as shown in the figure below. When you hover the cursor over an alarm description, a tool tip appears and provides more information on the alarm.

Figure 92: Alarm Table View

Alarm Description	NE	Source	Time Raised	Severity
Link down.	10.1.110.1	PVX-1-1-3-X1	14:06:48 EDT - 2012/09/28	CRITICAL
Link down.	10.1.110.1	PVX-1-1-3-X1	14:06:48 EDT - 2012/09/28	CRITICAL
Link down.	10.1.110.1	PVX-5-1-9-G10	14:06:44 EDT - 2012/09/28	CRITICAL
Link down.	10.1.110.1	PVX-5-1-9-G10	14:06:44 EDT - 2012/09/28	CRITICAL
Link down.	10.1.110.1	PVX-6-1-11-X3	14:06:31 EDT - 2012/09/28	CRITICAL
Link down.	10.1.110.1	PVX-3-11-5-X1	14:03:45 EDT - 2012/09/28	CRITICAL
Link down.	10.1.110.1	PVX-2-1-7-X1	14:03:45 EDT - 2012/09/28	CRITICAL

Summary: 16 (46) 2 (0) 0 (0) 0 (0) 67 (+65) Connected as admin/172.25.7.56 14:08:29



**NOTE:** Alarm times from each NE are translated into the current PSM server time, so variances in timezones are handled automatically when being displayed in the table. It is highly recommended that PSM and all NEs in the network use NTP servers for obtaining the time in order to avoid time discrepancies.

Alarms in the alarms table and in the alarms summary are color-coded by severity:

- Red - critical alarms
- Amber - major alarms
- Yellow - minor alarms
- Grey - acknowledged alarms
- Green - cleared alarms

An alarm remains in the table until it is cleared, at which time the alarm is removed from the table, either immediately or after a configurable delay. If no delay is configured, the alarm just disappears from the table, with no indication that the alarm has been cleared, save for its absence. If a delay is configured, the alarm changes color to green to signify that it has been cleared, and remains in the table for the delay period. At the end of this period, the alarm is removed from the table. For details on how to configure this option, see ["Setting Alarm Display Options" on page 269](#). Regardless of which option is configured,

when an alarm is cleared, the cleared alarms counters are incremented in the alarms summary bar at the bottom of the window. For information on the alarms summary bar, see [“Understanding the Alarms Summary Bar” on page 466](#)

Alarms are automatically retrieved from NEs and added to the alarms table upon initial node discovery and are kept synchronized using SNMP traps. When a device is discovered, the PSM server registers itself as a trap listener with the network element, which enables the application to receive notification of new or cleared alarms.

When you first log in to the PSM server, the PSM server retrieves outstanding alarms from discovered network elements, and populates the alarms table. Previously acknowledged alarms continue to be acknowledged, but previously cleared alarms are not remembered.

When a network element is deleted, the following occurs:

- Outstanding alarms raised by the deleted network element are removed from the alarms table, and the alarms counters in the summary bar are decremented accordingly.
- Acknowledged alarms for the deleted network element are removed from the alarms table, and the acknowledged alarms counters in the summary bar are decremented accordingly.



**NOTE:** Cleared alarms from the deleted network element are not removed and cleared alarms counters in the summary bar do not change from this deletion.

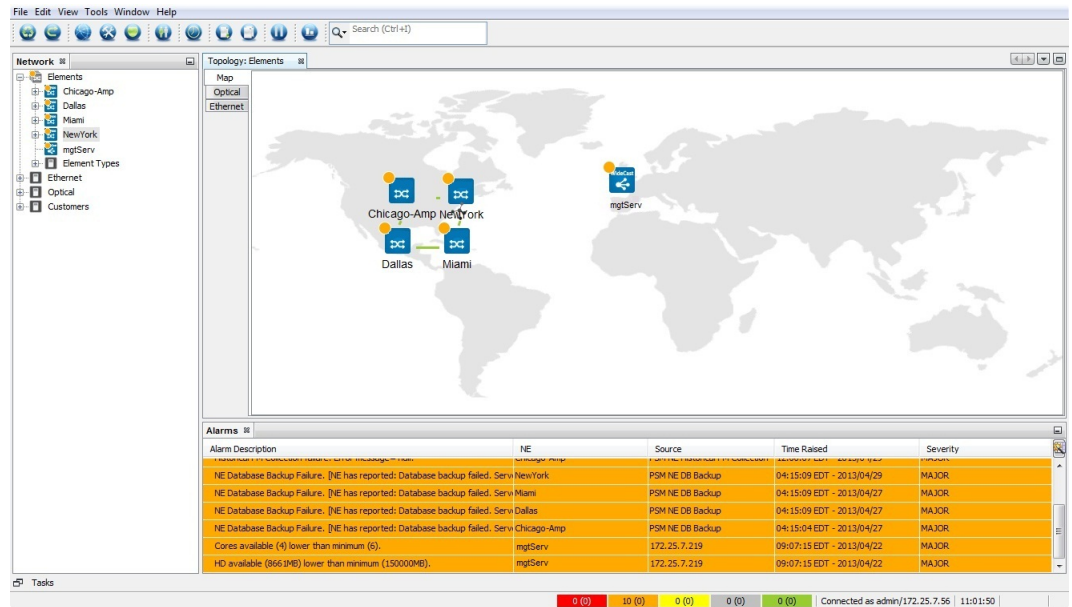
---

- [Viewing Current Alarms on page 460](#)
- [Understanding Alarm Timestamps on page 461](#)
- [Working with the Alarms Table on page 462](#)
- [Understanding the Alarms Summary Bar on page 466](#)

## Viewing Current Alarms

1. To view current alarms, from the main menu choose **View>Alarms > Alarms**.

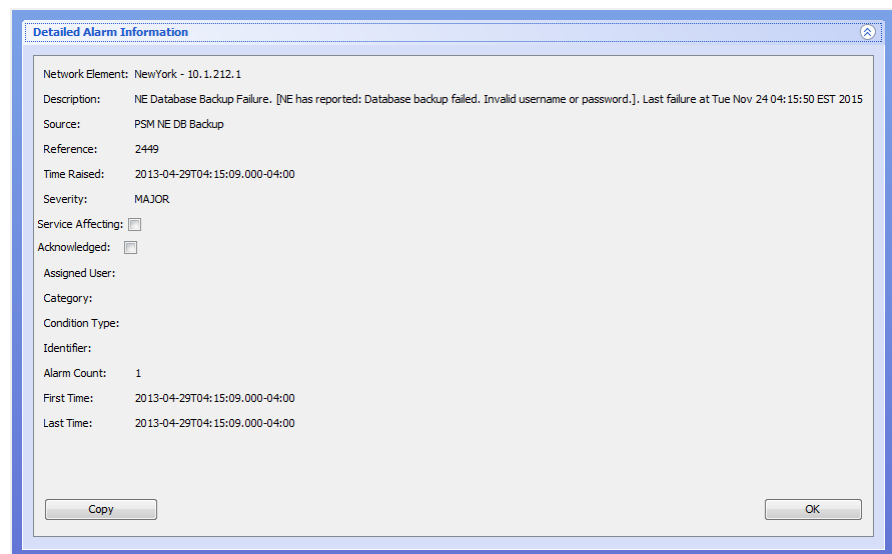
The current alarms are displayed in table form in the Alarms pane.



2. To filter the list of current alarms, see [“Working with the Alarms Table”](#) on page 462.

3. To view details of an alarm:
  - a. Right-click the alarm and select **Alarm Details >View**.

The **Detailed Alarm Information** window appears.







**NOTE:** Not all fields apply to all network elements. For an explanation of these fields, see [“BT17800 Alarm Details” on page 554](#).

- b. To copy to clipboard, click **Copy**.

You can now paste the alarms details text into another application.

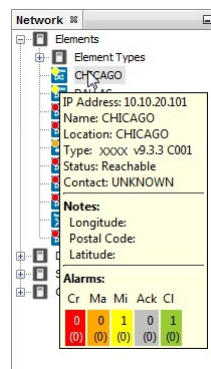
- c. Click **OK** to close the window.

4. To suspend alarm notifications, right-click in the Alarms pane title bar and select **Suspend Alarm Notifications**.

Alarms continue to be collected in the background but the alarms table and summary bar are not updated with newly-raised alarms, newly-cleared alarms, or newly-acknowledged alarms. The delay timer for existing cleared alarms continues to count down but the cleared alarms remain in the table even after the delay period expires.

Only after alarm notifications have resumed, either from operator intervention or from configured timeout, are the alarms table and summary bar updated. Newly-raised alarms are now added to the table. Cleared alarms that timed out while alarms were suspended are now removed from the table. Alarms that were cleared while alarms were suspended now change color to green and the delay timer started. Alarms that were acknowledged while alarms were suspended now change color to grey. The counters in the alarms summary bar are now updated accordingly.

5. To see an alarms summary for individual NEs or network element groups, hover over the element in the navigation pane.



## Understanding Alarm Timestamps

The timestamp of an alarm might undergo multiple time zone adjustments by the time the PSM Client displays the alarm to the user. The network element that raises the alarm, the PSM Server that receives the alarm, and the PSM Client that displays the alarm can all be in different time zones. In order to be able to correlate alarms, it is important to understand how PSM performs alarm timestamping.

### How the PSM Server Timestamps the Alarms

---

When an alarm condition occurs, the network element sends a trap to the PSM Server. The server timestamps the alarm based on when the server receives the trap. This timestamp is relative to the server's local time zone. Some network elements include a network element timestamp in the trap. In this situation, the PSM Server uses the network element timestamp (converted to the local server time zone) instead of the time when the server receives the trap.



**NOTE:** Some network elements might lose the original alarm timestamp when the network element is rebooted. In this situation, the alarm timestamp shown using the network element's CLI might be different from the timestamp shown on the PSM Server. The PSM Server continues to use the original alarm timestamp.

---

### How the PSM Server Timestamps the Clears

---

When an alarm condition is cleared, the network element sends a clear trap to the PSM Server. The server timestamps the clear based on when the server receives the clear trap. This timestamp is relative to the server's local time zone. Network elements do not include a network element timestamp in the clear trap, so the PSM Server always uses the time when the clear trap is received.

### How the PSM Client Displays Timestamps

---

The PSM Client converts the timestamp reported by the PSM Server to the client's local time zone. All timestamps displayed by the client are therefore local to the client's time zone.

## Working with the Alarms Table

The PSM client displays alarms in table format so you can sort alarms by column, and filter alarms by type.

### Sorting the Alarms Table

---

The alarms table can be sorted in the following ways:

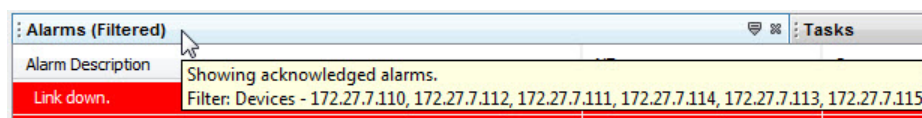
- To sort the Alarms table by a column, click the column title.
- To change the order (ascending or descending) of a column, click the column heading until the arrow shows ascending or descending order as desired.
- To hide a column, right-click any column title and uncheck the column name you want to hide in the drop-down menu. The Network Element/Alarm column cannot be hidden.
- To show or hide columns in the alarms table, right-click the Alarms Description column header and from the drop-down menu select the columns that you want to show or hide.

<input checked="" type="checkbox"/>	Alarm Description
	Category: The alarm's category, if applicable.
	Condition Type: The alarm's condition type, if applicable.
	Identifier: Shelf or port identifier, if applicable.
<input checked="" type="checkbox"/>	NE: IP address or system name of the NE.
	Service Affecting: Whether the alarm is Service Affecting or not.
<input checked="" type="checkbox"/>	Severity: Severity of the alarm, eg Critical, Major, Minor.
<input checked="" type="checkbox"/>	Source: Source of the alarm, eg port, card.
	Time Cleared: The time the alarm was cleared, in server time zone.
<input checked="" type="checkbox"/>	Time Raised: The time the alarm was raised, in server time zone.
	User Assigned: Indicates which user the alarm has been assigned to.

### Filtering the Alarms Table

The alarms table behaves as follows:

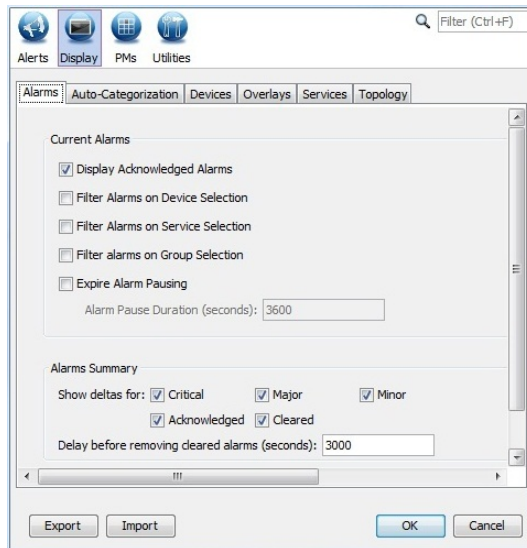
- If there is no alarm filtering applied, the alarms window title is displayed as "Alarms".
- If a filter is applied, the title changes to indicate the applied filter, for example "Alarms (Devices - 10.1.103.6)".
- If the filter description is too long to display completely, the title changes to "Alarms (filtered)".
- By hovering over the alarms table title bar, a tool tip is displayed listing the applied filter attributes.



- Each time a new entity or filter is chosen, the previous filtering is cleared and the alarms table displays the alarms that pertain to the chosen criteria.

The alarms table can be filtered in the following ways:

- From the main menu, choose **Tool>Options**. Click **Display**, and then click **Alarms** and configure the alarm display options as desired.



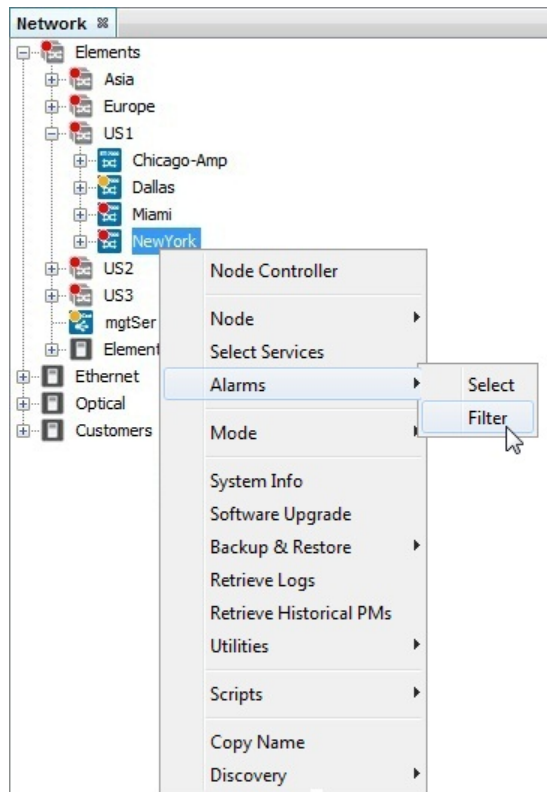
See “Setting Alarm Display Options” on page 269 for an explanation of these fields

- To filter the table to show only a particular set of alarms, right-click a cell in the column of the alarms table that has the data you want to filter with, and choose the filter option **Show only rows where** to filter out (hide) all other entries from the table. In the following screen, the filter chosen is to show only XFP failure alarms.

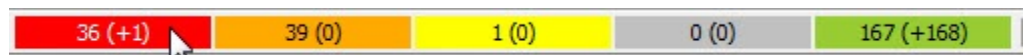
Alarms				
Alarm Description	NE	Source	Time Raised	Severity
XFP failure.	FRKTN-204-4	XFP-1-3-1	14:11:09 EDT - 2013/04/12	CRITICAL
XFP failure.	Node Controller	XFP-1-3-1	14:10:56 EDT - 2013/04/12	CRITICAL
XFP failure.		XFP-1-3-1	14:10:50 EDT - 2013/04/12	CRITICAL
XFP failure.		XFP-1-3-1	14:10:35 EDT - 2013/04/12	CRITICAL
XFP failure.		XFP-1-3-1	14:10:27 EDT - 2013/04/12	CRITICAL
XFP failure.		XFP-1-3-1	14:10:10 EDT - 2013/04/12	CRITICAL
XFP failure.		XFP-1-3-1	14:09:56 EDT - 2013/04/12	CRITICAL
XFP failure.		XFP-1-3-1	14:09:36 EDT - 2013/04/12	CRITICAL
XFP failure.	FRKTN-204-4	XFP-1-3-1	14:09:26 EDT - 2013/04/12	CRITICAL
XFP failure.	FRKTN-204-4	XFP-1-3-1	14:09:01 EDT - 2013/04/12	CRITICAL
XFP failure.	FRKTN-204-4	XFP-1-3-1	14:08:50 EDT - 2013/04/12	CRITICAL

Summary: 35 (0) -40 (+1) 1 (0) 0 (0) 90 (+91) Connected as admin/172.25.7.56 | 09:19:39

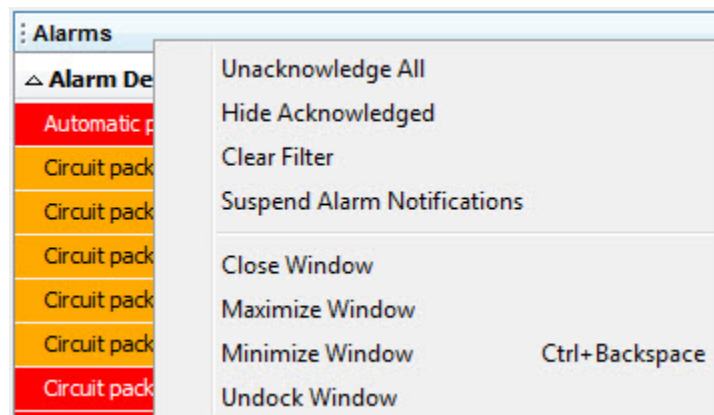
- To filter the table to show alarms that pertain only to a particular NE, service, or group, in the tree view right-click the entity and choose **Alarms>Filter**.



- To quickly filter alarms based on severity, click a severity in the alarms summary bar to apply a filter for that severity. For example, clicking in the critical alarms section of the summary bar applies a **Severity = CRITICAL** filter to alarms in the alarms pane.



- To remove filtering, right-click the alarms table header, and choose **Clear Filter** from the drop down menu.



Alternatively, right-click any cell in the alarms table and choose **Show only rows where>No Filter**.

## Using Service/Alarm Correlation

PSM provides the capability to view the alarms that pertain to a particular service, or to view the services that are affected by a given alarm.

- To view the alarms that pertain to a service, in the Service tree view, select the service, right-click a service and choose **Alarms>Select**. The alarms that pertain to the selected service are highlighted in blue. In the following illustration, there is a single alarm affecting the selected service.

Alarms (Filtered)		Tasks		
Alarm Description	NE	Source	Time Raised	Severity
SFP missing.	10.1.210.31	SFP-1-1-G4	10:47:12 EST - 2011/11/29	CRITICAL
Link down.	10.1.210.30	PVX-1-1-1-G12	14:31:00 EST - 2011/11/18	CRITICAL

- To determine the service(s) affected by an alarm, in the Alarms window select the alarm, right-click and choose **Select Affected Services**.

Alarms (Filtered)		Tasks		
Alarm Description	NE	Source	Time Raised	Severity
SFP missing.	10.1.210.31	SFP-1-1-G4	10:47:12 EST - 2011/11/29	CRITICAL
Link down.	10.1.210.30	PVX-1-1-1-G12	14:31:00 EST - 2011/11/18	CRITICAL
Link down.	10.1.210.32	GigE/4	13:18:36 EST - 2011/11/18	CRITICAL
SFP missing.	10.1.210.31	SFP-1-1-G3	10:46:01 EST - 2011/11/11	CRITICAL
Link down.	10.1.210.32	GigE/3	10:41:06 EST - 2011/11/11	CRITICAL
Link down.	ARDNIDMLR1	GigE/6	14:13:14 EDT - 2011/10/27	CRITICAL
Link down.	ARDNIDMLR1	GigE/5	14:13:14 EDT - 2011/10/27	CRITICAL

The affected service is highlighted in the Services tree.

- To see an alarm summary for the service, hover over the service name.

A summary of the number of critical, major, minor, and acknowledged alarms is displayed beneath the service name.

## Suspending Alarm Notification

If the network is undergoing a lot of alarm activity, you can suspend changes to the alarms table.

- To suspend alarm notification, from the main menu click the **Suspend Alarm Notifications** icon, or, alternatively, right-click the alarms table header, and choose **Suspend Alarm Notifications** from the drop-down menu. In this case the alarms window title is displayed as "Alarms (Suspended)" and the alarms window does not show any new alarms changes.
- To resume alarm notification, from the main menu click the **Resume Alarm Notifications** icon, or, alternatively, right-click the alarms table header, and choose **Resume Alarm Notifications** from the drop-down menu. The PSM client asks the PSM Server for the latest active alarms list (including alarm clear requests) and updates the alarms window appropriately. The alarms window title changes back to "Alarms".

## Understanding the Alarms Summary Bar

The PSM Client displays an alarms summary at the bottom of the window, and in various summary views, color-coded by severity.

20 (+10)	2 (0)	0 (0)	0 (0)	113 (+111)
----------	-------	-------	-------	------------

Table 53: Alarms Summary Bar

Color	Type	Notes
Red	Critical	<p>The value outside the parentheses represents the current number of outstanding alarms at the indicated severity, and is equivalent to the number of outstanding alarms in the alarms table for that severity. This counter is not resettable.</p> <p>The value inside the parentheses is an incremental value that represents the difference (or delta) between the current number of outstanding alarms and the number of outstanding alarms when the counter was last reset. A positive value indicates that the number of outstanding alarms has increased. A negative value indicates that the number of outstanding alarms has decreased. This value is not individually resettable, and can only be reset together with the deltas for the other alarms.</p> <p>Both values are incremented for any alarms retrieved when a new network element is discovered.</p> <p>Both values are decremented for any alarms removed when a network element is deleted.</p>
Amber	Major	
Yellow	Minor	
Grey	Acknowledged	<p>The value outside the parentheses represents the current number of acknowledged alarms, and is equivalent to the number of acknowledged alarms in the alarms table. This counter is not resettable.</p> <p>The value inside the parentheses is an incremental value that represents the difference (or delta) between the current number of acknowledged alarms and the number of acknowledged alarms when the counter was last reset. A positive value indicates that the number of acknowledged alarms has increased. A negative value indicates that the number of acknowledged alarms has decreased (through an operator unacknowledge action). This value is not individually resettable, and can only be reset together with the deltas for the other alarms.</p> <p>Both values are decremented for any acknowledged alarms removed when a network element is deleted.</p>
Green	Cleared	<p>The value outside the parentheses is an incremental value that represents the difference between the current number of cleared alarms and the number of cleared alarms when the counter was last reset. This number can only increment and cannot decrement. There is no correlation between this value and the number of cleared alarms in the alarms table. Cleared alarms are automatically purged from the alarms table after a configurable time period. This value is individually resettable.</p> <p>The value inside the parentheses is an incremental value that represents the difference (or delta) between the current number of cleared alarms and the number of cleared alarms when the counter was last reset. This number can only increment and cannot decrement. This value is not individually resettable, and can only be reset together with the deltas for the other alarms.</p> <p>Both values are unaffected by the addition or deletion of any network elements.</p>

### Resetting the Deltas

When you first log in to the PSM server, the delta values (including both cleared alarms counters) are reset to 0. Subsequently, the delta values can be reset as follows:

- To reset the values inside the parentheses, right-click anywhere in the alarms summary bar or in the Alarms pane title bar and select **Reset Summary Deltas**. This resets all deltas concurrently.
- To reset the cleared alarms value outside the parentheses, right-click anywhere in the alarms summary bar or in the Alarms pane title bar and select **Reset Clear Summary**.

### Interpreting the Deltas

The alarms summary provides hints on what is happening in the network. You might need to interpret the summary holistically rather than as independent counters.

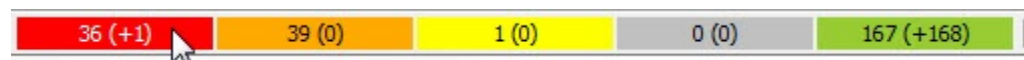
[Table 54 on page 468](#) lists general guidelines on how to interpret the summary, and describes some common causes that could precipitate the observed situations. Because other causes are possible, you should investigate further to confirm what is indeed transpiring.

**Table 54: Interpreting the Alarms Summary**

Observed situation	Might indicate ...
High critical/major/minor alarms delta, high cleared alarms delta	Flapping port or frequent intermittent failure and restoration, together with a failure of a shared component, network element, or link.
High critical/major/minor alarms delta, low cleared alarms delta	Failure of a shared component, network element, or link.
Low critical/major/minor alarms delta, high cleared alarms delta	Flapping port or frequent intermittent failure and restoration.
Low critical/major/minor alarms delta, low cleared alarms delta	No change.
High (negative) critical/major/minor alarms delta, high cleared alarms delta	Restoration of a shared component, network element, or link, and a possible flapping port or frequent intermittent failure and restoration.

### Filtering Based on Alarm Severity

The alarms summary bar provides a quick way to filter alarms based on alarm severity. Simply click on a severity to apply a filter for that severity. For example, clicking in the critical alarms section of the summary bar applies a **Severity = CRITICAL** filter to alarms in the alarms pane.





## Acknowledging, Emailing, and Clearing Alarms

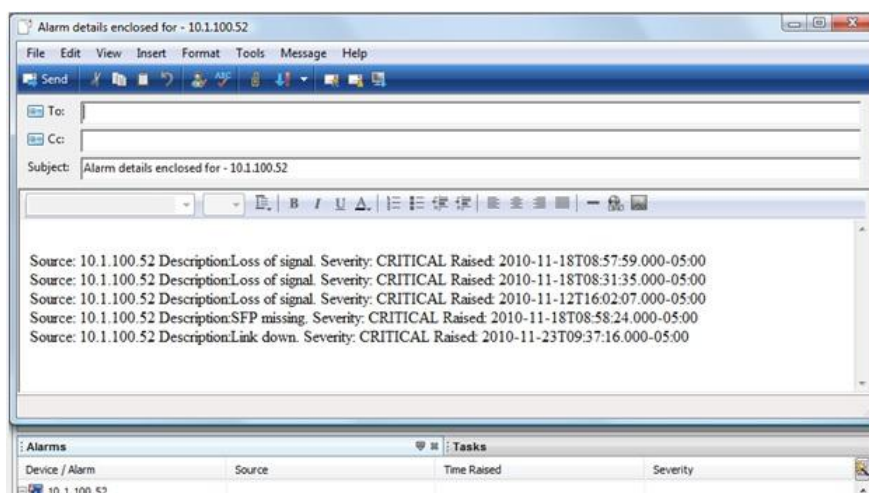
1. To acknowledge an alarm, select the alarm from the table, right-click and select **Acknowledge**.

The alarm is set to "Acknowledged" and turns grey, or, if "Hide Acknowledged" has been selected, is removed from the list.



**NOTE:** Alarm acknowledgements are part of the replicated data set when running with multiple servers. For more information on replicated data, see ["Running Multiple Servers with Server Replication" on page 30](#).

2. To hide acknowledged alarms, right-click on the **Alarms** tab and choose **Hide Acknowledged**. All alarms that are set to "Acknowledged" are removed from the alarms list. The alarms remain in the server and are available to other clients.
3. To show acknowledged alarms, right-click on the **Alarms** tab and choose **Show Acknowledged**. Acknowledged alarms are displayed and are grey in color.
4. To unacknowledge all alarms on the client, right-click the Alarms view heading and select **Unacknowledge All**.
5. To email details about one or more alarms, select one or more alarms (by holding the Shift or Ctrl key on the keyboard) from the list, right-click and select **Alarm Details >Email**. A new email is created in your local email application with the details of all the selected alarms populated in the body of the email.



6. You cannot clear an NE-generated alarm. You can only clear alarms that have been generated by the PSM. To manually clear a PSM-generated alarm, right-click on the

alarm and choose **Clear NMS Generated Alarm**. Once cleared, you cannot restore an alarm.

## Assigning an Alarm to a User

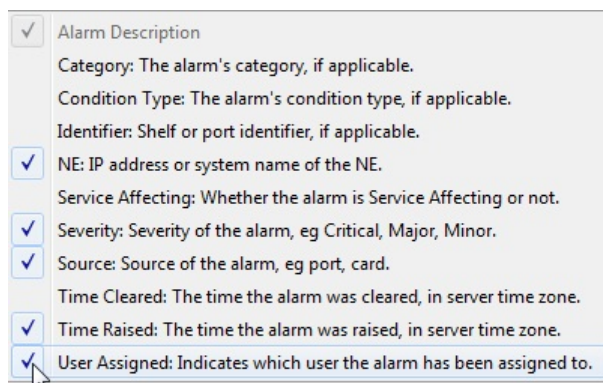
By assigning an alarm to a user, alarms can be filtered by user name.

1. In the alarm window, right-click on an alarm and choose **Assign Alarm to User** and choose the desired user from the list.



**NOTE:** Alarm assignments are part of the replicated data set when running with multiple servers. For more information on replicated data, see [“Running Multiple Servers with Server Replication” on page 30](#).

2. To filter the list of current alarms by assigned user, the "User Assigned" column must be displayed. Do this by right-clicking beside one of the column headers to display the drop-down menu and ensure that the "User Assigned:..." attribute is checked.



For more information on filtering options, see [“Working with the Alarms Table” on page 462](#).

## Viewing Historical Alarms

Use this procedure to view the historical alarms table.

Historical Alarms provides you with a view of all resolved and unresolved alarms. To help you manage this list, PSM allows you to apply filters to narrow down the view to the desired subset.

PSM builds the historical alarms list from active alarms as they are raised (and when NEs are discovered).

Additionally, for the BT17000 Series NEs, PSM reads the Alarm Logs table available on the NE, and supplements the historical alarms list with any alarms that are found in that table but missing from PSM's historical alarms list. The PSM server reads that table

during NE discovery, and periodically thereafter to ensure the lists are synchronized. The timestamps for the added alarms are based on the timestamps retrieved from the network element, adjusted for the local PSM server's time zone.

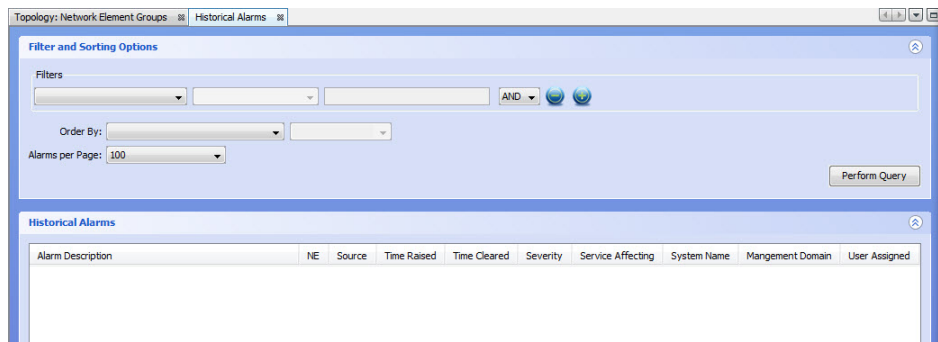
For the other types of NEs (including the BT17800 Series NEs), PSM builds the historical alarms list based solely on alarms it sees. Consequently, for those NEs, historical alarms do not contain alarms that were raised and cleared prior to PSM managing the device.



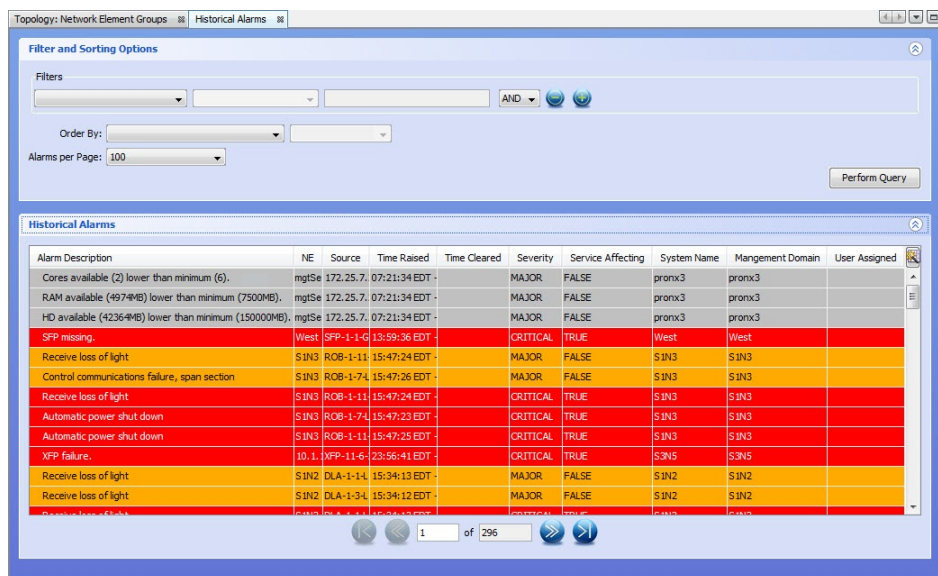
**NOTE:** In some cases, you might see duplicate alarms in the historical alarms table. If you delete and then rediscover a network element, PSM might insert the same alarm into the table as it reprocesses the outstanding alarms for the rediscovered NE.

To access Historical Alarms:

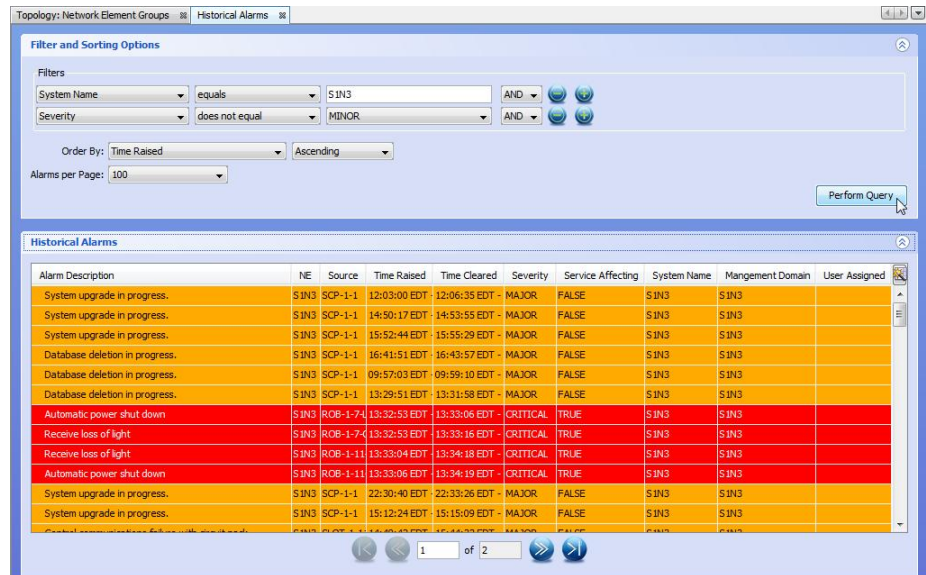
1. From the main menu choose **View>Alarms > Historical Alarms**.



2. To see the full alarm list, select **Perform Query** with no filters chosen.



- To filter historical alarms, select the desired filtering options from the Filter and Sorting Options dialog. You can order results by a specific field and with a set number of alarms displayed per page specified.



## Viewing Alarms Through an RSS Feed

The proNX Service Manager Client allows the user to view active alarms on their web browser through an RSS feed. To activate this way of viewing alarms, type the following URL into your web browser:

*https:<IP address of PSM server host>:<port>/AlarmsFeed*

You can also filter the alarms sent to your browser by adding an alarm severity to the URL, such as:

*https:<IP address of PSM server host>:<port>/AlarmsFeed/major*

The port number is specified by the **resources.address.port** attribute in the **common.properties** file.

The screen below shows a list of active alarms displayed in a web browser.

### PSM Alarms Feed

You are viewing a feed that contains frequently updated content. When you subscribe to a feed, it is added to the Common Feed List. Updated information from the feed is automatically downloaded to your computer and can be viewed in Internet Explorer and other programs. [Learn more about feeds.](#)

[Subscribe to this feed](#)

Displaying 154 / 154

All 154

Sort by:

▼ Date

Title

**10.1.204.15: Fan Fault - Fan 3**

Today, October 24, 2013, 1 minute ago

Raised by: 10.1.204.15 Description: Fan Fault Severity: MAJOR Raised: 2013-10-24T16:06:18.000-04:00

**10.1.220.65: Automatic power shutdown - line:1/8/1/1**

Today, October 24, 2013, 4 minutes ago

Raised by: 10.1.220.65 Description: Automatic power shutdown Severity: CRITICAL Raised: 2013-10-24T16:03:48.000-04:00

**10.1.220.65: Optical back reflection high threshold exceeded. - osc:1/8/1/1.1**

Today, October 24, 2013, 4 minutes ago

Raised by: 10.1.220.65 Description: Optical back reflection high threshold exceeded. Severity: MINOR Raised: 2013-10-24T16:03:47.000-04:00

**10.1.220.65: Loss of light, receive - osc:1/8/1/1.1**

Today, October 24, 2013, 4 minutes ago

Raised by: 10.1.220.65 Description: Loss of light, receive Severity: MAJOR Raised: 2013-10-24T16:03:47.000-04:00

**10.1.220.65: Loss of light, receive - line:1/8/1/1**

Today, October 24, 2013, 4 minutes ago

Raised by: 10.1.220.65 Description: Loss of light, receive Severity: MAJOR Raised: 2013-10-24T16:03:47.000-04:00

## Sending Traps on the Northbound Interface

The PSM northbound interface refers to communications between PSM and a higher level network management system, such as from the PSM server to a network management system in the NOC.

You can add trap receivers to transmit traps northbound from the PSM server. To limit the information that is forwarded, you can specify filtering parameters, such as **Date Raised**, **Severity**, and **Service Affecting** for each trap receiver.

When the PSM server receives an NE trap, PSM maps the NE trap information into a PSM trap before sending the resulting PSM trap to northbound trap receivers. This mapping is described in the PSM MIB (**bti-psm.my**). The northbound NMS must be able to parse the resulting PSM trap.

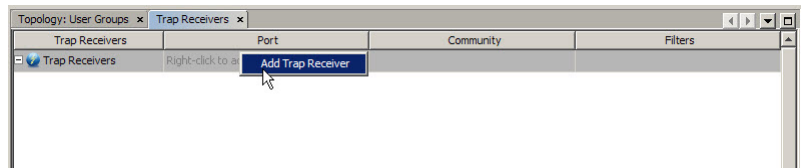


**NOTE:** The OID of the northbound trap is the BTI-PSM-MIB::notificationAlarms OID.

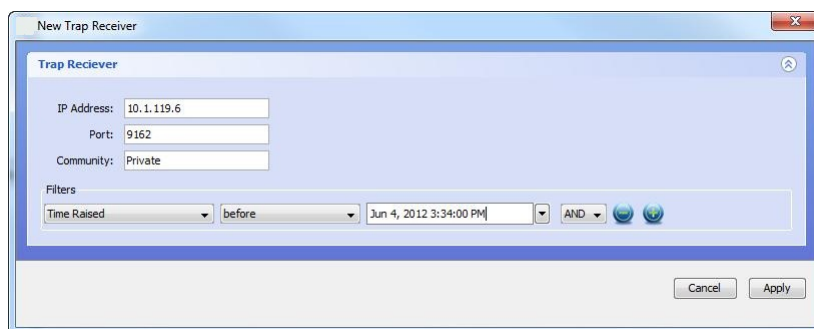
- [Adding a Trap Receiver for Alarms on page 473](#)
- [Modifying a Trap Receiver for Alarms on page 475](#)
- [Deleting a Trap Receiver for Alarms on page 475](#)

## Adding a Trap Receiver for Alarms

1. From the **Edit** menu, choose **Trap Receivers**.
2. On the **Trap Receivers** tab, right-click **Right-Click to Add**, and then click **Add Trap Receiver**.







3. In the **New Trap Receiver** dialog, specify the following settings:
  - **IP Address**
  - **Port**
  - **Community**
4. Optionally, choose values from the **Filters** drop-down lists to limit (filter) the information that is forwarded. Information can be filtered according to one or more of the following alarm-related parameters:
  - Alarm Description
  - IP Address
  - Source
  - Time Raised
  - Time Cleared
  - Severity
  - Service Affecting
  - Acknowledged
  - System Name
  - Domain Name
  - User Assigned
  - Category
  - Condition Type



5. Click **Apply**.





The trap receiver appears in the list on the **Trap Receivers** tab.

Topology: EvPlan  Trap Receivers 			
Trap Receivers	Port	Community	Filters
<div>  Trap Receivers         </div> <div>  10.1.119.6         </div>	<div>Right-click to add.</div> <div>9162</div>	Private	Time Raised less than 15:34:00 EDT -

- Repeat 2 to 5 for each trap receiver to be added.

## Modifying a Trap Receiver for Alarms

- From the **Edit** menu, choose **Trap Receivers**.
- On the **Trap Receivers** tab, right-click a trap-receiver, and then click **Edit Trap Receiver**.

Topology: EvPlan  Trap Receivers 			
Trap Receivers	Port	Community	Filters
<div>  Trap Receivers         </div> <div>  10.1.119.6         </div>	<div>Right-click to add.</div> <div>9162</div>	Private	Time Raised less than 15:34:00 EDT -

Edit Trap Receiver  
 Delete Trap Receiver

- In the **Edit Trap Receiver** dialog, modify settings as required, and then click **Apply**.

Edit Trap Receiver

Trap Receiver

IP Address: 10.1.119.6

Port: 9162

Community: Private


Filters


Time Raised

before

Jun 4, 2012 3:34:00 PM

AND





Cancel

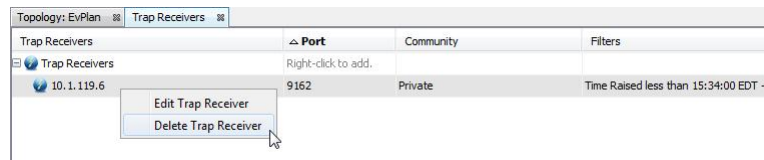
Apply

The modifications are applied and the **Edit Trap Receiver** dialog closes.

- Repeat 2 and 3 for each trap receiver to be modified.

## Deleting a Trap Receiver for Alarms

- From the **Edit** menu, choose **Trap Receivers**.
- On the **Trap Receivers** tab, right-click a trap receiver, and then click **Delete Trap Receiver**.



3. In the confirmation dialog, click **OK**.



The trap receiver is removed from the list on the **Trap Receivers** tab.

4. Repeat 2 and 3 for each trap receiver to be deleted.



# Managing Network Element System Software and FTP Servers

- [Adding an FTP or SFTP Server on page 477](#)
- [Modifying the Configuration for an FTP or SFTP Server on page 479](#)
- [Deleting an FTP or SFTP Server on page 480](#)
- [Manually Backing Up a Network Element Configuration Database on page 481](#)
- [Restoring a Configuration Database to a Network Element on page 482](#)
- [Upgrading System Software for a Network Element on page 484](#)
- [Restoring a Database to Factory Defaults on a BT17800 Network Element on page 487](#)

## Adding an FTP or SFTP Server

---

Use this procedure to add an FTP or SFTP server to the list of servers that PSM can use.

PSM tests the connectivity to the newly-added server and posts a status indicating whether the server can be reached and whether the specified subdirectory can be used.

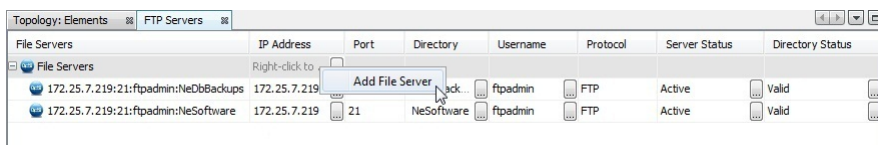
The PSM server installation includes a local (S)FTP server that is configured and used by default for NE database backup and restore, and NE system software upgrades. The local (S)FTP server is accessible using the following credentials:

- username: ftpadmin
- password: ftpadmin

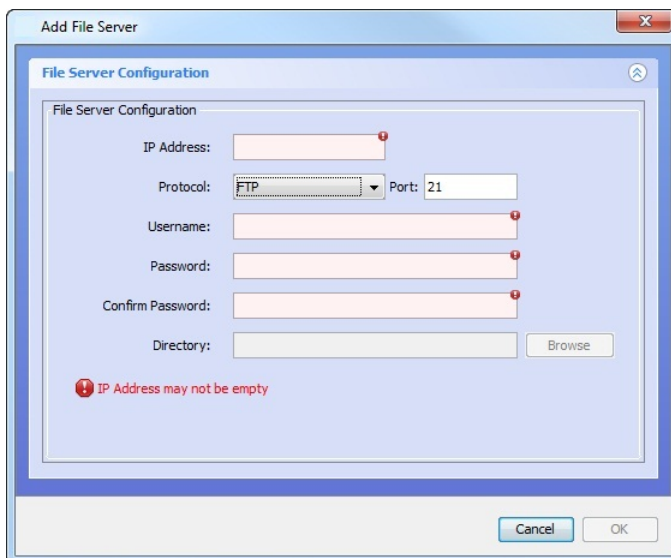
The default subdirectories created for database backups and software loads on the local (S)FTP server are **NeDbBackups** and **NeSoftware** respectively. The paths are relative to the FTP root directory, which, in the case of the local (S)FTP server, is **/home/ftpadmin**.

You can choose to use external (S)FTP servers. For the list of third party (S)FTP servers that have been verified with PSM and Juniper Networks network elements, see the *proNX Service Manager Installation and Administration Guide*.

1. From the main menu choose **Edit>FTP Servers**.
2. On the **FTP Servers** tab, right-click **Right-Click to Add a File Server**, and then click **Add File Server**.



3. In the **File Server Configuration** dialog, enter valid values in the **IP Address**, **Port**, **Username**, **Password**, and **Confirm Password** fields. For an SFTP server, select **SFTP** on the **Protocol** drop-down menu.



The (S)FTP server connection is tested. If the server is unreachable, an **Inactive** indication appears. If the server is reachable but the supplied password is incorrect, an **Invalid Credentials** indication appears, and you will not be able to add the server.

4. Specify the directory you want to use as the subdirectory by typing in the directory name or by browsing. The subdirectory path is relative to the (S)FTP root directory. The directory must already exist.

**Add File Server**

**File Server Configuration**

File Server Configuration

IP Address: 172.25.7.219 Active

Protocol: FTP Port: 21

Username: john

Password: •••••

Confirm Password: •••••

Directory: Backup Browse

Cancel OK

If the server is reachable and the password is correct but the directory is invalid, an **Invalid Directory** indication appears, and you will not be able to add the server. To add the server, you must enter or browse to a valid directory, or leave this field blank (indicating the FTP root directory).

5. Click **OK**.

The (S)FTP server is added to the list on the **FTP Servers** tab. If there are no errors when configuring the server, the Server Status should be **Active** and the Directory Status should be **Valid**.



**NOTE:** You are allowed to add the server even if the server is unreachable.

6. Repeat 2 to 5 for each FTP server to be added.

## Modifying the Configuration for an FTP or SFTP Server

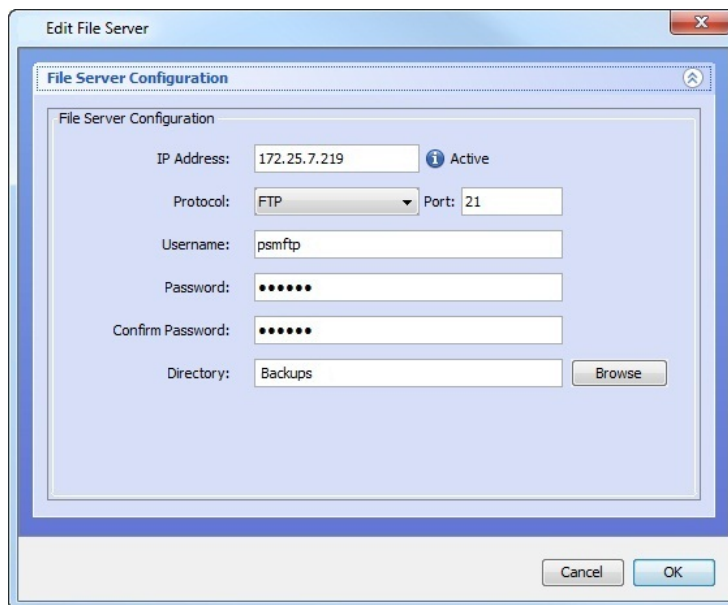
1. From the main menu choose **Edit>FTP Servers**.
2. On the **FTP Servers** tab, right-click an FTP server, and then click **Edit File Server**.

File Servers	IP Address	Port	Directory	Username	Protocol	Server Status	Directory Status
172.25.7.219:21:ftpadmin:Backup	172.25.7.219	21		ftpadmin	FTP	Active	Valid
172.25.7.219:21:ftpadmin:NeDbBackups	172.25.7.219	21		ftpadmin	FTP	Active	Valid
172.25.7.219:21:ftpadmin:NeSoftware	172.25.7.219	21		ftpadmin	FTP	Active	Valid



**NOTE:** The pre-installed server entries (<PSM server host>:ftpadmin:NeDbBackups and <PSM server host>:ftpadmin:NeSoftware) cannot be edited. If you try to edit these entries, you will receive an error and the changes do not take effect.

3. In the **File Server Configuration** dialog, modify settings as required, and then click **OK**.



The modifications are applied and the **File Server Configuration** dialog closes.

4. Repeat 2 and 3 for each FTP server configuration to be modified.

## Deleting an FTP or SFTP Server

1. From the main menu choose **Edit>FTP Servers**.
2. On the **FTP Servers** tab, right-click an FTP server, and then click **Delete File Server**.



**NOTE:** The pre-installed server entries (<PSM server host>:ftpadmin:NeDbBackups and <PSM server host>:ftpadmin:NeSoftware) cannot be deleted. If you try to delete these entries, you will receive an error and the deletion does not take effect.

3. In the confirmation dialog, click **OK**.

The FTP server is removed from the list on the **File Server Configuration** tab.

4. Repeat 2 and 3 for each FTP server to be deleted.

## Manually Backing Up a Network Element Configuration Database

Use this procedure to back up a network element configuration database.

The (S)FTP server must be set up and active prior to backing up an NE's database to it. See [“Adding an FTP or SFTP Server” on page 477](#) for information about setting up an (S)FTP server.

PSM supports network element database backup for the following:

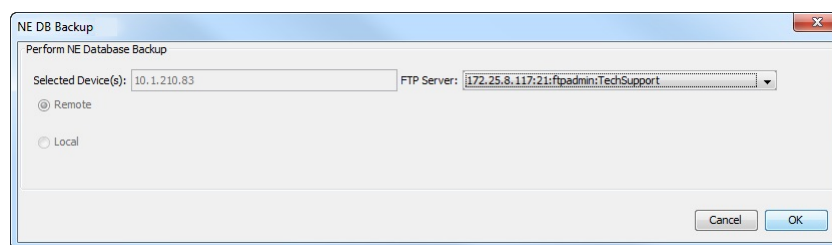
- BTI7800 Series network elements
- BTI7000 Series network elements
- BTI800 Series network elements (FTP only)
- BTI700 Series network elements (FTP only)
- MX Series and PTX Series routers (FTP only)
- QFX Series switches (FTP only)



**NOTE:** To protect network and server resources, limits are placed on the number of backups that can be run concurrently. See [“Managing Task Status” on page 537](#) for more details.

1. Right-click a network element (or select multiple NEs), and choose **Backup & Restore > NE DB Backup**.

The **NE DB Backup** dialog is displayed.



2. Select whether you want to back up the database to **Local** or **Remote** storage.

The **Local** option is only available for selection if the NE supports local storage.

3. If you choose **Remote** storage, select an active FTP server from the pulldown menu.
4. Click **OK**.

The NE's database is backed up to local storage or to the configured SFTP/FTP server. Use the **View > Server > Tasks** command to monitor the progress of the database backup task. For some network elements, this might take 15 minutes or more to complete.



**NOTE:** PSM-generated NE database backup related alarms are not automatically cleared once the problem has been resolved. You must clear PSM-generated NE database backup alarms manually. To manually clear a PSM-generated alarm, right click the alarm and choose **Clear NMS Generated Alarm**. Once cleared, you cannot restore an alarm.

---

## Restoring a Configuration Database to a Network Element

---

Use this procedure to restore a configuration database to a network element.

### Prerequisites:

The (S)FTP server must be set up and active. See [“Adding an FTP or SFTP Server” on page 477](#) for information about setting up an (S)FTP server.

PSM supports network element database restore for the following:

- BTI7800 Series network elements
- BTI7000 Series network elements
- BTI800 Series network elements (FTP only)
- BTI700 Series network elements (FTP only)
- MX Series and PTX Series routers (FTP only)
- QFX Series switches (FTP only)



**NOTE:** To protect network and server resources, limits are placed on the number of restores that can be run concurrently. See [“Managing Task Status” on page 537](#) for more details.



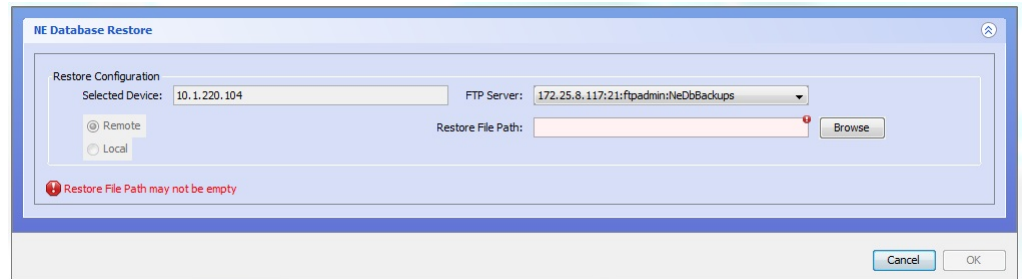
**NOTE:** For the BTI7000 Series network elements, PSM performs both the Load/Invoke and Commit phases. The NE cannot be viewed between the invoke and commit stages (to verify the data before committing the restore). To verify the data before restoring, use the proNX 900 to perform each of the individual operations.



**NOTE:** For the MX Series and PTX Series routers and QFX Series switches, PSM downloads the configuration to the router as the candidate version. PSM does not perform the commit. You have to log in to the router CLI to perform the commit.

1. Right-click a network element, and choose **Backup & Restore > NE DB Restore**.

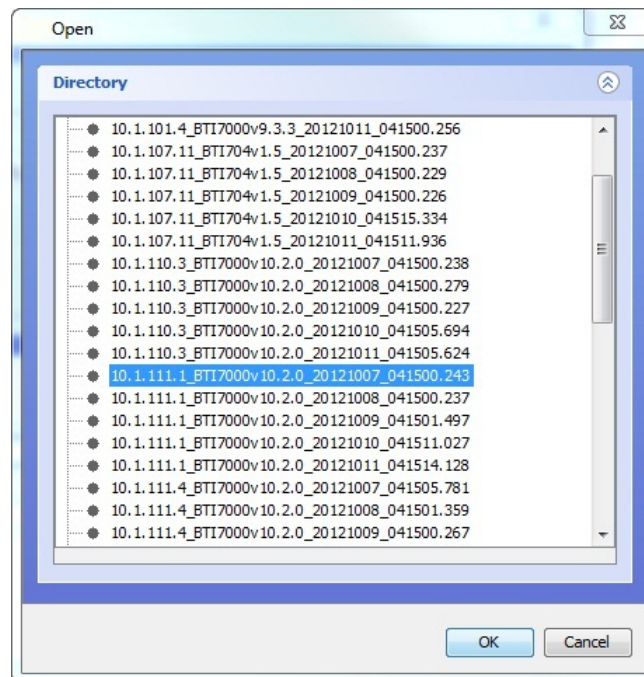
The **NE DB Restore** dialog is displayed.



2. Select whether you want to restore the database from **Local** or **Remote** storage.

The **Local** option is only available for selection if the NE supports local storage.

3. If you choose **Remote** storage, select an active FTP server and subdirectory from the pulldown menu and click **Browse** to navigate to and select the backup file from which you want to restore the database.





**NOTE:** You can only browse within the starting directory and its subdirectories. The starting directory is the directory you specified when adding the (S)FTP server.

The file you select appears in the **Restore File** field of the **NE DB Restore** dialog.

4. Click **OK**.

Use the **View > Server > Tasks** command to monitor the progress of the database restore task. For some network elements, this might take 15 minutes or more to complete.



**NOTE:** PSM-generated NE database backup related alarms are not automatically cleared once the problem has been resolved. You must clear PSM-generated NE database backup alarms manually. To manually clear a PSM-generated alarm, right click the alarm and choose **Clear NMS Generated Alarm**. Once cleared, you cannot restore an alarm.



**NOTE:** If you are using inband management communications for PSM through a BTI7000 Series NE, then you will not receive a response from the NE indicating the successful completion of the database restore.

---

## Upgrading System Software for a Network Element

---

Use this procedure to upgrade the system software for a network element.

The (S)FTP server must be selected, set up, and active prior to downloading system software to an NE. See [“Adding an FTP or SFTP Server” on page 477](#) for information about setting up an (S)FTP server.

PSM supports network element software upgrade for the following:

- BTI7800 Series network elements
- BTI7000 Series network elements
- BTI800 Series network elements (FTP only)
- BTI700 Series network elements (FTP only)



**NOTE:** A software upgrade to a previous software version is not supported.





**NOTE:** To protect network and server resources, limits are placed on the number of upgrades that can be run concurrently. See “[Managing Task Status](#)” on page 537 for more details.

1. Right-click a network element in the Network tree view, and then click **Software Upgrade**.

The **Software Upgrade** dialog is displayed.

The **Software Upgrade** dialog box is shown. It has a title bar with a close button. The main area is divided into sections. The **Version** section contains three text boxes: **Selected Device:** 10.1.220.4, **Current Software Version:** 10.4.0 C007, and **Inactive Software Version:** 11.1.0 BRCH 23. To the right, there is an **FTP Server:** dropdown menu showing 172.25.7.219:21:ftpadmin:NeSoftware, a **Software:** text box with a red error icon, and a **Browse** button. Below these is a **Software Selection:** section with three bullet points: "- For 7000 select a directory.", "- For 7xx/810 select compressed file.", and "- For 7800 select RPM file." At the bottom, there is an **Option** section with five checkboxes: ☒ Check, ☐ Load, ☐ Invoke, ☐ Commit, and ☐ Cancel. A red error message "Software may not be empty" is displayed at the bottom left. At the bottom right are **Cancel** and **OK** buttons.

Alternatively, select multiple NEs, right-click and choose **Software Upgrade**. In this case the following dialog is displayed. If a combination of mixed NE types are selected then the **Select Device** pulldown contains the various NE types available for upgrade, and you must select a single NE type to upgrade.

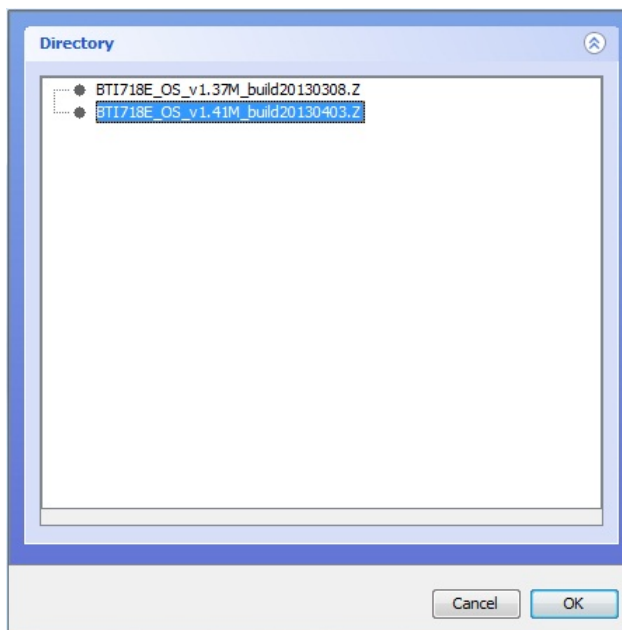


**NOTE:** Exercise caution when upgrading multiple NEs concurrently. This feature has been provided for convenience and should only be used after you have performed a limited rollout of the new software and resolved any deployment issues.

The **Software Upgrade** dialog box is shown. It has a title bar with a close button. The main area is divided into sections. The **Version** section contains three text boxes: **Selected Device:** BTI-718E (dropdown), **Current Software Version:** 2.0, and **Inactive Software Version:** N/A. To the right, there is an **FTP Server:** dropdown menu showing 172.25.7.219:21:ftpadmin:NeSoftware, a **Software:** text box with a red error icon, and a **Browse** button. Below these is a **Software Selection:** section with three bullet points: "- For 7000 select a directory.", "- For 7xx/810 select compressed file.", and "- For 7800 select RPM file." At the bottom, there is an **Option** section with four checkboxes: ☐ Check, ☒ Load, ☐ Invoke, and ☐ Commit. A red error message "Software may not be empty" is displayed at the bottom left. At the bottom right are **Cancel** and **OK** buttons.

2. In the **Software Upgrade** dialog, select an active FTP server from the pulldown menu.

3. Click **Browse** to navigate to and select the software version that you want to download. For BTI7000 Series software, select the directory of the release. For BTI700 Series and BTI800 Series software, select the compressed file with the correct device type and extension.



**NOTE:** You can only browse within the starting directory and its subdirectories. The starting directory is the directory you specified when adding the (S)FTP server.

The version you selected appears in the **Software** field of the **Software Upgrade** dialog.

4. For BTI7000 Series devices, select one or more check boxes as desired. Only valid combinations are allowed to be selected. The general sequence is to check, load, invoke, and then commit the upgrade. You can choose to perform all of this in one step or in multiple steps at different times.
  - **Check** - This selection verifies that the system is ready for the upgrade process, and that the load files on the server are accessible.
  - **Load** - This selection downloads the software images from the server to the SCP.
  - **Invoke** - This selection installs the new load on all circuit packs in the system and reboots each card in the system.



**NOTE:** If you are using inband management communications for PSM through a BT17000 Series NE, then you will not receive a response from the NE indicating success when performing the **Invoke** phase of a software upgrade. In this case the upgrade process can be completed by using the proNX 900.

- **Commit** - This selection completes the upgrade procedure, and can only be performed after an **Invoke** has taken place, either in a previous step, or with **Invoke** concurrently selected with **Commit**.
- **Cancel** - This selection cancels the upgrade procedure and rolls the system back to the previous set of loads. It can only be selected after an **Invoke** has taken place previously and prior to a **Commit**.

For BT1700 Series and BT1800 Series devices, select the desired check boxes:

- **Load** - This selection downloads the software image from the server.
- **Commit** - This selection activates the new image.

PSM attempts to validate the BT1700 Series file using the selected filename. If the filename does not indicate a BT1700 Series-specific device, a warning is displayed.

5. Click **OK**.

Use the **Tasks** tab in the main window to monitor the progress of the software upgrade.



**NOTE:** PSM-generated NE software upgrade related alarms are not automatically cleared once the problem has been resolved. Any PSM-generated NE software upgrade alarms that occur must be manually cleared. To manually clear a PSM-generated alarm, right-click on the alarm and choose **Clear NMS Generated Alarm**. Once cleared, you cannot restore an alarm.

## Restoring a Database to Factory Defaults on a BT17800 Network Element

Use this procedure to restore the configuration database back to factory defaults on a BT17800 network element.

1. Right click a network element in the Network tree or in the Topology Map view and select **Node >Database >Factory Restore**.
2. Click **OK** in the confirmation dialog.

The factory database is restored on the selected network element.



## CHAPTER 17

# Managing Reports

- [Generating Alarms Reports on page 489](#)
- [Generating Ethernet Reports on page 493](#)
- [Generating Pseudowire Reports on page 494](#)
- [Generating Transport Reports on page 495](#)
- [Generating NE Logs Reports on page 496](#)
- [Generating Optical Reports on page 498](#)
- [Generating Inventory Reports on page 499](#)
- [Generating Task History Reports on page 501](#)
- [Changing the Report Generation Timeout on page 504](#)

### Generating Alarms Reports

---

PSM supports alarm report generation for the following:

- BTI7800 Series network elements
- BTI7000 Series network elements
- BTI800 Series network elements
- BTI700 Series network elements
- MX Series and PTX Series routers
- QFX Series switches
- [Generating an Active Alarms Report on page 489](#)
- [Generating a Historical Alarms Report on page 490](#)

### Generating an Active Alarms Report

Use this procedure to generate an active alarms report in spreadsheet format, and save it to the local drive.

1. From the main menu, choose **Tools > Reports > Alarms > Active**.
2. Wait while the report generates. The bottom of the GUI shows "Requesting Report:" followed by the selected report type.



**NOTE:** If the report fails to generate, see if [“Changing the Report Generation Timeout” on page 504](#) applies to your situation.

3. When the report has been generated, the tool automatically launches your web browser and points it to the location of the report (report URL) on the PSM Server. Log in using your PSM user name and password.



**NOTE:** The report is stored indefinitely on the server at the location specified by the report URL, and is accessible from any browser. To prevent unauthorized access to this possibly sensitive data, the report location is password protected. If you have generated reports previously, your web browser might have cached your user name and password, and might log in automatically for you.



**NOTE:** Your browser might require you to explicitly verify and accept the server certificate before you can have access to the report. This is normal because communication between the browser and the server is through HTTPS.

After logging in, a file download dialog box opens.

4. Open or save the report.

The following is an example of an Active Alarms report:

	A	B	C	D	E	F
1	Report Type:	<b>Active Alarms</b>				
2	Date Collected:	Oct 28, 2013 2:06 PM				
3	ID	Description	Address	Source	Identifier	Time Raised
4	18797	Link down	10.1.107.2	GigE/1		2013-06-23 22:40:29
5	48560	Circuit pack missing	10.1.203.1	SLOT-1-7		2013-07-30 13:50:41
6	48561	Circuit pack missing	10.1.203.1	SLOT-1-12		2013-07-30 13:14:56
7	48562	Circuit pack missing	10.1.203.1	SLOT-1-14		2013-07-30 13:14:56
8	48563	System upgrade in progress	10.1.203.1	SCP-1-1		2013-07-30 13:18:33
9	214717	Circuit pack missing	10.1.203.1	SLOT-1-15		2013-10-11 09:32:23
10	215003	Circuit pack missing	10.1.203.1	SLOT-1-16		2013-10-11 13:55:09
11	224441	Link down	10.1.204.14	GigE/5		2013-10-19 17:42:05

## Generating a Historical Alarms Report

Use this procedure to generate a historical alarms report in spreadsheet format, and save it to the local drive.

1. From the main menu, choose **Tools > Reports > Alarms > Historical**.

The **Historical Alarms Report** dialog appears:

**Historical Alarms Report**

Description Contains:

Device Address Starts With:

Source Contains:

Raised Time After:  ▼

Before:  ▼

Cleared Time After:  ▼

Before:  ▼

Severity:   
 Critical  
 Major  
 Minor  
 None

Service Affecting:  ▼

Acknowledged:  ▼

Assigned User Contains:

System Name Contains:

Domain Name Contains:

Cancel Run

2. Specify the alarms you want to include in the report.
  - **Description Contains** Include alarms with the specified text string in the alarm description.
  - **Device Address Starts With** Include alarms raised by a node with the specified IP address prefix.
  - **Source Contains** Include alarms with the specified text string in the source description.
  - **Raised Time After** Include alarms raised after the specified time.
  - **(Raised Time) Before** Include alarms raised prior to the specified time.

- **Cleared Time After** Include alarms cleared after the specified time.
  - **(Cleared Time) Before** Include alarms cleared prior to the specified time.
  - **Severity** Include alarms at the indicated alarm severity. If no severity is selected, alarms at all severities are included.
  - **Service Affecting** Include alarms that are service affecting, non-service affecting, or either.
  - **Acknowledged** Include alarms that are acknowledged, unacknowledged, or either.
  - **Assigned User Contains** Include alarms with the specified text string in the user assignment.
  - **System Name Contains** Include alarms with the specified text string in the system name.
  - **Domain Name Contains** Include alarms with the specified text string in the domain name.
3. Click **Run** to generate the report based on the filters you specify.
  4. Wait while the report generates. The bottom of the GUI shows "Requesting Report:" followed by the selected report type.



**NOTE:** If the report fails to generate, see if [“Changing the Report Generation Timeout”](#) on page 504 applies to your situation.

5. When the report has been generated, the tool automatically launches your web browser and points it to the location of the report (report URL) on the PSM Server. Log in using your PSM user name and password.



**NOTE:** The report is stored indefinitely on the server at the location specified by the report URL, and is accessible from any browser. To prevent unauthorized access to this possibly sensitive data, the report location is password protected. If you have generated reports previously, your web browser might have cached your user name and password, and might log in automatically for you.



**NOTE:** Your browser might require you to explicitly verify and accept the server certificate before you can have access to the report. This is normal because communication between the browser and the server is through HTTPS.

After logging in, a file download dialog box opens.

6. Open or save the report.



The following is an example of a Historical Alarms report:

	A	B	C	D	E
1	Report Type:	<b>Historical Alarms</b>			
2	Date Collected:	2015-09-24 3:40 PM			
3					
	IP Address	Description	Source	Identifier	Time Raised
4					
5	10.1.204.13	Approximate data transfer rate writing to /backups/pms (12 MB/sec) is lower than	PSM Server Storage Det		2015-07-17 14:20:48
6	10.1.204.13	Approximate data transfer rate writing to /backups/pms (12 MB/sec) is lower than	PSM Server Storage Det		2015-08-04 14:27:18
7	10.1.204.13	Approximate data transfer rate writing to /backups/pms (12 MB/sec) is lower than	PSM Server Storage Det		2015-08-04 14:27:34
8	10.1.204.13	Client -> Server latency (3565) higher than maximum (1200.0).	Client at 10.64.8.14		2015-08-05 13:31:41
9	10.1.204.13	Client -> Server latency (4369) higher than maximum (1200.0).	Client at 10.64.8.14		2015-08-05 13:46:18
10	10.1.204.13	Approximate data transfer rate writing to /backups/pms (12 MB/sec) is lower than	PSM Server Storage Det		2015-08-05 13:50:04
11	10.1.204.13	Approximate data transfer rate writing to /backups/pms (11 MB/sec) is lower than	PSM Server Storage Det		2015-08-05 13:50:34
12	10.1.204.13	Client -> Server latency (3698) higher than maximum (1200.0).	Client at 10.64.8.14		2015-08-05 18:36:18
13	10.1.204.13	Approximate data transfer rate writing to /backups/pms (14 MB/sec) is lower than	PSM Server Storage Det		2015-08-05 18:39:37
14	10.1.204.13	Approximate data transfer rate writing to /backups/pms (14 MB/sec) is lower than	PSM Server Storage Det		2015-08-05 18:40:12
15	10.1.204.13	Client -> Server latency (1436) higher than maximum (1200.0).	Client at 10.64.8.14		2015-08-05 20:01:47
16	10.1.204.13	Client -> Server latency (4691) higher than maximum (1200.0).	Client at 10.64.8.14		2015-08-05 20:02:18
17	10.1.204.13	Approximate data transfer rate writing to /backups/pms (21 MB/sec) is lower than	PSM Server Storage Det		2015-08-05 20:04:22
18	10.1.204.13	Approximate data transfer rate writing to /backups/pms (15 MB/sec) is lower than	PSM Server Storage Det		2015-08-05 20:05:50
19	10.1.204.13	Client -> Server latency (4554) higher than maximum (1200.0).	Client at 10.64.8.14		2015-08-05 20:27:51
20	10.1.204.13	Approximate data transfer rate writing to /backups/pms (12 MB/sec) is lower than	PSM Server Storage Det		2015-08-05 20:31:31
21	10.1.204.13	Approximate data transfer rate writing to /backups/pms (12 MB/sec) is lower than	PSM Server Storage Det		2015-08-05 20:32:06
22	10.1.204.13	Client -> Server latency (1991) higher than maximum (1200.0).	Client at 10.64.8.14		2015-08-05 20:49:06
23	10.1.204.13	Approximate data transfer rate writing to /backups/pms (12 MB/sec) is lower than	PSM Server Storage Det		2015-08-05 20:53:28

## Generating Ethernet Reports

Ethernet report generation is supported for the BTI7000 Series, BTI700 Series (excluding BTI718E), and BTI800 Series devices.

The proNX Service Manager allows the user to generate Ethernet reports in spreadsheet format, and save them to their local drive.

1. From the main menu, choose **Tools >Reports >Ethernet** and select either **Network Elements** or **Services**.
2. Wait while the report generates. The bottom of the GUI shows "Requesting Report:" followed by the selected report type.



**NOTE:** If the report fails to generate, see if ["Changing the Report Generation Timeout"](#) on page 504 applies to your situation.

3. When the report has been generated, the tool automatically launches your web browser and points it to the location of the report (report URL) on the PSM Server. Log in using your PSM user name and password.



**NOTE:** The report is stored indefinitely on the server at the location specified by the report URL, and is accessible from any browser. To prevent unauthorized access to this possibly sensitive data, the report location is password protected. If you have generated reports previously, your web browser might have cached your user name and password, and might log in automatically for you.



**NOTE:** Your browser might require you to explicitly verify and accept the server certificate before you can have access to the report. This is normal because communication between the browser and the server is through HTTPS.

After logging in, a file download dialog box opens.

4. Open or save the report.

The following is an example of an Ethernet Services report.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	Report Type:	<b>Ethernet Services</b>												
2	Date Collected:	Oct 24, 2013 4:16 PM												
3	Management Domain	Customer	Service Name	Service Type	Service State	SVLAN	Critical	Major	Minor	Acked	IP Address (System Name)		Port	
4	Default		VzW_CCT_345678A	evplane	up	1010	0	0	0	0	10.10.20.201 (Chicago)		NNI 1:1:3:GIGE:10	
5	Default		VzW_CCT_345678A	evplane	up	1010	0	0	0	0	10.10.20.201 (Chicago)		UNI 1:1:3:GIGE:7	
6	Default		VzW_CCT_345678A	evplane	up	1010	0	0	0	0	10.10.20.201 (Chicago)		NNI 1:1:3:GIGE:1	
7	Default		VzW_CCT_345678A	evplane	up	1010	0	0	0	0	10.10.20.201 (Chicago)		NNI 1:1:3:GIGE:2	
8	Default		VzW_CCT_345678A	evplane	up	1010	0	0	0	0	10.10.20.201 (Chicago)		NNI 2:1:1:GIGE:10	

## Generating Pseudowire Reports

Pseudowire report generation is supported for the BT1810 devices.

The proNX Service Manager allows the user to generate pseudowire reports in spreadsheet format, and save them to the local drive.

1. From the main menu, choose **Tools > Reports > Ethernet > Pseudowire**.
2. Wait while the report generates. The bottom of the GUI shows "Requesting Report:" followed by the selected report type.



**NOTE:** If the report fails to generate, see if "[Changing the Report Generation Timeout](#)" on page 504 applies to your situation.

3. When the report has been generated, the tool automatically launches your web browser and points it to the location of the report (report URL) on the PSM Server. Log in using your PSM user name and password.



**NOTE:** The report is stored indefinitely on the server at the location specified by the report URL, and is accessible from any browser. To prevent unauthorized access to this possibly sensitive data, the report location is password protected. If you have generated reports previously, your web browser might have cached your user name and password, and might log in automatically for you.



**NOTE:** Your browser might require you to explicitly verify and accept the server certificate before you can have access to the report. This is normal because communication between the browser and the server is through HTTPS.

After logging in, a file download dialog box opens.

4. Open or save the report.

The following is an example of a Pseudowire report.

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Report Type:			Pseudowire									
2	Date Collected:			Dec 11, 2013 10:39 PM									
3	Pseudowire												
	Service ID	Service Name	ECID	Customer	Domain	Ethernet Service Name	Ethernet SVLAN	Ethernet Service State	NE Name		NE IP	NE Slot	
4	10.1.210.52: 1:1:TIMESLOT:Default::	JAMES_PW_2	2		Default	PW_SERVICE_SLOT1	200	up	RICHARDSON		10.1.210.52	1	
5	10.1.210.52: 1:2:TIMESLOT:Default::	TEST123	3		Default	PW_SERVICE_SLOT1_2	210	up	RICHARDSON		10.1.210.52	1	

## Generating Transport Reports

Transport report generation is supported for transport services on a BTI7800 network and for transport services with BTI7800, MX Series, PTX Series, or QFX Series endpoints over a BTI7000 optical network.

The proNX Service Manager allows the user to generate transport reports in spreadsheet format, and save them to their local drive. There are four transport report types available: Transport Services, Transport Services per Span, Transport Topology, and Transport Cross-Connects.

1. From the main menu, choose **Tools > Reports > Transport** and one of **Services**, **Cross-Connects**, **Services per Span**, **Topology**.
2. Wait while the report generates. The bottom of the GUI shows "Requesting Report:" followed by the selected report type.



**NOTE:** If the report fails to generate, see if "[Changing the Report Generation Timeout](#)" on page 504 applies to your situation.

3. When the report has been generated, the tool automatically launches your web browser and points it to the location of the report (report URL) on the PSM Server. Log in using your PSM user name and password.



**NOTE:** The report is stored indefinitely on the server at the location specified by the report URL, and is accessible from any browser. To prevent unauthorized access to this possibly sensitive data, the report location is password protected. If you have generated reports previously, your web browser might have cached your user name and password, and might log in automatically for you.



**NOTE:** Your browser might require you to explicitly verify and accept the server certificate before you can have access to the report. This is normal because communication between the browser and the server is through HTTPS.

After logging in, a file download dialog box opens.

4. Open or save the report.

The following is an example of a Transport Services report.

	A	C	E	F	G	H	I
1	Report Type:	Transport Services					
2	Date Collected:	October 1, 2014 10:01:26 AM					
	Customer	Service	Site A	Site A IP	Site A Port	Site Z	Site Z IP
3							
4				10.1.220.104	10ge:1/2/1/5		10.1.220.104
5				10.1.220.104	10ge:1/8/1/1		10.1.220.104
6				10.1.220.104	10ge:1/8/1/1		10.1.220.104
7				10.1.220.104	10ge:1/8/1/2		10.1.220.104
8				10.1.220.104	10ge:1/8/1/3		10.1.220.104
9				10.1.220.104	10ge:1/8/1/4		10.1.220.104

## Generating NE Logs Reports

The proNX Service Manager allows the user to generate NE logs reports in spreadsheet format, and save them to their local drive.

PSM supports NE log report generation for the following:

- BTI7800 Series network elements
- BTI7000 Series network elements
- MX Series and PTX Series routers
- QFX Series switches

1. From the main menu, choose **Tools>Reports>NE Logs**.

The Network Elements Logs Report window is displayed.

2. Using the options in the Network Elements Logs Report window, specify the attributes of the report. The bottom of the GUI shows "Requesting Report:" followed by the selected report type.
3. **Click Run.**
4. Wait while the report generates. The bottom of the GUI shows "Requesting Report:" followed by the selected report type.



**NOTE:** If the report fails to generate, see if [“Changing the Report Generation Timeout”](#) on page 504 applies to your situation.

- When the report has been generated, the tool automatically launches your web browser and points it to the location of the report (report URL) on the PSM Server. Log in using your PSM Client user name and password.



**NOTE:** The report is stored indefinitely on the server at the location specified by the report URL, and is accessible from any browser. To prevent unauthorized access to this possibly sensitive data, the report location is password protected. If you have generated reports previously, your web browser might have cached your user name and password, and might log in automatically for you.



**NOTE:** Your browser might require you to explicitly verify and accept the server certificate before you can have access to the report. This is normal because communication between the browser and the server is through HTTPS.

- A file download dialog box opens asking "Do you want to open or save this file?". Click **Save as**.
- Choose where to save the report on your local drive, then click **Save** to download the file.

The following image is an example of an NE Logs report file.

	A	B	C	D	E	F
1	Report Type:	<b>Network Element Logs</b>				
2	Date Collected:	Oct 28, 2013 2:38 PM				
3						
4	ID	Message	IP Address	System Name	Time Logged	
5	133634	User 'admin': RTRV-NETTYPE:FRKTWN2043:166	10.1.204.3	FRKTWN2043	2012-09-24 15:13:56	
6	133636	User 'admin': RTRV-NETTYPE:FRKTWN2043:172	10.1.204.3	FRKTWN2043	2012-09-24 15:15:36	
7	133641	User 'admin': RTRV-SYS:FRKTWN2043:102	10.1.204.3	FRKTWN2043	2012-09-27 10:33:30	
8	133642	User 'admin': RTRV-NETTYPE:FRKTWN2043:103	10.1.204.3	FRKTWN2043	2012-09-27 10:33:30	
9	133643	User 'admin': RTRV-DB-RST:FRKTWN2043:104	10.1.204.3	FRKTWN2043	2012-09-27 10:33:30	
10	133644	User 'admin': RTRV-SYS-RELNUM:FRKTWN2043:105	10.1.204.3	FRKTWN2043	2012-09-27 10:33:30	
11	133645	User 'admin': RTRV-SER:FRKTWN2043:ALL:106	10.1.204.3	FRKTWN2043	2012-09-27 10:33:30	
12	133646	User 'admin': RTRV-INV:FRKTWN2043:ALL:107	10.1.204.3	FRKTWN2043	2012-09-27 10:33:30	
13	133647	User 'admin': RTRV-EQPT:FRKTWN2043:ALL:108	10.1.204.3	FRKTWN2043	2012-09-27 10:33:39	

## Generating Optical Reports

Optical report generation is supported for the BTI7000 Series and BTI7800 Series network elements.

The proNX Service Manager allows the user to generate optical reports in spreadsheet format, and save them to their local drive. There are four optical report types available: Optical Services, Optical Services per Span, Optical Topology, and Optical Cross-Connects.

1. From the main menu, choose **Tools > Reports > Optical** and one of **Services, Topology, Cross-Connects, Services per Span**.
2. Wait while the report generates. The bottom of the GUI shows "Requesting Report:" followed by the selected report type.



**NOTE:** If the report fails to generate, see if [“Changing the Report Generation Timeout” on page 504](#) applies to your situation.

3. When the report has been generated, the tool automatically launches your web browser and points it to the location of the report (report URL) on the PSM Server. Log in using your PSM user name and password.



**NOTE:** The report is stored indefinitely on the server at the location specified by the report URL, and is accessible from any browser. To prevent unauthorized access to this possibly sensitive data, the report location is password protected. If you have generated reports previously, your web browser might have cached your user name and password, and might log in automatically for you.



**NOTE:** Your browser might require you to explicitly verify and accept the server certificate before you can have access to the report. This is normal because communication between the browser and the server is through HTTPS.

After logging in, a file download dialog box opens.

4. Open or save the report.

The following is an example of an Optical Topology report.

	A	B	C	D	E	F	G	H	I
1	Report Type:	Optical Topology							
2	Date Collected:	October 28, 2013 1:50:47 PM							
	Source Site Name	Source Site IP		Source Group-Degree	Source Port	Far End Site Name	Far End Site IP	Far-End Group-Degree	
3									
4	Miami	10.10.20.99		G1-D1	ROB-1-7-L1	Dallas	10.1.213.1	G1-D2	
5	Dallas	10.1.213.1		G1-D2	ROB-1-15-L1	Miami	10.10.20.99	G1-D1	
6									
7									

## Generating Inventory Reports

The proNX Service Manager allows the user to generate inventory reports in spreadsheet format, and save them to their local drive. The inventory report contains the same information as in the network element inventory view (see [“Viewing Network Element Inventory Information” on page 97](#)).

PSM supports inventory report generation for the following:

- BTI7800 Series network elements
- BTI7000 Series network elements
- BTI800 Series network elements
- BTI700 Series network elements
- MX Series and PTX Series routers
- QFX Series switches

1. From the main menu, choose **Tools>Reports>Inventory**.
2. Wait while the report generates. The bottom of the GUI shows "Requesting Report:" followed by the selected report type.



**NOTE:** If the report fails to generate, see if [“Changing the Report Generation Timeout” on page 504](#) applies to your situation.

3. When the report has been generated, the tool automatically launches your web browser and points it to the location of the report (report URL) on the PSM Server. Log in using your PSM user name and password.



**NOTE:** The report is stored indefinitely on the server at the location specified by the report URL, and is accessible from any browser. To prevent unauthorized access to this possibly sensitive data, the report location is password protected. If you have generated reports previously, your web browser might have cached your user name and password, and might log in automatically for you.



**NOTE:** Your browser might require you to explicitly verify and accept the server certificate before you can have access to the report. This is normal because communication between the browser and the server is through HTTPS.

After logging in, a file download dialog box opens.

4. Open or save the report.

The following is an example of an Inventory report.



	A	B	C	D	E	F	G
1	Report Type:	<b>Inventory Report</b>					
2	Date Collected:	<b>Oct 28, 2013 2:12 PM</b>					
3	Address	System Name	System Location	System Contact	Version	Row Type	AID
4	10.1.212.1	NewYork	NYC	UNKNOWN	10.3.5 C004	Shelf	MS-1
5	10.1.212.1	NewYork	NYC	UNKNOWN	10.3.5 C004	Pack	CU-1-1
6	10.1.212.1	NewYork	NYC	UNKNOWN	10.3.5 C004	Pack	CU-1-2
7	10.1.212.1	NewYork	NYC	UNKNOWN	10.3.5 C004	Pack	CU-1-3
8	10.1.212.1	NewYork	NYC	UNKNOWN	10.3.5 C004	Pack	CU-1-4
9	10.1.212.1	NewYork	NYC	UNKNOWN	10.3.5 C004	Pack	SLOT-1-1
10	10.1.212.1	NewYork	NYC	UNKNOWN	10.3.5 C004	Pack	SLOT-1-3

## Generating Task History Reports

The proNX Service Manager allows the user to generate task history reports in spreadsheet format, and save them to their local drive. The task history shows a record of tasks performed by users as well as scheduled tasks by the system.

PSM supports task history report generation for the following:

- BTI7800 Series network elements
- BTI7000 Series network elements
- BTI800 Series network elements
- BTI700 Series network elements

1. From the main menu, choose **Tools > Reports > Task History**.

The **Task History Report** window is displayed.

**Task History Report**

**Task History Criteria**

Network Element:

Task Type:

Username:

Start Time:  ▼

End Time:  ▼

Running a report with empty search fields will return ALL tasks.

Cancel Run

2. Select the task history filtering criteria as follows:

- **Network Element:** Specify the IP address or IP address prefix of the network element(s) that you want to be included in the task history report. The address is in standard dotted decimal notation. By specifying a prefix, you can include a set of prefixes. For example, **10.1.** returns all network elements within the address range **10.1.0.0** to **10.1.255.255**. A **10.1.210.71** address returns the **10.1.210.71** network element as well as network elements in the address range **10.1.210.710** to **10.1.210.719**.
- **Task Type:** Specify the task type of the tasks you want to be included in the task history report. When you type in the box, a drop-down menu appears that shows the task types that match what you have typed so far. The matches are based on a simple unanchored pattern match of the typed string against the set of supported PSM task types. In other words, all matching task types contain the typed string. You can choose a specific task type from the drop-down menu, or keep typing to narrow down your selections further, or simply keep the string that you have typed so far to include all current task types in the drop-down menu.
- **Username:** Specify the user you want to be included in the task history report. When you type in the box, a drop-down menu appears that shows the user names that match what you have typed so far. The matches are based on a simple unanchored pattern match of the typed string against the set of PSM users. In other words, all matching user names contain the typed string. You can choose a specific user from the drop-down menu, or keep typing to narrow down your selections further, or simply keep the string that you have typed so far to include all current user names in the drop-down menu.
- **Start Time:** Specify the start time of the report period.
- **End Time:** Specify the end time of the report period.



**NOTE:** If you leave any box blank, then no filter is applied for the associated criterion.

3. **Click Run.**
4. Wait while the report generates. The bottom of the GUI shows "Requesting Report:" followed by the selected report type.



**NOTE:** If the report fails to generate, see if "[Changing the Report Generation Timeout](#)" on [page 504](#) applies to your situation.

5. When the report has been generated, the tool automatically launches your web browser and points it to the location of the report (report URL) on the PSM Server. Log in using your PSM user name and password.



**NOTE:** The report is stored indefinitely on the server at the location specified by the report URL, and is accessible from any browser. To prevent unauthorized access to this possibly sensitive data, the report location is password protected. If you have generated reports previously, your web browser might have cached your user name and password, and might log in automatically for you.



**NOTE:** Your browser might require you to explicitly verify and accept the server certificate before you can have access to the report. This is normal because communication between the browser and the server is through HTTPS.

After logging in, a file download dialog box opens.

#### 6. Open or save the report.

The following is an example of a Task History report.

	A	B	C	D	E	F	G	H
1	Report Type: Task History							
2								
3	Date Collected: 2015-11-30 15:32:28							
4								
5								
6	Task ID	Parent Task ID	IP Address	User	Type	State	Detailed State	Start Time
7	15702718		10.1.207.1	system	NE_DISCOVERY	SUCCESS	OK:success	11/30/2015 11:44
8	15702719		10.10.20.99	system	NE_DISCOVERY	SUCCESS	OK:success	11/30/2015 11:44
9	15702720		10.1.207.3	system	NE_DISCOVERY	SUCCESS	OK:success	11/30/2015 11:44
10	15702721		10.1.210.81	system	NE_DISCOVERY	SUCCESS	OK:failed-Walk terminated [Walk timed out]	11/30/2015 11:44
11	15702722		10.1.210.70-7	admin	NE_DISCOVERY	SUCCESS	OK:SUCCESS	11/30/2015 11:46
12	15702724	15702722			NE_DISCOVERY	SUCCESS	OK:failed-Failed to get System Object Id from device [10.1.210.70] [No response from device. Please confirm that the device is running normally and verify the SNMP community strings.]	11/30/2015 11:46
13	15702725	15702722			NE_DISCOVERY	SUCCESS	OK:failed-Failed to get System Object Id from device [10.1.210.71] [No response from device. Please confirm that the device is running normally and verify the SNMP community strings.]	11/30/2015 11:46
14	15702728		10.1.204.3	system	NE_DISCOVERY	SUCCESS	OK:success	11/30/2015 11:46
15	15702729		10.10.20.203	system	NE_DISCOVERY	SUCCESS	OK:success	11/30/2015 11:46
16	15702730		10.10.20.202	system	NE_DISCOVERY	SUCCESS	OK:success	11/30/2015 11:46
17	15702731		10.127.45.90	system	NE_DISCOVERY	SUCCESS	OK:success	11/30/2015 11:46

## Changing the Report Generation Timeout

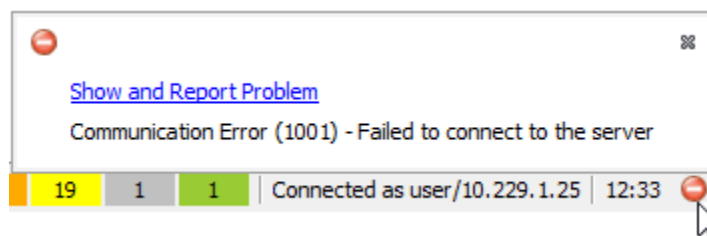
Use this procedure to change the time that the PSM client waits for the PSM server to finish generating a report.

Report generation might require the PSM server to collect information from all network elements in the network. This might take some time, especially in slow networks. If the PSM client times out while waiting for report generation to complete, you can adjust the PSM client timeout value to be more appropriate for your network.

You do not need to change the timeout value if report generation works for your network.

When report generation fails due to a timeout, you will see an error icon in the lower right corner of the PSM client window. If you click on the error icon, you will see the following generic error indicating PSM client-server communication problems:

Figure 93: PSM Client Communication Timeout



The parameter that dictates how long the PSM client waits for the report is found on the PSM client machine.

1. Locate the **ems.properties** file in the *<PSM\_client\_installation\_folder>/psmclient* folder.
2. Open the **ems.properties** file using a text editing application such as WordPad and change the **ems.client.reports.socket.timeout** parameter. The units are in milliseconds.

For example, this sets the timeout to 900000 milliseconds or 15 minutes:

```
ems.client.reports.socket.timeout = 900000
```



**NOTE:** If you installed the PSM client using the supplied installer, you might need to edit this file as an administrator. In Windows 10, click on the Start menu and go to All apps>Windows Accessories and scroll down to WordPad, right-click and select More>Run as administrator. Then open the **ems.properties** file from within the WordPad application.

3. Save and close the **ems.properties** file.



.....

**NOTE:** The updated setting takes effect the next time you launch the PSM client.

.....

4. Close and relaunch the PSM client.



## CHAPTER 18

# Performance Monitoring

- [Viewing Current Port, Interface, and Channel PMs on page 507](#)
- [Viewing Real-time Optical Service PMs on page 507](#)
- [Viewing Real-time Transport Service PMs on page 515](#)
- [Viewing Real-time Ethernet PMs and SLAs on page 520](#)
- [Viewing Real-time Pseudowire PMs on page 528](#)
- [Collecting and Viewing Historical PMs on page 531](#)

### Viewing Current Port, Interface, and Channel PMs

To view current port, interface, and channel PMs, follow the applicable procedures in the Nodal Management chapter:

- [Viewing Port PMs on a BTI7000 Series Network Element on page 166](#)
- [Viewing Interface PMs on a UFM on page 215](#)
- [Viewing Port PMs on a ROADM Element on page 238](#)
- [Viewing OMS PMs on a ROADM Element on page 239](#)
- [Viewing OSC PMs on a ROADM Element on page 240](#)
- [Viewing Optical Channel PMs on a ROADM Element on page 240](#)
- [Viewing Port PMs on a 96-Channel Amplifier on page 251](#)
- [Viewing Interface PMs on an MX Series or PTX Series Router or QFX Series Switch on page 263](#)

### Viewing Real-time Optical Service PMs

Use this procedure to enable and view real-time PMs for optical services on BTI7000 Series and BTI7800 Series network elements. The PMs are displayed in both textual and graphical formats.

PSM supports the following BTI7000 Series optical service PMs:

Table 55: BT17000 Series Optical Service PMs

Description	Port PMs	OSC PMs	Service Channel PMs
Instantaneous optical power received	Yes	No	No
Minimum optical power received	Yes	No	No
Maximum optical power received	Yes	No	No
Average optical power received	Yes	No	No
Optical power loss received	Yes	No	No
Standard deviation power received	Yes	No	No
Instantaneous optical power transmitted	Yes	No	No
Minimum optical power transmitted	Yes	No	No
Maximum optical power transmitted	Yes	No	No
Average optical power transmitted	Yes	No	No
Optical power loss transmitted	Yes	No	No
Standard deviation power transmitted	Yes	No	No
OSC optical power received	No	Yes	No
OSC optical power transmitted	No	Yes	No
Code violations	No	Yes	No
Errored seconds	No	Yes	No
OSC optical back-reflected power	No	Yes	No
Severely errored framing seconds	No	Yes	No
Severely errored seconds	No	Yes	No
Unavailable seconds	No	Yes	No
Instantaneous channel power received	No	No	Yes
Minimum channel power received	No	No	Yes
Maximum channel power received	No	No	Yes
Instantaneous channel power transmitted	No	No	Yes



Table 55: BTI7000 Series Optical Service PMs (continued)

Description	Port PMs	OSC PMs	Service Channel PMs
Minimum channel power transmitted	No	No	Yes
Maximum channel power transmitted	No	No	Yes

PSM supports the following BTI7800 Series optical PMs:

Table 56: BTI7800 Series Optical Service PMs

Description	Port PMs	OMS PMs	OSC PMs	Service Channel PMs
Instantaneous optical power received	Yes	Yes	No	No
Minimum optical power received	Yes	Yes	No	No
Maximum optical power received	Yes	Yes	No	No
Average optical power received	Yes	Yes	No	No
Standard deviation power received	Yes	No	No	No
Instantaneous optical power transmitted	Yes	Yes	No	No
Minimum optical power transmitted	Yes	Yes	No	No
Maximum optical power transmitted	Yes	Yes	No	No
Average optical power transmitted	Yes	Yes	No	No
Standard deviation power transmitted	Yes	No	No	No
OSC optical power received	No	No	Yes	No
OSC optical power transmitted	No	No	Yes	No
Instantaneous channel power received	No	No	No	Yes
Minimum channel power received	No	No	No	Yes
Maximum channel power received	No	No	No	Yes
Instantaneous channel power transmitted	No	No	No	Yes
Minimum channel power transmitted	No	No	No	Yes
Maximum channel power transmitted	No	No	No	Yes

Table 56: BT17800 Series Optical Service PMs (continued)

Description	Port PMs	OMS PMs	OSC PMs	Service Channel PMs
Instantaneous optical back reflection ratio	No	Yes	No	No
Minimum optical back reflection ratio	No	Yes	No	No
Maximum optical back reflection ratio	No	Yes	No	No
Average optical back reflection ratio	No	Yes	No	No
Standard deviation optical back reflection ratio	No	Yes	No	No

1. To enable real-time PMs, right-click on an optical service in the tree view or in the background of an optical service topology view, and choose one of the following:

- **Enable Realtime PMs>Port**
- **Enable Realtime PMs>OMS** for BT17800 Series
- **Enable Realtime PMs>OSC**
- **Enable Realtime PMs>Service Channel**
- **Enable Realtime PMs>All Channels**

Real-time PM collection for the optical service is started, and a PM data widget title bar is displayed for each PM collection point. Additionally, a graphical view displaying the instantaneous power along with the detected power range is provided at the bottom of the screen.



**NOTE:** When you enable PMs on a stranded service<sup>1</sup>, you might see PM data widgets that do not have lines connecting them to the network elements. This behavior is normal.



**NOTE:** <sup>1</sup>A service is stranded if one or more segments in the path between the service endpoints has not been configured.

2. Click the PM data widget title bar to show or hide the PM data.

Figure 94: Real-time PMs Port View

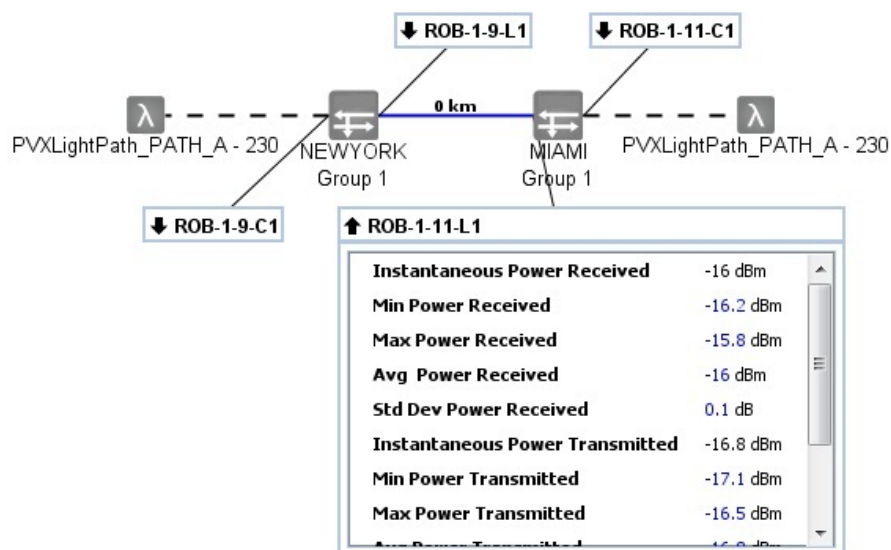


Figure 95: Real-time PMs OSC View

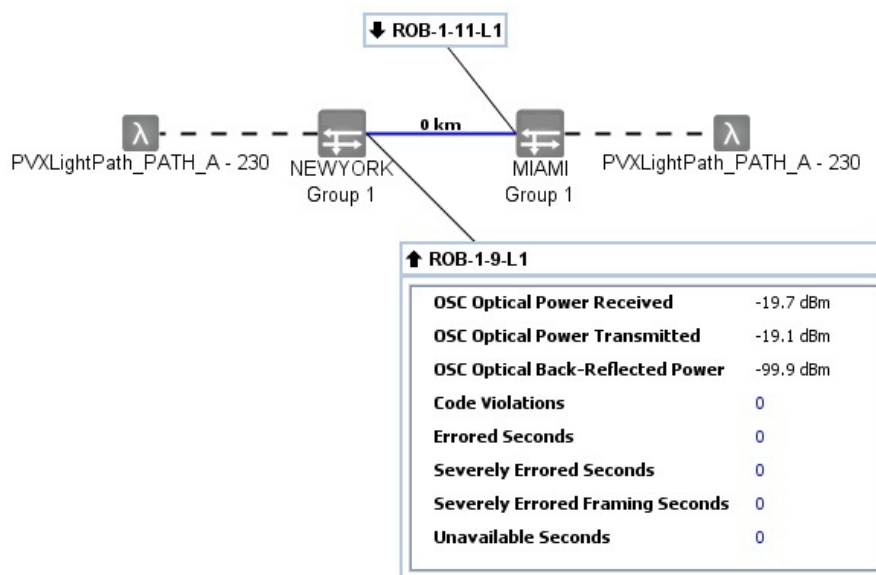


Figure 96: Real-time PMs Service Channel View

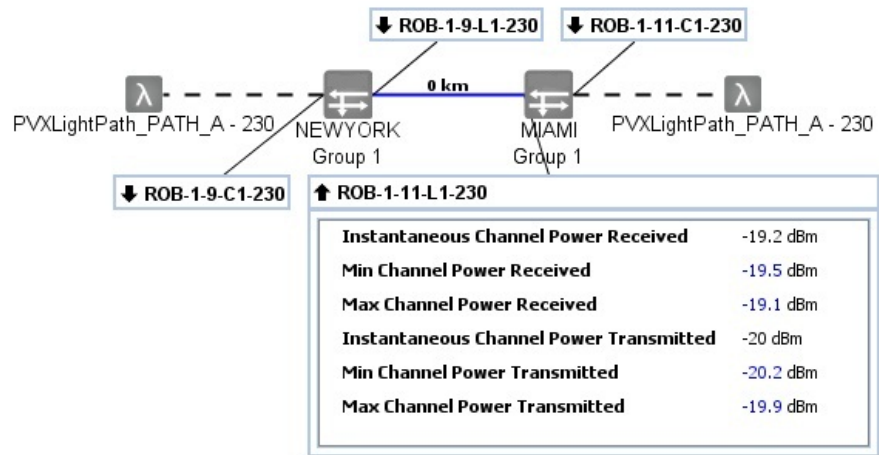
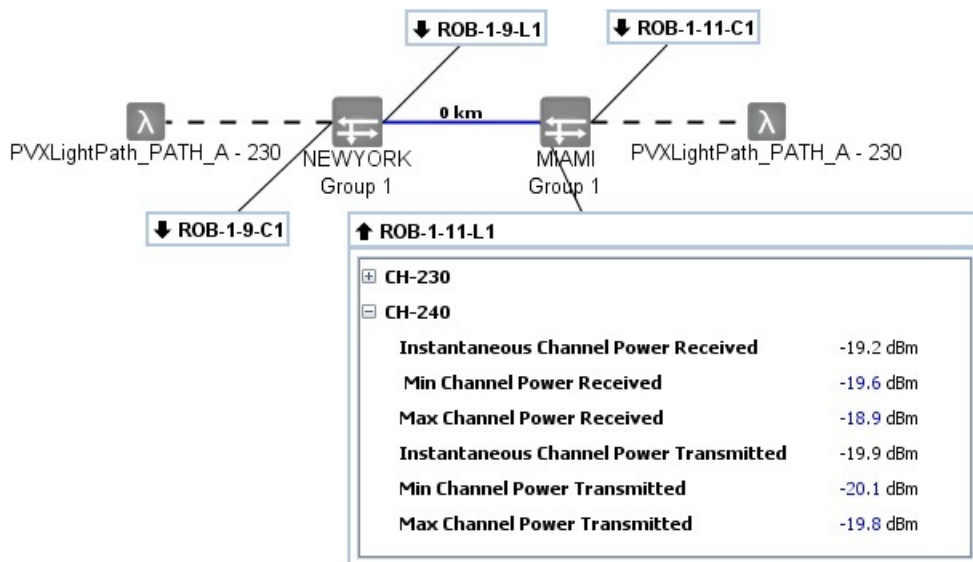


Figure 97: Real-time PMs All Channels View



- To undock the graph to its own window, right-click on the tab in the graph window and select **Undock**.

The graph appears in a window that you can reposition and resize.

Figure 98: Real-time PMs Port View Graph

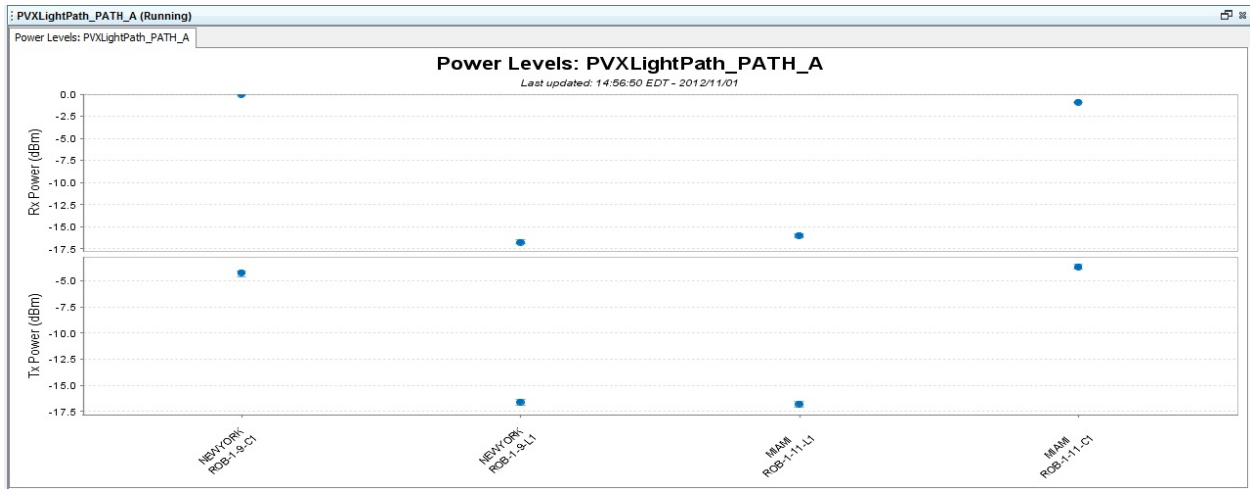


Figure 99: Real-time PMs OSC View Graph

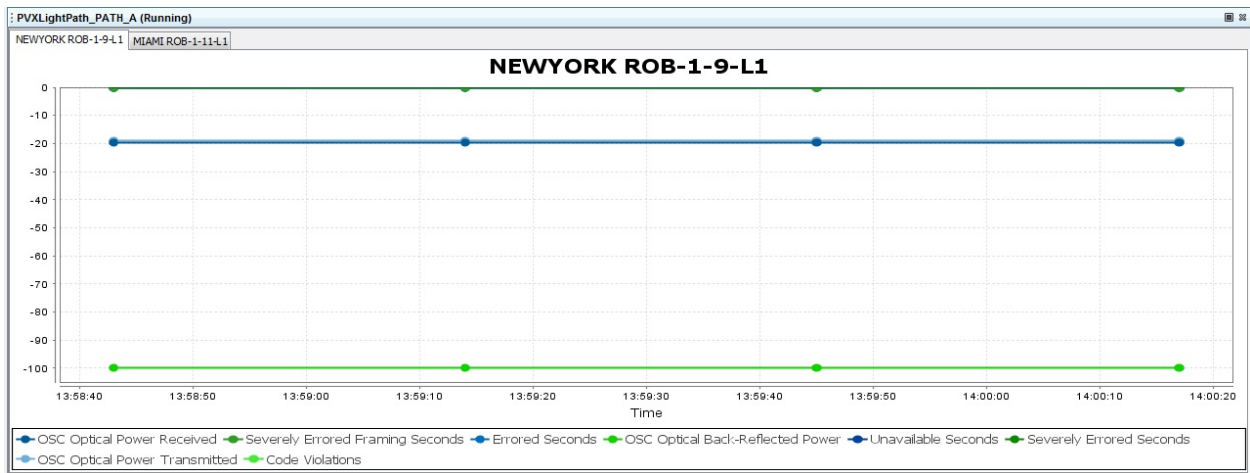


Figure 100: Real-time PMs Service Channel View Graph

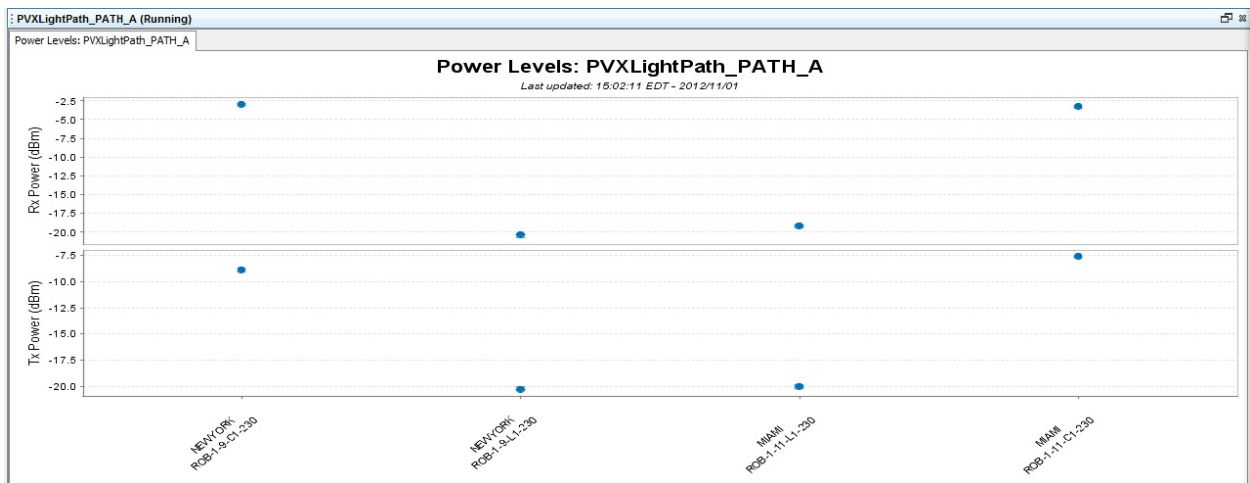
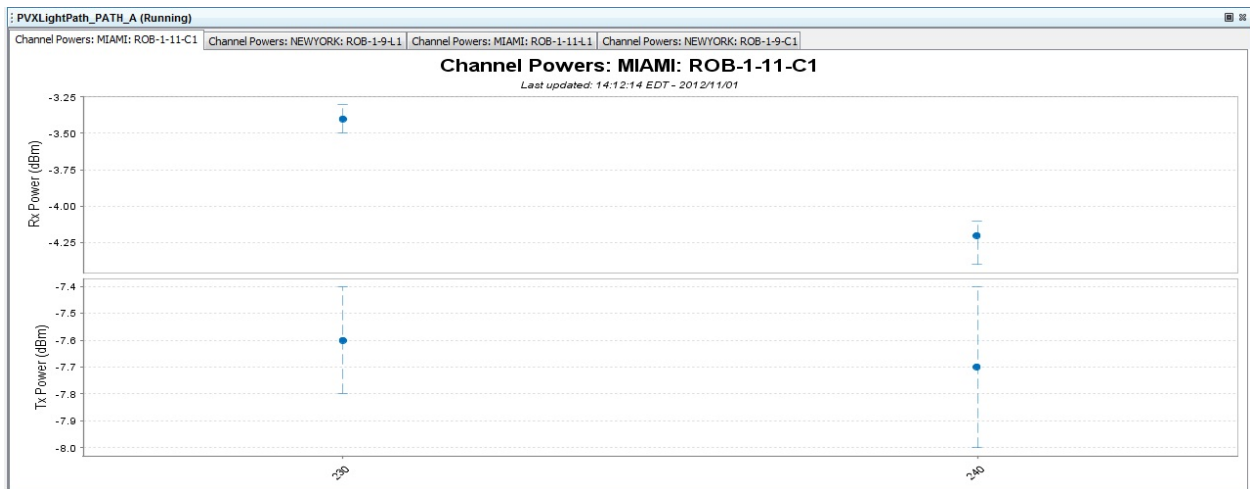
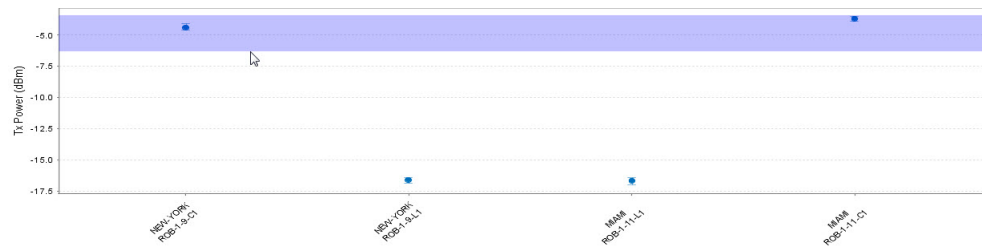


Figure 101: Real-time PMs All Channels View Graph

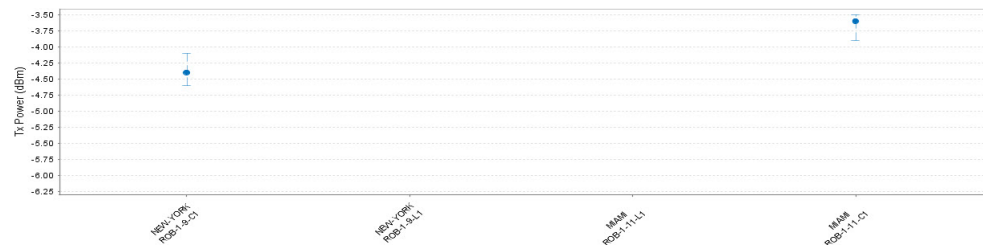


**NOTE:** The information displayed on the domain (horizontal) axis of the real-time PMs all channels graph is selectable. See [“Setting Optical Graphing Options” on page 278](#) for details on how to select what is shown.

- To change the range (vertical) scale of the graphs, highlight the desired area by left-clicking and dragging the mouse to highlight the area of focus, and release.



Repeat until the desired magnification is achieved.





**NOTE:** You can also change the scale by right-clicking on a graph, and selecting **Zoom In** or **Zoom Out**.

5. To turn off real-time PMs, right-click in the optical services topology window and choose **Disable Realtime PMs**.

## Viewing Real-time Transport Service PMs

Use this procedure to enable and view real-time PMs for transport services on a BT17800 network and transport services with BT17800, MX Series, PTX Series, or QFX Series endpoints connected across a BT17000 optical network. The PMs are displayed in both textual and graphical formats.

PSM supports the following BT17800 transport service PMs:

*Table 57: BT17800 Series Transport Service PMs*

Description	Simple	Detailed
<b>Optical and physical layer PMs</b>		
Optical power received	Yes	Yes
Minimum optical power received	No	Yes
Maximum optical power received	No	Yes
Average optical power received	No	Yes
Optical power transmitted	Yes	Yes
Minimum optical power transmitted	No	Yes
Maximum optical power transmitted	No	Yes
Average optical power transmitted	No	Yes
<b>ODU PMs</b>		
ODU errored blocks	Yes	Yes
ODU background block errors	Yes	Yes
ODU errored seconds	Yes	Yes
ODU severely errored seconds	Yes	Yes
ODU bit error ratio	Yes	Yes

Table 57: BT17800 Series Transport Service PMs (continued)

Description	Simple	Detailed
ODU minimum bit error ratio	No	Yes
ODU maximum bit error ratio	No	Yes
ODU average bit error ratio	No	Yes
<b>OTU PMs</b>		
FEC bit error ratio	Yes	Yes
FEC minimum bit error ratio	No	Yes
FEC maximum bit error ratio	No	Yes
FEC average bit error ratio	No	Yes
OTU errored blocks	Yes	Yes
OTU background block errors	Yes	Yes
OTU errored seconds	Yes	Yes
OTU severely errored seconds	Yes	Yes
OTU out of frame seconds	Yes	Yes
OTU bit error ratio	Yes	Yes
OTU minimum bit error ratio	No	Yes
OTU maximum bit error ratio	No	Yes
OTU average bit error ratio	No	Yes
<b>Ethernet PMs</b>		
Octets received	Yes	Yes
Octets OK received	No	Yes
Octets OK transmitted	No	Yes
Packets received	Yes	Yes
Packets transmitted	Yes	Yes
Packets OK received	No	Yes



Table 57: BT17800 Series Transport Service PMs (continued)

Description	Simple	Detailed
Packets OK transmitted	No	Yes
Broadcast packets received	No	Yes
Broadcast packets transmitted	No	Yes
Multicast packets received	No	Yes
Multicast packets transmitted	No	Yes
<b>Fibre Channel PMs</b>		
Optical power transmitted	Yes	Yes
Optical power received	Yes	Yes

The MX Series and PTX Series routers and QFX Series switches support the following **Simple** PMs: optical power transmit (current/average/minimum/maximum) and optical power receive (current/average/minimum/maximum). For the list of **Detailed** PMs supported on an MX Series or PTX Series router or QFX Series switch, see [“PM Counters for Optical Interfaces on MX Series and PTX Series Routers and QFX Series Switches” on page 576](#).

1. To enable real-time PMs, right-click a transport service in the tree view or in the background of a transport service topology view, and choose one of the following:

- **Enable Realtime PMs >Simple**
- **Enable Realtime PMs >Detailed**

Real-time PM collection for the transport service is started, and a PM data widget title bar is displayed in the main window for each PM collection point. Additionally, a graphical view is displayed in the bottom window.



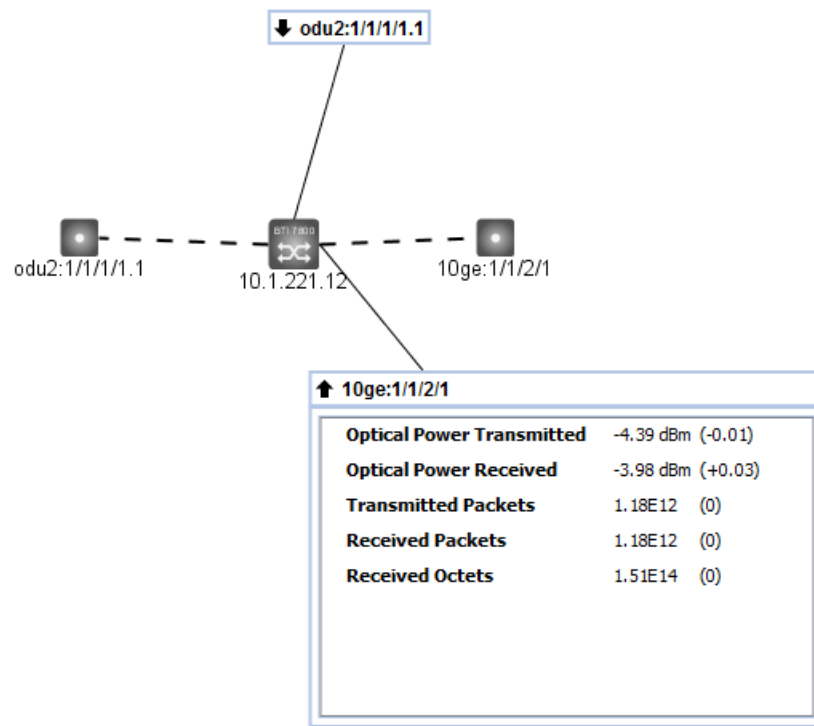
**NOTE:** When you enable PMs on a stranded service<sup>1</sup>, you might see PM data widgets that do not have lines connecting them to the network elements. This behavior is normal.



**NOTE:** <sup>1</sup>A service is stranded if one or more segments in the path between the service endpoints has not been configured.

2. Click the PM data widget title bar to show or hide the PM data.

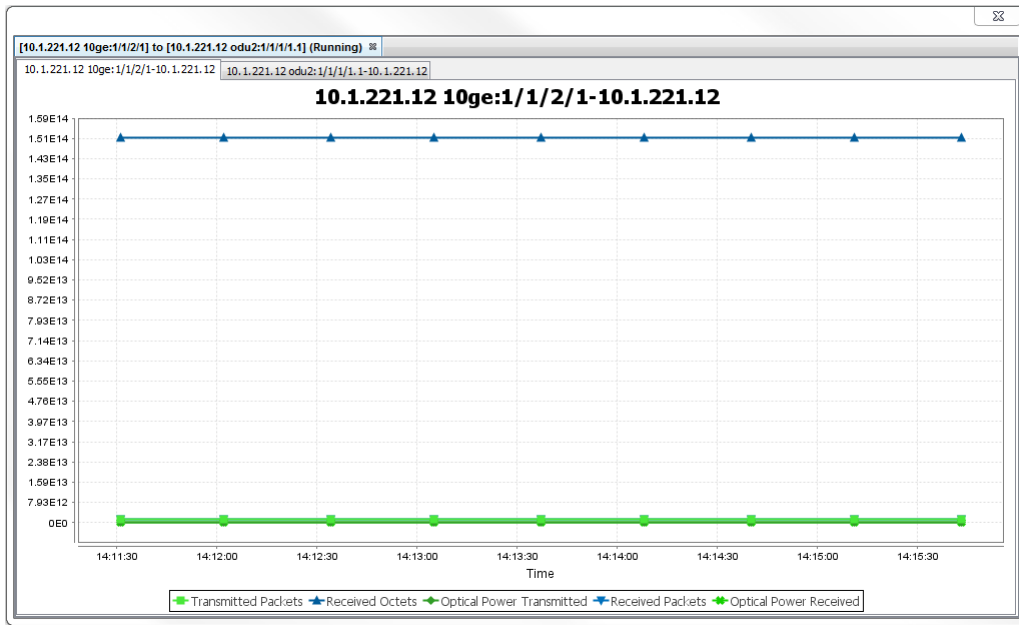
Figure 102: Real-time PMs Simple View



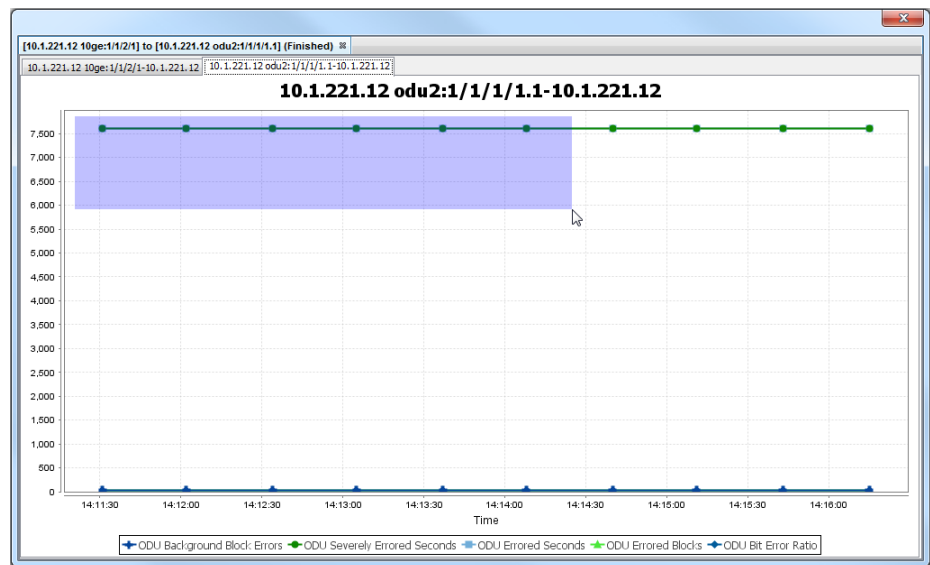
3. To undock the graph to its own window, right-click on the tab in the graph window and select **Undock**.

The graph appears in a window that you can reposition and resize.

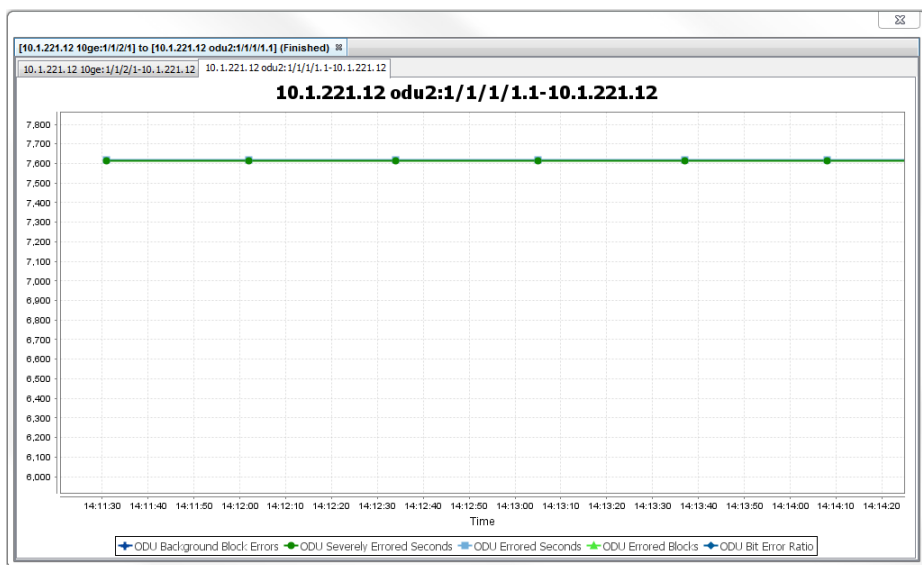
Figure 103: Real-time PMs Simple View Graph



4. To change the scale of the graphs, highlight the desired area by left-clicking and dragging the mouse to highlight the area of focus, and release.



Repeat until the desired magnification is achieved.



**NOTE:** You can also change the scale by right-clicking on a graph, and selecting **Zoom In** or **Zoom Out**.

- To turn off real-time PMs, right-click in the optical services topology window and choose **Disable Realtime PMs**.

## Viewing Real-time Ethernet PMs and SLAs

Use this procedure to enable and view real-time Ethernet PMs and SLAs on BT17000 Series, BT1700 Series, and BT1800 Series network elements.

PSM supports the following Layer 2 Ethernet PMs for UNIs:

**Table 58: BT17000 Series PMs**

Counter	Detailed	Simple	Port Utilization	Bandwidth Utilization
TFRCRX - Received Packets	Yes	Yes	-	-
TFRCTX - Transmitted Packets	Yes	Yes	-	-
TBYCRX - Received Byte Count	Yes	-	Yes	-
TBYCTX - Transmitted Byte Count	Yes	-	Yes	-
FRDR - Discarded Packets	Yes	-	-	-
BCST - Broadcast Packets	Yes	-	-	-
MCST - Multicast Packets	Yes	-	-	-

Table 58: BT17000 Series PMs (continued)

Counter	Detailed	Simple	Port Utilization	Bandwidth Utilization
Bandwidth Utilization	-	-	-	Per bandwidth profile, either at the interface or for each class map

Table 59: BT1700 Series PMs

Counter	Detailed	Simple	Port Utilization	Bandwidth Utilization
RxPkts - Received Packets	Yes	Yes	-	-
TxPkts - Transmitted Packets	Yes	Yes	-	-
RxOctets - Received Octets	Yes	-	Yes	-
TxOctets - Transmitted Octets	Yes	-	Yes	-
RxUnicastPkts - Received Unicast Packets	Yes	-	-	-
TxUnicastPkts - Transmitted Unicast Packets	Yes	-	-	-
RxMulticastPkts - Received Multicast Packets	Yes	-	-	-
TxMulticastPkts - Transmitted Multicast Packets	Yes	-	-	-
RxBroadcastPkts - Received Broadcast Packets	Yes	-	-	-
TxBroadcastPkts - Transmitted Broadcast Packets	Yes	-	-	-
Last5MinsRxPkts - Last 5 minutes (Received) Packets	Yes	-	-	-
Last5MinsTxPkts - Last 5 minutes (Transmitted) Packets	Yes	-	-	-
Last5MinsRxUtilizationRate - Last 5 minutes (Received) Utilization	Yes	-	-	-
Last5MinsTxUtilizationRate - Last 5 minutes (Transmitted) Utilization	Yes	-	-	-
RxDiscard - Received Discard Packets	Yes	-	-	-
DropEvent - Drop Events	Yes	-	-	-

Table 60: BTI800 Series PMs

Counter	Detailed	Simple	Port Utilization	Bandwidth Utilization
RxPkts - Received Packets	Yes	Yes	-	-
TxPkts - Transmitted Packets	Yes	Yes	-	-
RxOctets - Received Octets	Yes	-	Yes	-
TxOctets - Transmitted Octets	Yes	-	Yes	-
RxUnicastPkts - Received Unicast Packets	Yes	-	-	-
TxUnicastPkts - Transmitted Unicast Packets	Yes	-	-	-
RxMulticastPkts - Received Multicast Packets	Yes	-	-	-
TxMulticastPkts - Transmitted Multicast Packets	Yes	-	-	-
RxBroadcastPkts - Received Broadcast Packets	Yes	-	-	-
TxBroadcastPkts - Transmitted Broadcast Packets	Yes	-	-	-

PSM supports the following SLAs for UNIs:

Table 61: BTI7000 Series, BTI700 Series, BTI800 Series SLAs

	BTI7000 Series	BTI700 Series	BTI800 Series
NearEndFrameLoss - Near End Frame Loss Ratio	Yes	Yes <sup>1</sup>	Yes
		NOTE: <sup>1</sup> The BTI718E reports frame counts instead of ratios.	
FarEndFrameLoss - Far End Frame Loss Ratio	Yes	Yes <sup>1</sup>	Yes
2WayDelayMinimum - Minimum Delay	Yes	Yes	Yes
2WayDelayMaximum - Maximum Delay	Yes	Yes	Yes
2WayDelayAverage - Average Delay	Yes	Yes	Yes
2WayDelayVariationMinimum - Minimum Delay Variation	Yes	Yes	Yes
2WayDelayVariationMaximum - Maximum Delay Variation	Yes	Yes	Yes

Table 61: BTI7000 Series, BTI700 Series, BTI800 Series SLAs (continued)

	BTI7000 Series	BTI700 Series	BTI800 Series
2WayDelayVariationAverage - Average Delay Variation	Yes	Yes	Yes

- To enable real-time PMs or SLAs, right-click on an Ethernet service in the tree view or in an Ethernet topology view, and choose one of the following:

- Enable realtime PMs>Detailed
- Enable realtime PMs>Simple
- Enable realtime PMs>SLA
- Enable realtime PMs>Port Utilization
- Enable realtime PMs>Bandwidth Utilization

Real-time PM/SLA collection for the Ethernet service is started, and for each PM/SLA collection point in the service, a PM data widget is displayed with the current PMs/SLAs for that collection point (the statistics displayed for a given collection point are the total statistics for that point, and not just the totals for the selected service). Additionally, a graphical view is provided at the bottom of the screen.



**NOTE:** For SLA PMs, an SLA pair needs to have been created on the service view and applied.

- Click the PM data widget title bar to show or hide the PM data.

PM/SLA absolute values (and their change from the previous collection) are shown.

Figure 104: Real-time PMs Detailed View

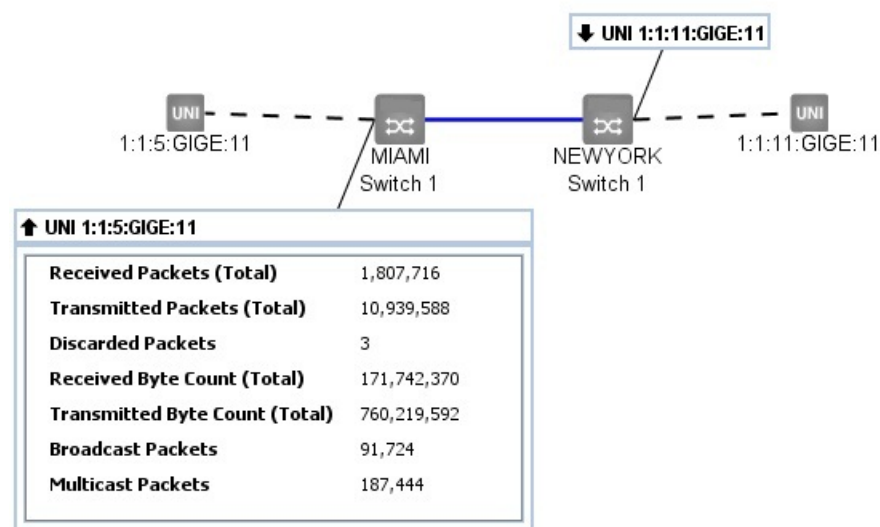


Figure 105: Real-time PMs Simple View

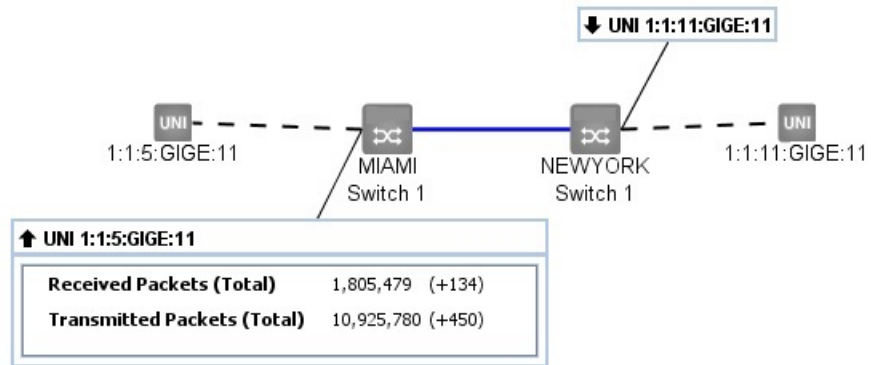


Figure 106: Real-time PMs SLA View

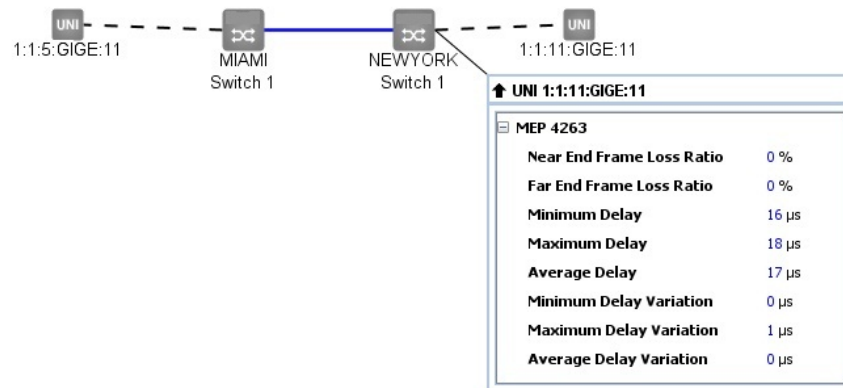


Figure 107: Real-time PMs Port Utilization View

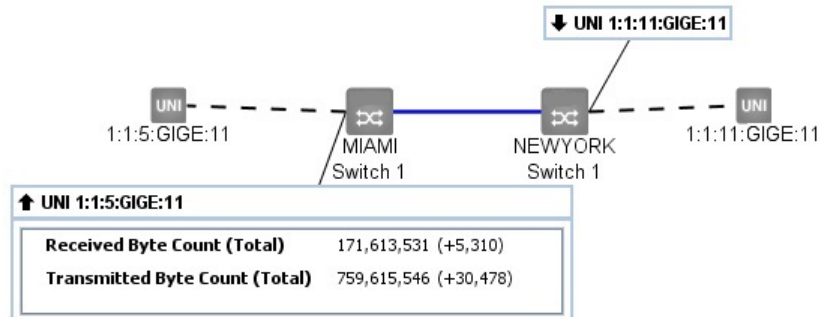
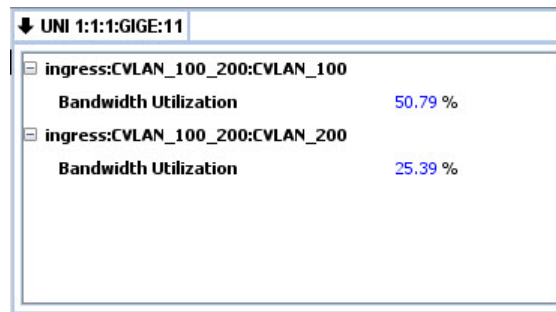




Figure 108: Real-time PMs Bandwidth Utilization View



3. To expand the graphical view to full screen, right-click on the graph window title bar and select **Maximize Window**.

Figure 109: Real-time PMs Detailed View Graph

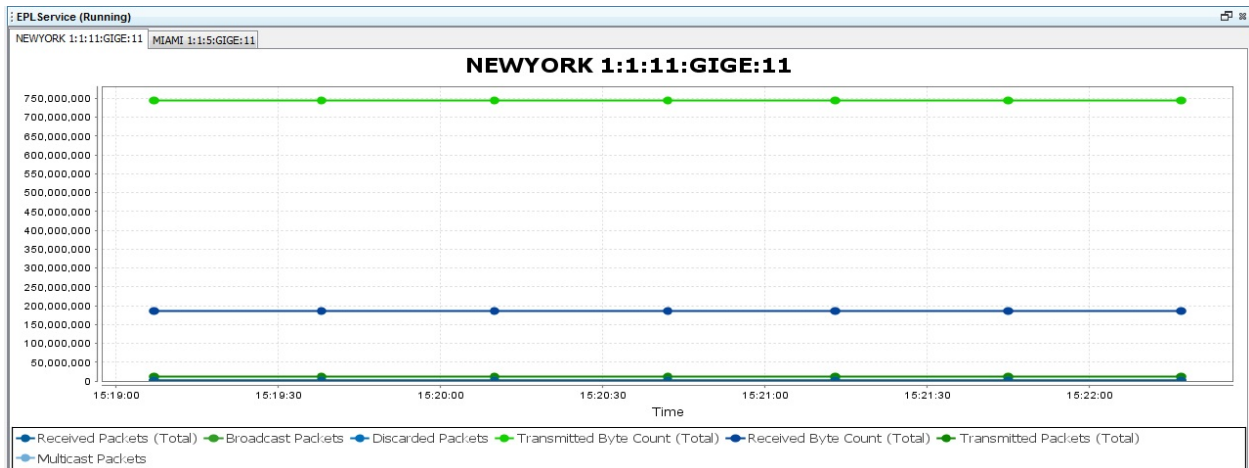


Figure 110: Real-time PMs Simple View Graph

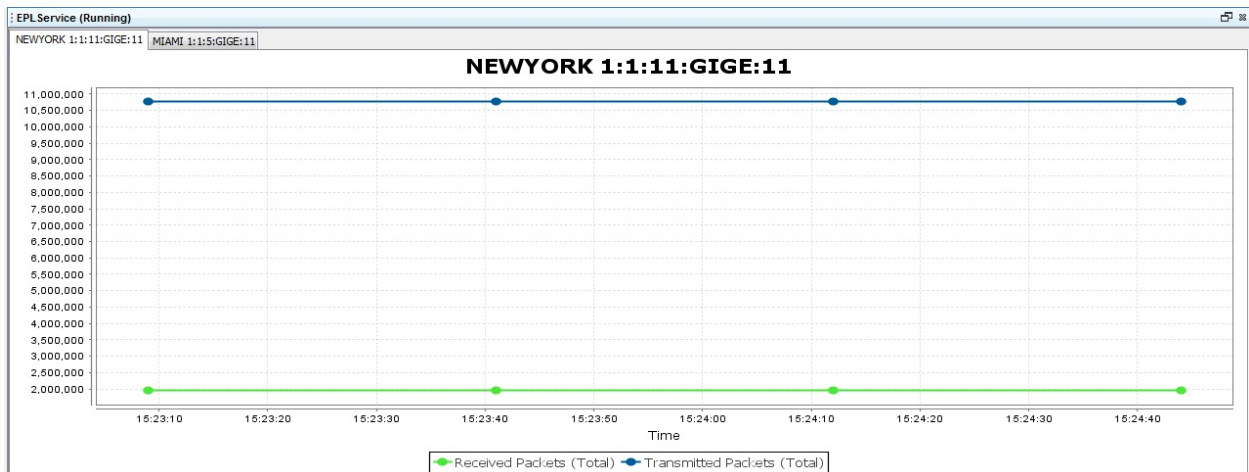


Figure 111: Real-time SLAs View Graph

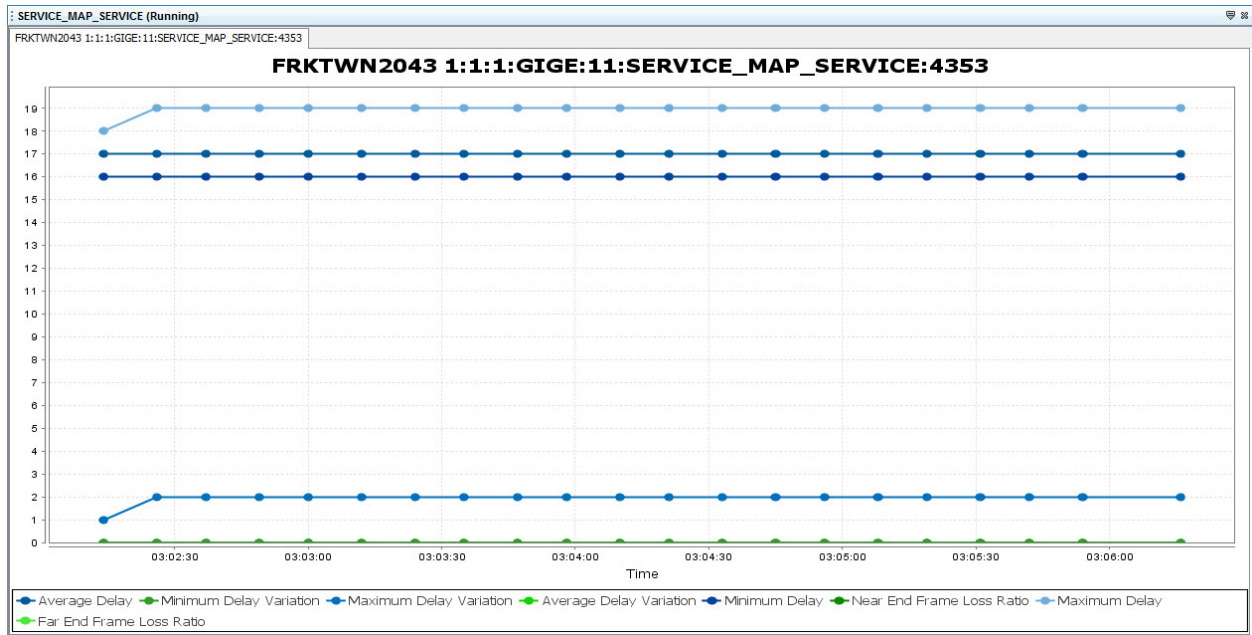


Figure 112: Real-time PMs Port Utilization View Graph

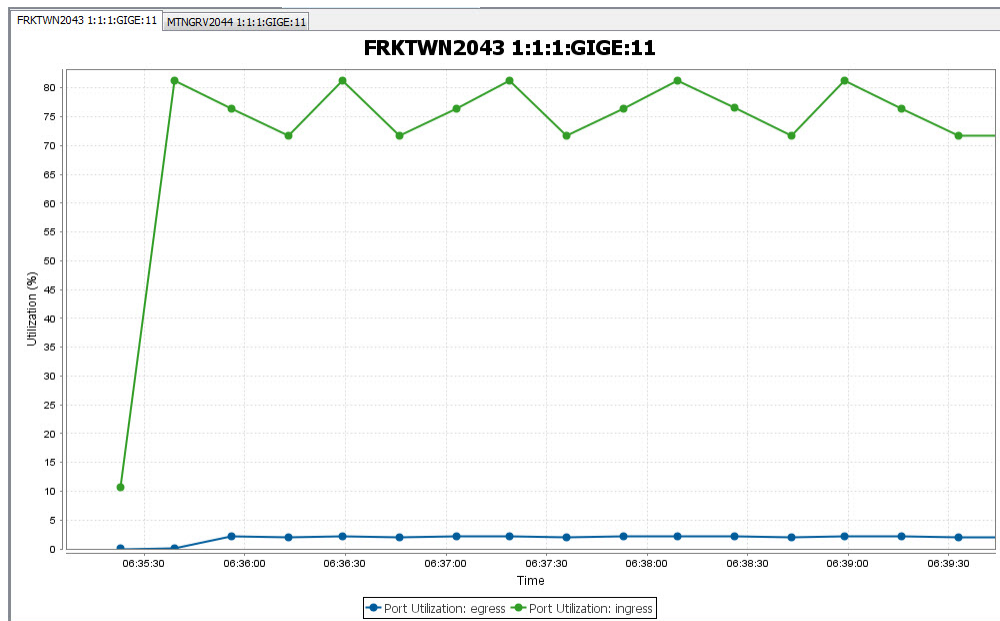
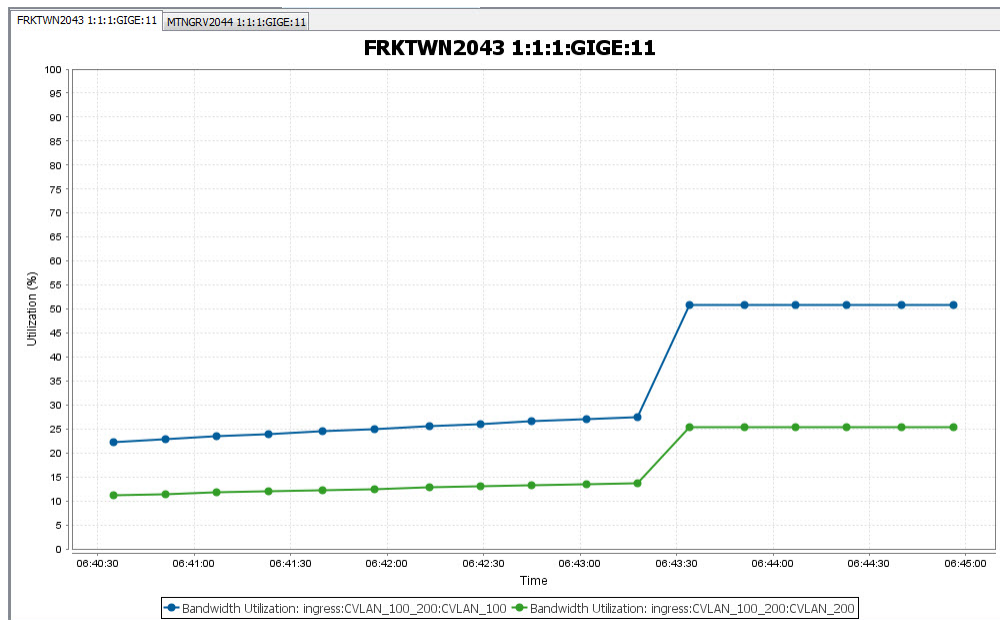
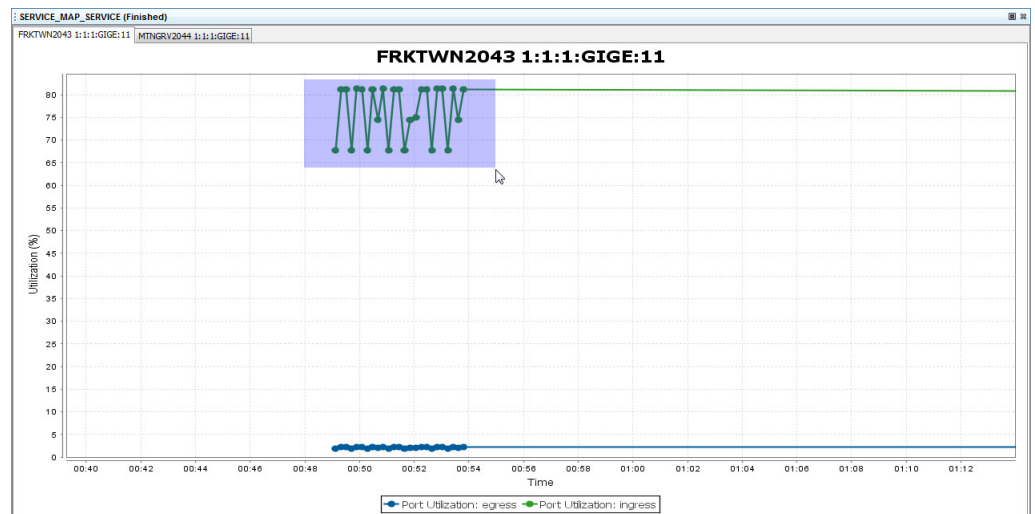


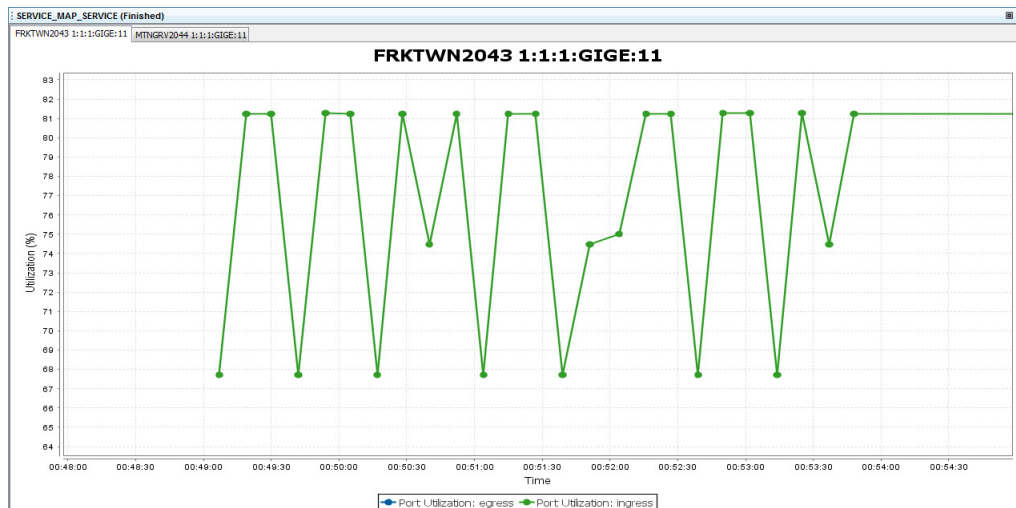
Figure 113: Real-time PMs Bandwidth Utilization Graph



- To change the scale of the graphs, highlight the desired area by left-clicking and dragging the mouse to highlight the area of focus, and release. The scale for both the domain (horizontal) axis and the range (vertical) axis can be changed.



Repeat until the desired magnification is achieved.



**NOTE:** You can also change the scales by right-clicking on a graph, and selecting **Zoom In>Range Axis**, **Zoom Out>Range Axis**, **Zoom In>Domain Axis**, and **Zoom Out>Domain Axis**. This changes the respective scales while keeping the center of the range and/or domain as the area of focus.

- To turn off real-time PMs, right-click in the Ethernet topology window and choose **Disable Realtime PMs**.

## Viewing Real-time Pseudowire PMs

Use this procedure to enable and view real-time PMs for pseudowire services on BT1800 Series network elements. The PMs are displayed in both textual and graphical formats.

PSM supports the following PMs for the pseudowire service:

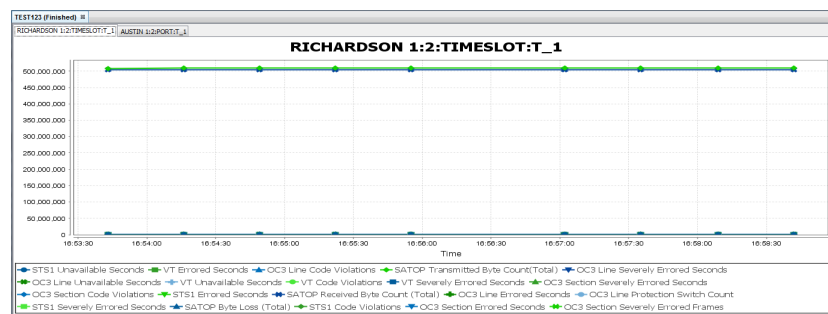
T1 PMs	E1 PMs	SONET PMs	SDH PMs	SATOP PMs
Code Violations - Line	Errored Seconds	Code Violations - Line	Code Violations - Regenerator Section	SATOP Transmitted Byte Count (Total)
Errored Seconds - Line	Severely Errored Seconds	Errored Seconds - Line	Errored Seconds - Regenerator Section	SATOP Received Byte Count (Total)
Severely Errored Seconds - Line	Background Block Error count	Severely Errored Seconds - Line	Severely Errored Seconds - Regenerator Section	SATOP Byte Loss (Total)

T1 PMs	E1 PMs	SONET PMs	SDH PMs	SATOP PMs
Code Violations - Path	Unavailable Seconds	Unavailable Seconds - Line	Unavailable Seconds - Regenerator Section	
Errored Seconds - Path	Errored Second Ratio	Code Violations - Path	Code Violations - Multiplex Section	
Severely Errored Seconds - Path	Severely Errored Second Ratio	Errored Seconds - Path	Errored Seconds - Multiplex Section	
Severely Errored Frame Seconds - Path	Background Block Error Ratio	Severely Errored Seconds - Path	Severely Errored Seconds - Multiplex Section	
Unavailable Seconds - Path		Unavailable Seconds - Path	Unavailable Seconds - Multiplex Section	
		Code Violations - Section	Code Violations - VC4 (AU4 mode only)	
		Errored Seconds - Section	Errored Seconds - VC4 (AU4 mode only)	
		Severely Errored Seconds - Section	Severely Errored Seconds - VC4 (AU4 mode only)	
		Severely Errored Frame Seconds - Section	Unavailable Seconds - VC4 (AU4 mode only)	
		Code Violations - VT	Code Violations - VC3 (AU3 mode only)	
		Errored Seconds - VT	Errored Seconds - VC3 (AU3 mode only)	
		Severely Errored Seconds - VT	Severely Errored Seconds - VC3 (AU3 mode only)	
		Unavailable Seconds - VT	Unavailable Seconds - VC3 (AU3 mode only)	
		Protection Switch Count	Code Violations - Path	
			Errored Seconds - Path	

T1 PMs	E1 PMs	SONET PMs	SDH PMs	SATOP PMs
			Severely Errored Seconds - Path	
			Unavailable Seconds - Path	
			Protection Switch Count	

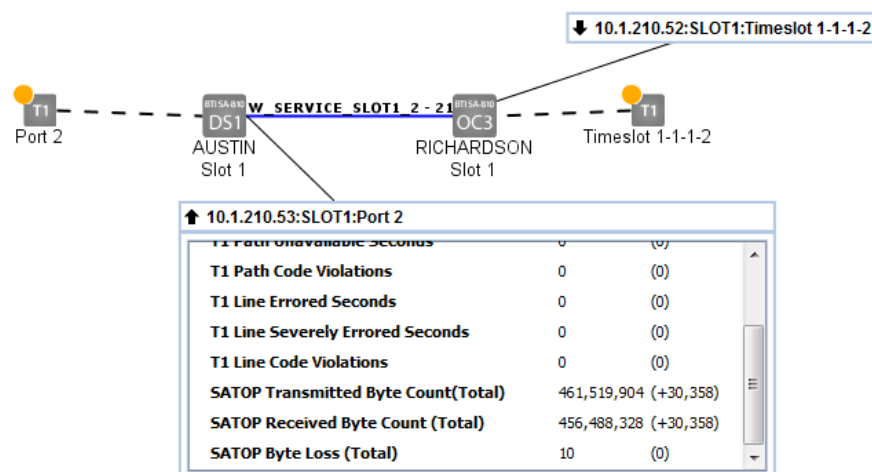
- To enable real-time PMs, right-click on a pseudowire service in the tree view or in the background of a pseudowire service topology view, and select **Enable Realtime PMs >Pseudowire**

Real-time PM collection for the pseudowire service is started, and a PM data widget title bar is displayed for each PM collection point. Additionally, a graphical view displaying the PMs pops up on the screen.

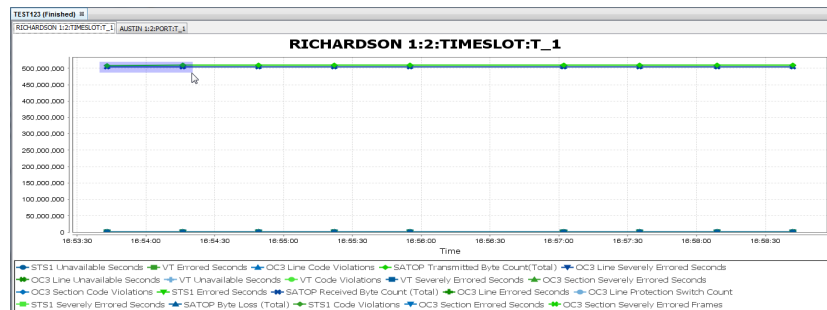


- Click the PM data widget title bar to show or hide the PM data.

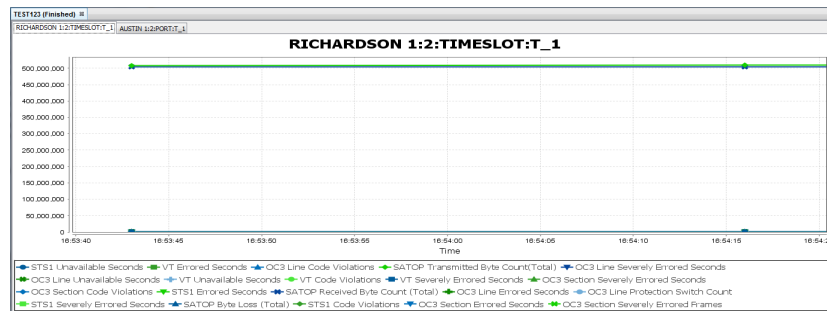
Figure 114: Real-time PMs



- To change the domain (horizontal) scale of the graphs, highlight the desired area by left-clicking and dragging the mouse to highlight the area of focus, and release.



Repeat until the desired magnification is achieved.



**NOTE:** You can also change the scale by right-clicking on a graph, and selecting **Zoom In>Domain Axis** or **Zoom Out>Domain Axis**. This changes the horizontal scale while keeping the center of the range as the area of focus.

- To turn off real-time PMs, right-click the background in the pseudowire services topology window and choose **Disable Realtime PMs**.

## Collecting and Viewing Historical PMs

Use this procedure to collect and view historical PMs for BT17000 Series, BT17800 Series, BT1800 Series, and BT1718E network elements, and supported interfaces on MX Series and PTX Series routers and QFX Series switches. See [“Nodal Management for Juniper Networks Routers and Switches”](#) on page 257 for the list of supported interfaces.

**Prerequisites:**

- For scheduled collections, ensure the scheduled historical PM retrieval capability is enabled and the retrieval schedule is set up. For information on how to do this, see the *proNX Service Manager Installation and Administration Guide*. By default, scheduled historical PM collection is disabled.



**NOTE:** When using PSM to collect historical PMs from BTI800 Series network elements, you must perform additional steps on the network element itself. See [“Configuring Historical PM Collection on BTI800 Series Network Elements” on page 558](#) for information.

Historical PMs are PMs that are collected and binned (aggregated over a measurement interval, timestamped, and discretely stored) by the network element.

You can use PSM to retrieve these historical PMs on demand and/or on a regular, pre-defined schedule. When you enable scheduled historical PM collection, PSM retrieves historical PMs every 12 hours by default, which allows you time to correct any retrieval failures for the 1-day bin while minimizing unnecessary processing.

PSM stores these collected PMs in a database for 30 days and makes them available for viewing. PM data points older than 30 days are purged from the database.

Both 15-minute and 1-day bins are collected. PM points in 15-minute bins are timestamped on the hour and at every 15 minutes thereafter. PM points for the 1-day bin are timestamped at midnight (local time of the PSM Client).

For the list of historical PMs that PSM collects for BTI7000 Series, BTI800 Series, and BTI718E network elements and MX Series and PTX Series routers, see [“PM Counters” on page 560](#). For information on BTI7800 Series historical PMs, see the BTI7800 Series documentation.

1. Retrieve historical PMs from the NE.

This is performed automatically based on the collection schedule (default every 12 hours). Optionally, you can direct PSM to retrieve historical PMs on demand by right-clicking a network element in the Network tree or in the Topology Map view and selecting **Retrieve Historical PMs**. If you do this, you must wait for the retrieval task to complete before proceeding to the next step.



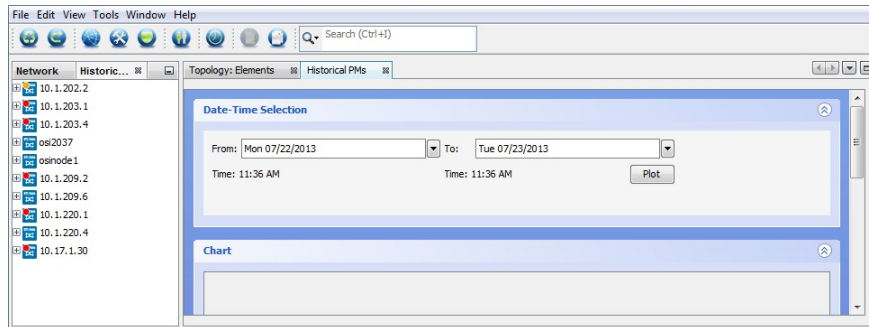
**NOTE:** It is recommended that you always run scheduled collections. Depending solely on on-demand PM retrieval will limit the collected data to what is stored on the NEs at the time of the on-demand retrievals.

2. From the main menu, choose **View > Historical PMs**, or click on the **Historical PMs** icon



The Historical PMs window appears:

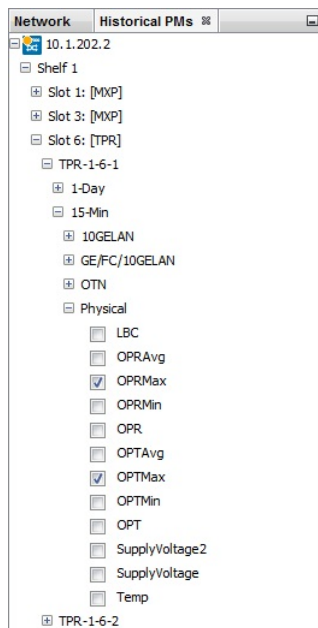




- Expand the Historical PMs tree and select the PMs you want to display. You can select PM points from more than one network element.



**NOTE:** You can select which PMs you want to view but you cannot select which historical PMs you want PSM to retrieve. PSM retrieves all historical PMs from all discovered NEs.



Discovered and reachable network elements are shown in black. Discovered and unreachable network elements are shown in red. Undiscovered network elements are shown in grey.



**NOTE:** This list might contain network elements (in grey) that no longer appear in the main Topology view. This can occur if the network elements are removed from the Topology view, but still have historical PM data associated with them.

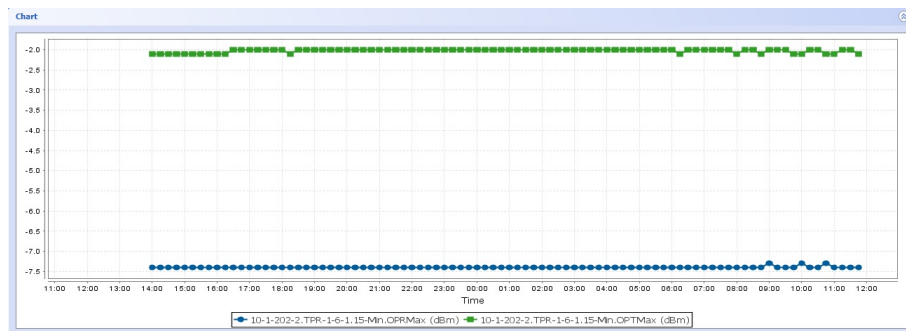


**NOTE:** When a port is reconfigured (e.g. with a different protocol), you will see PM points in the Historical PMs tree for both the old and the new protocol. This is normal behavior. PSM stores historical PM data for 30 days, at which time the data for the old protocol is purged.

- Select the time range you want to view by using the drop-down menus in the Date-Time Selection pane.

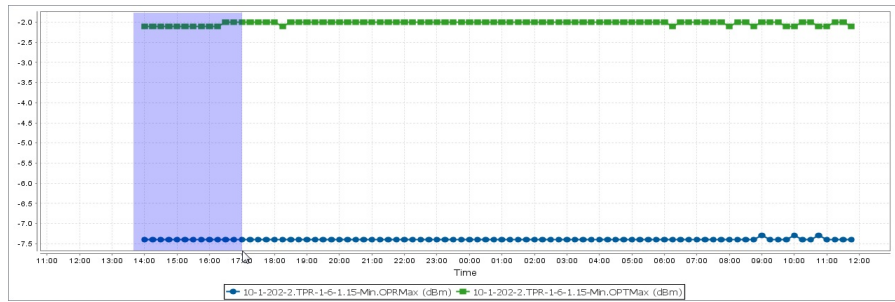
The Date-Time Selection dialog box is shown. It has a 'From:' field set to 'Mon 07/22/2013' and a 'To:' field set to 'Tue 07/23/2013'. Below these is a calendar for July 2013. The calendar shows dates from 1 to 23. The 22nd is highlighted. To the right of the calendar is a 'Time:' field set to '11:53 AM' and a 'Plot' button. Below the calendar is a 'Time:' field set to '11:53 AM'.

- Click **Plot** to plot the graph.
- The data is plotted and displayed in the Chart pane.

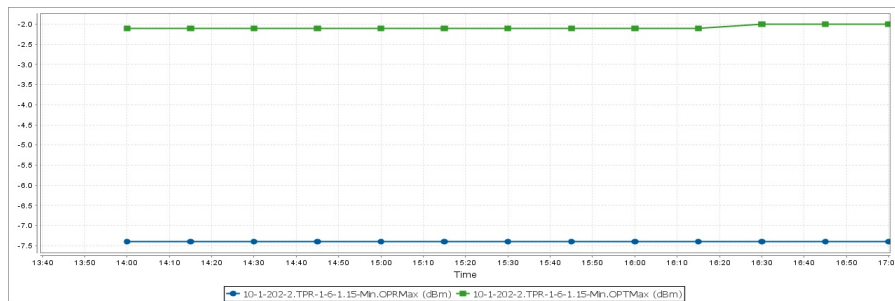


**NOTE:** In the likely event that the From: and To: times do not fall on monitoring period boundaries at the NE, the time of the first and last collections shown might not match exactly the start and end times requested.

- To zoom in on the graph, click and drag the portion you want to zoom, and then release.



The zoomed portion of the graph is displayed.



7. To select other PM counters to display in the same date and time range, go back to step 3. Remember to deselect the PM counters from the current run first.

Alternatively, you can close and re-open the Historical PMs window, but you will need to set the date and time range again.



## CHAPTER 19

# Troubleshooting

- [Managing Task Status on page 537](#)
- [Exporting Client and Server Logs on page 539](#)
- [Performing Diagnostics on page 540](#)
- [Viewing the PSM Client Log on page 540](#)
- [Testing Network Element Connectivity on page 541](#)
- [Verifying PSM Client-server Connectivity on page 542](#)
- [Collecting and Viewing NE Logs on page 542](#)
- [Saving Network Element Configuration Information on page 545](#)
- [Troubleshooting Server Replication on page 545](#)

### Managing Task Status

---

The proNX Service Manager provides a Tasks status screen that allows you to view the progress and status of running tasks. The Tasks status screen shows the list of tasks that this client has requested the server to execute. Tasks launched by other clients or scheduled tasks which are run by the server itself are not shown in this view.



**NOTE:** When performing a task on a network element, you should wait until that task completes before starting a new task on that network element.

Some tasks are displayed with a 'parent' or 'top level' task that can be expanded to show all the subtasks that the server will execute to fulfill the user request.

In the following example, Task13881 is made up of two subtasks.

Tasks			Alarms	
Task ID	Description	Type	State	Details
13770	Southeast	Ethernet Service Creation	FINISHED	
13772	10.1.204.9	NE Update	SUCCESS	
13773	10.1.204.10	NE Update	SUCCESS	
13809	Southwest	Ethernet Service Creation	FINISHED	
13811	10.1.204.9	NE Update	SUCCESS	
13812	10.1.204.8	NE Update	SUCCESS	
13881	EastWest	Ethernet Service Creation	RUNNING	
13812	13883	10.1.204.8	SUCCESS	
	13884	10.1.204.10	RUNNING	

The State column displays the current status of the tasks as RUNNING or FINISHED as reported by the server. The possible subtask states are RUNNING, SUCCESS, or FAILURE. When all subtasks are complete, the task State will transition to FINISHED. The Details column provides additional details about a task or subtask.

In an effort to protect network and server resources, the server might queue tasks that it is unable to service at the requested time. These queued tasks are **not** shown in the Tasks status window.

- If the server is busy, new task requests are placed onto a queue. These new task requests are dequeued for servicing as the server completes existing tasks. If a client requests a task that is identical to a task already queued, PSM returns an error and does not queue the new task. The error can be for a subtask if the subtask is a duplicate, or a top level task if the top level task is a duplicate.

Tasks				
Task Id	Description	Type	State	Details
2194818	10.1.204.3	Discovery Range	FINISHED	
2195664	Resync Network	Discovery Range	FAILURE	Task is already queued so will not be run. ...
2195672	10.1.111.1	Discovery Range	FINISHED	
2195729	Resync Network	Discovery Range	FINISHED	

- Limits are placed on the number of tasks that can be started by the server. These limits apply for each type of task and span across all clients. See </usr/local/ems9001/resources/serverConfigurations/workers.xml> for the specific limits.



**NOTE:** This file must not be changed or unintended consequences might occur.

Once a specific task limit is reached, any additional requests for that same type of task by any client are queued by the server. Once a running task of that type is completed,

the server dequeues the next task from that queue, and only then starts and places this new task in the respective client's Tasks status window.

- [Discovering Task Status on page 539](#)
- [Clearing Completed Tasks on page 539](#)

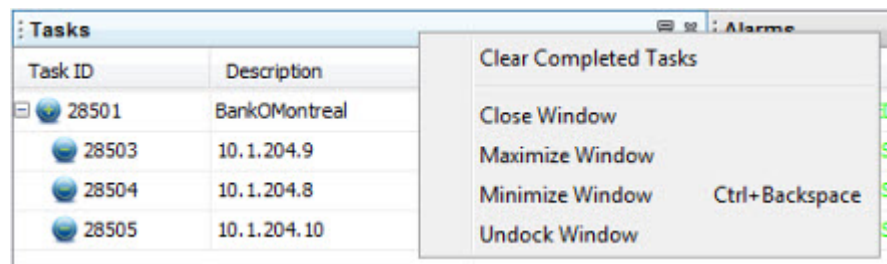
## Discovering Task Status

1. To access the Tasks status screen, click the **Tasks** tab, or, from the main menu choose **View>Server>Tasks**.

The Tasks screen is displayed in the lower right corner of the main client window.

## Clearing Completed Tasks

1. To clear the completed tasks from the Tasks status screen, right-click the title bar and select Clear Completed Tasks.



Completed tasks are removed from the Tasks screen.

## Exporting Client and Server Logs

Users can export client and server log files, and save them to a zip file on the local drive where the client resides. Client and server logs are useful in providing information to Juniper Networks Support for issue resolution.

1. To export files, click on the **Archive Logs** button on the toolbar shown below.
2. In the resulting pop-up dialog, enter the location of the directory in which you want to store the archive and click **OK**.

The filename format is **psmLogs-<date-time>.zip**. By default, the file is stored in the following locations in the user's home directory.

- Windows XP and Linux

```
Application Data\psmclient\dev\Archivedlogs
```

- Windows 7

```
AppData\Roaming\psmclient\dev\ArchivedLogs
```

- MAC OS X

Library/Application Support/psmclient/dev/ArchivedLogs



.....  
**NOTE:** These paths are relative to the user's home directory, which varies depending on the operating system. For Windows 7, the directory is C:\Users\<user\_name>\AppData\Roaming\psmclient\dev\ArchivedLogs.  
.....

---

## Performing Diagnostics

You can request the PSM client to perform the following diagnostic operations on demand to troubleshoot active issues:

- Save Configuration - saves an xml file of the network element configuration details to your local computer (for more information, see [“Saving Network Element Configuration Information” on page 545](#)).
  - Ping - performs an ICMP ping on the network element.
  - Traceroute - performs a traceroute on the network element.
  - SNMP Ping - performs an on-demand SNMP Ping.
1. In the Map view or Network tree, right-click a network element and choose **Utilities>Diagnostics** and the type of diagnostic operation you want the PSM client to perform (Save Configuration, Ping, Traceroute, or SNMP Ping).

---

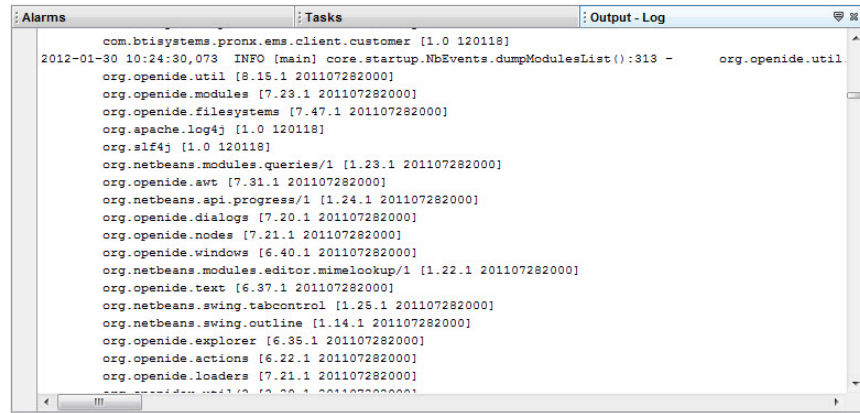
## Viewing the PSM Client Log

Use this procedure to view the active PSM Client log when troubleshooting active issues.



1. From the main menu choose **View>Log**.

The active client log tab is displayed.



## Testing Network Element Connectivity

Use this procedure to check connectivity to a discovered network element. This procedure tests IP, SNMP, and NETCONF (where applicable) connectivity to the network element.

1. Right-click the network element in the Network tree or in the Topology Map view and select **Node >Connectivity Test**.

PSM pings the NE, and checks SNMP and NETCONF connectivity where applicable. You can see the results of the test through the **View >Server >Tasks** window.

Tasks ⓘ			
Task Id	Description	Type	State
11351249	10.1.204.3	Connectivity Check	FINISHED
11351264	10.1.204.3	Connectivity Ping	SUCCESS
11351273	10.1.204.3	Connectivity Snmp	SUCCESS

If the ping fails, PSM runs a traceroute command and displays the results. The traceroute task shows SUCCESS if the traceroute command can be run. A successful traceroute task does not mean that the destination is reachable. To see the results of the traceroute, click in the Details column of the task.



**NOTE:** PSM also runs this test automatically when log collection or NE database backup/restore fails. In this case, the results are provided in the logs.

## Verifying PSM Client-server Connectivity

Use this procedure after installation or at any other time to verify that the PSM client is receiving asynchronous events from the PSM server.

1. Click **Tools >Network Element Discovery**.
2. In the **Device Discovery** window, enter a non-existent IP address in the **Discovery Criteria** box.
3. Click **OK**.

Look in the Tasks window and make sure you see the NE Discovery task for the non-existent IP address being launched and subsequently failing. If you do not see this task failing, check and fix your firewall settings and repeat this procedure.

Tasks ⓘ				
Task Id	Description	Type	State	Details
1409667	192.168.0.111	Discovery Range	FINISHED	
1409669	192.168.0.111	NE Discovery	FAILURE	Device [192.168.0.111] is not reachable

## Collecting and Viewing NE Logs

Use this procedure to collect and view logs from a BTI7000 Series NE or a BTI7800 Series NE or an MX Series or PTX Series router or QFX Series switch on demand.

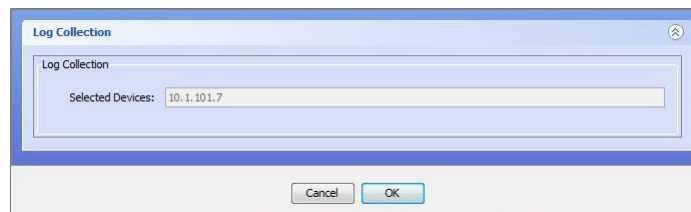


**NOTE:** The PSM server does not keep track of what logs have been retrieved from previous collections. Each time a new log collection request is made, the PSM server retrieves the full set of logs from the specified network element(s).

For information on how to set up NE log collection, including how to set up scheduled NE log collection, see the *proNX Service Manager Installation and Administration Guide*.

1. To collect the latest logs for an NE, right-click on the NE, either in the Network tree or on the Topology Map view, and choose **Retrieve Logs**.

The **Log Collection** dialog box is displayed.



2. In the **Log Collection** dialog box, click **OK**.

The logs for the NE are collected.



**NOTE:** The time that it takes for logs to be collected from a network element depends largely on the speed of the network connection. For slower connections, monitor the Tasks window for completion before viewing the logs.

3. To view the logs that have been collected, from the main menu choose **View >Network >NE Logs**.

The **Log Collection** tab is displayed.

**Filter and Sorting Options**

Filters: [ ] AND [ ] [ ]

Order By: [ ]

Logs per Page: 100

**Logs**

Log Message	Log ID	NE	System Name	Log Type	Log Number	Log Code	Log Time
-------------	--------	----	-------------	----------	------------	----------	----------

- In the **Log Collection** tab, specify the log filtering options as desired, and then click **Perform Query**.

The collected logs are filtered, sorted, and displayed according to the options specified.



**NOTE:** The Log Id might not be a unique number. When filtering, use a combination of fields to locate the desired log entries.

**Filter and Sorting Options**

Filters: NE equals 10.1.202.2 AND [ ] [ ]

Order By: Log Time Descending

Logs per Page: 100

**Logs**

Log Message	Log Id	NE	System Name	Log Type	Log Num	Log Code	Log Time
MXP-31-1-L-1-28:T-HP-UAS,,12-20,08-30-00,,,10,10,15-H	1728000	10.1.202.2	NYC2	EVENT	111635	REPT-EVT-VC4	08:30:11 EST ...
MXP-31-1-L-1-43:T-HP-UAS,,12-20,08-30-00,,,10,10,15-H	1728001	10.1.202.2	NYC2	EVENT	111636	REPT-EVT-VC4	08:30:11 EST ...
MXP-31-1-L-1-44:T-HP-UAS,,12-20,08-30-00,,,10,10,15-H	1728002	10.1.202.2	NYC2	EVENT	111637	REPT-EVT-VC4	08:30:11 EST ...
MXP-31-1-L-1-45:T-HP-UAS,,12-20,08-30-00,,,10,10,15-H	1728003	10.1.202.2	NYC2	EVENT	111638	REPT-EVT-VC4	08:30:11 EST ...
MXP-31-1-L-1-46:T-HP-UAS,,12-20,08-30-00,,,10,10,15-H	1728004	10.1.202.2	NYC2	EVENT	111639	REPT-EVT-VC4	08:30:11 EST ...
MXP-31-1-L-1-47:T-HP-UAS,,12-20,08-30-00,,,10,10,15-H	1728005	10.1.202.2	NYC2	EVENT	111640	REPT-EVT-VC4	08:30:11 EST ...
MXP-31-1-L-1-48:T-HP-UAS,,12-20,08-30-00,,,10,10,15-H	1728006	10.1.202.2	NYC2	EVENT	111641	REPT-EVT-VC4	08:30:11 EST ...
MXP-31-1-L-1-49:T-HP-UAS,,12-20,08-30-00,,,10,10,15-H	1728007	10.1.202.2	NYC2	EVENT	111642	REPT-EVT-VC4	08:30:11 EST ...
TPR-21-4-1:T-OTU-UAS,,12-20,08-30-00,,,10,10,15-MIN	1728008	10.1.202.2	NYC2	EVENT	111643	REPT-EVT-XCVR	08:30:11 EST ...
MXP-31-1-L-1-27:T-HP-UAS,,12-20,08-30-00,,,10,10,15-H	1727999	10.1.202.2	NYC2	EVENT	111634	REPT-EVT-VC4	08:30:11 EST ...
MXP-31-1-L-1:T-RS-UAS,,12-20,08-30-00,,,10,10,15-MIN	1727985	10.1.202.2	NYC2	EVENT	111620	REPT-EVT-STM64	08:30:10 EST ...
MXP-31-1-L-1:T-MS-UAS,,12-20,08-30-00,,,10,10,15-MIN	1727986	10.1.202.2	NYC2	EVENT	111621	REPT-EVT-STM64	08:30:10 EST ...



**NOTE:** PSM-generated NE log collection related alarms are not automatically cleared once the problem has been resolved. Any PSM-generated NE log collection alarms that occur must be manually cleared. To manually clear a PSM-generated alarm, right-click the alarm and choose **Clear NMS Generated Alarm**. Once cleared, you cannot restore an alarm.

## Saving Network Element Configuration Information

Use this procedure to save network element configuration data learned through SNMP to your local computer.

PSM lets you save an XML-formatted set of configuration data for a selected NE to your local computer. This configuration data is learned through SNMP. You can view the configuration data to troubleshoot issues, or attach the XML document to an e-mail to send to your support organization.

1. To save the configuration data for an NE, right-click the NE and select **Utilities >Diagnostics >Save Configuration**
2. In the Save window, select a path in the **Save in:** field where you want to save the file. The tool automatically assigns a .xml file extension to the file name.

## Troubleshooting Server Replication

This section describes how to troubleshoot server replication.

- [Loss Of Connectivity to the Cluster on page 545](#)
- [Loss Of Synchronization with a Cluster Member on page 546](#)
- [Re-establishment Of Connectivity to the Cluster on page 546](#)
- [Synchronizing Replicated Data Manually on page 546](#)
- [Restarting the Cluster on page 547](#)

### Loss Of Connectivity to the Cluster

When the PSM server loses connectivity with another member in the cluster, the server raises a 'PSM cluster node connection lost' alarm, identifying the member with which connectivity has been lost. Typically, the servers at both ends of the connection will raise the alarm, signifying a loss of connectivity with their counterpart.

PSM cluster node 10.64.6.24 connection lost	cartman	PSM cluster node availability	15:24:20 EDT - 201	15:26:00 EDT - 2	MAJOR
---	---------	-------------------------------	--------------------	------------------	-------

When this occurs, it is best that you do not change any replicated data on the local server or on any server with which connectivity has been lost. If you do make changes, you might have to manually reconcile these changes later. This becomes particularly complicated if there are more than two servers in the cluster.

## Loss Of Synchronization with a Cluster Member

When the PSM server loses synchronization with another member in the cluster, the server raises a 'Synchronization failed against cluster node' alarm, identifying the member with which synchronization has been lost. Synchronization is declared lost when the remote member does not respond to a synchronization request. A server sends out synchronization requests on restart and on manual command.

When this problem occurs, perform a manual synchronization ( [“Synchronizing Replicated Data Manually” on page 546](#) ).

## Re-establishment Of Connectivity to the Cluster

When the PSM Server re-establishes connectivity with the other member(s), the server clears the 'PSM cluster node connection lost' alarm(s).

If you did not make any changes to the replicated data on the local server or on any of the servers for which connectivity was lost, then you do not need to take any action. All servers have the correct replicated data and are synchronized.

If you did make changes to the replicated data on the local server and/or on any of the other servers for which connectivity was lost, then you will need to take the following action:

- If there are only two members in the cluster, then follow the procedure in [“Synchronizing Replicated Data Manually” on page 546](#).
- If there are more than two members in the cluster, then follow the procedure in [“Restarting the Cluster” on page 547](#).

## Synchronizing Replicated Data Manually

Use this procedure to manually synchronize replicated data with other servers in a cluster.

Before executing this command, ensure the following:

- When running with two servers in the cluster, ensure the other server has the correct replicated data.
- When running with more than two servers in the cluster, ensure all other servers have the correct replicated data. If not all of the other servers have the correct replicated data, then do not run this command.

Perform manual synchronization of replicated data on the local server when you want the local server to retrieve and adopt replicated data from the other servers. This is typically performed after recovering from a loss of connectivity, but can be done at any time.

Servers in a cluster do not automatically resynchronize with each other after recovering from a loss of connectivity because the servers have no way of knowing which server has the correct replicated data. Instead, you have to decide which server has the correct replicated data, and then manually resynchronize all the other servers with that server.

1. To force the local PSM server to manually synchronize with all servers in the cluster, select **Tools > Synch Replication**.



**NOTE:** This option is not available for selection if server replication is disabled. See the *proNX Service Manager Installation and Administration Guide* for information on how to enable server replication.

The local PSM server retrieves replicated data from all other servers in the cluster, and overwrites its own replicated data with the retrieved data.

## Restarting the Cluster

Use this procedure to restart the cluster with the correct replicated data.

In order to execute this procedure, you must have access to the Linux operating system shell on the PSM Server.

1. Decide which server in the cluster has the correct replicated data. Leave this server running.
2. Stop the PSM server application on all the other servers.
3. Start the PSM server application on each server one by one.



**NOTE:** Ensure each server is up and has the correct replicated data before bringing up the next server.

4. Proceed until all the servers are up and have the correct replicated data.



**NOTE:** For information on how to stop and start the PSM Server, see the *proNX Service Manager Installation and Administration Guide*.





# Appendix

- [Service Activation Error Messages on page 549](#)
- [PSM Alarms on page 550](#)
- [BTI7800 Alarm Details on page 554](#)
- [Installing Net-SNMP on page 555](#)
- [Configuring Historical PM Collection on BTI800 Series Network Elements on page 558](#)
- [PM Counters on page 560](#)
- [Regular Expressions on page 578](#)

## Service Activation Error Messages

The following tables list the error messages that are sent when a subtask fails during a service activation task. For the BTI7000 Series network elements, all errors are accompanied by the error code and string retrieved from the node at the time of failure. If the error occurs on a specific port, the error message will also include the port index. For the BTI700 Series devices, all error messages originate within PSM.

**Table 62: BTI7000 Series Error Messages**

Task	Error message
Create Service	Failure adding Service to Switch
	Failure updating Max Frame Size on [L2 Port Type]
	Failure provisioning Bandwidth Profile
	Failure provisioning Class Map Profile
	Failure provisioning Service Policy Profile
	Failure provisioning Port as [L2 Port Type]
	Failure associating [L2 Port Type] to Service
	Failure adding CVLAN Mapping to UNI

**Table 62: BT17000 Series Error Messages (continued)**

Task	Error message
Update Service  (Includes all of the Create Service error messages, and these error messages)	Failure updating Profiles on [L2 Port Type]
	Failure removing CVLAN Mapping on UNI
	Failure removing [L2 Port Type] from Service
	Failure removing Service from Switch
Delete Service	Failure removing [L2 Port Type] from Service
	Failure removing CVLAN Mapping on UNI
	Failure removing Service from Switch

**Table 63: BT1700 Series Error Messages**

Task	Error message
Create Service	Failure adding Service to Switch
	Failure adding Ports to Service
	Failure provisioning [L2 Port Type]
	Failure adding CVLAN Mappings to UNI
	Failure adding VLAN 4094 for PVID on UNI
	Failure setting PVID on UNI
	Failure setting Profiles on [L2 Port Type]
Update Service  (Includes all of the Create Service error messages, and these error messages)	Failure removing CVLAN Mappings from UNI
	Failure removing [L2 Port Type] from Service
Delete Service	Failure removing CVLAN Mappings from UNI
	Failure removing Profiles from [L2 Port Type]
	Failure removing Service from Switch

## PSM Alarms

The following table lists the alarms that are raised by PSM.



**NOTE:** You can modify the severity of a PSM alarm. See the *proNX Service Manager Installation and Administration Guide* for details. Modifying the severity of an alarm only affects new alarms raised after the modification takes effect. Existing alarms continue to show the unmodified severity.

Table 64: PSM Alarms

Alarm	Description	Example
Client cores	This alarm indicates that the number of processors available on the machine running the PSM Client is less than the recommended minimum. The PSM Client compares the number of available processors on the client machine with the "client.minimumCores" value configured in common.properties.	Client cores available (1) lower than minimum (2).
Client RAM	This alarm indicates that the amount of RAM available on the machine running the PSM Client is less than the recommended minimum. The PSM Client compares the amount of RAM on the client machine with the "client.minimumRAMSizeMb" value configured in common.properties.	Client RAM available (2048MB) lower than minimum (4000MB).
Client - server latency	This alarm indicates that the client/server latency is more than the recommended maximum. The PSM Client compares the last measured latency time between the client and server with the "client.maximumLatencyMs" value configured in common.properties.	Client -> Server latency (850ms) higher than maximum (700ms).
Server cores	This alarm indicates that the number of processors available on the machine running the PSM server is less than the recommended minimum. The PSM server compares the number of processors on the server machine with the "widecastOS.minimumCores" value configured in common.properties.	Cores available (6) lower than minimum (8).
Server RAM	This alarm indicates that the amount of RAM available on the machine running the PSM server is less than the recommended minimum. The PSM server compares the amount of RAM on the server machine with the "widecastOS.minimumRAMSizeMb" value configured in common.properties.	RAM available (3964MB) lower than minimum (8000MB).
Server hard disk	This alarm indicates that the amount of free Hard Disk space available on the machine running the PSM server is less than the recommended minimum. The PSM server compares the amount of HDD space on the server machine with the "widecastOS.minimumDiskSizeMb" value configured in common.properties.	HD available (24568MB) lower than minimum (150000MB).

Table 64: PSM Alarms (continued)

Alarm	Description	Example
Unreachable network element	This alarm is raised when an attempt to discover a device fails. The device will be pinged periodically to test whether it has become reachable again. If the device becomes reachable then the alarm is cleared.	Network element 10.10.10.10 is unreachable.
Notifications stopped	Connectivity to the indicated network element for receiving notifications has gone down and cannot be re-established. The NE is placed into an AUTO out-of-service mode.  If this occurs, fix the underlying problem and rediscover the network element with the correct credentials.	Notifications stopped for 10.53.4.32 on stream StatusChange
Invalid FTP server configured	This alarm is raised when the server fails to retrieve the FTP server configuration information based on the ID it is supplied from the request to perform an NE DB Backup task.	NE Database backup on PSM Server has invalid FTP server configured: 10.10.10.10:21:ftpuser
Invalid Remote ID	This alarm is raised when the server encounters an incorrectly-formatted Remote ID during topology discovery.	Invalid Remote ID format found [PVX-1-5-G2] PSM NE Invalid Remote ID
Remote ID mismatch	This alarm is raised when the server detects a Remote ID mismatch where the two endpoints are not referring to each other in bookended configurations. One alarm is raised at each endpoint.  This alarm is also raised in single-ended configurations where the frequency/wavelength associated with the multiplexer/demultiplexer channel port does not match the frequency/wavelength at the other end.	Remote ID mismatch found [PVX-1-5-G2] PSM NE Farend Mismatch
NE Link mismatch	This alarm is raised when the server detects a mismatch in topology between the LLDP data and the Remote ID configuration. The server ignores the Remote ID and shows the LLDP topology.	
NE DB backup failure	This alarm is raised when an NE DB backup process fails (either scheduled or started manually). The cause of the alarm can be attributed with any number of PSM server or NE issues, e.g. the NE DB backup process might have exceeded the maximum time allowed (300s), communication to the NE was interrupted, or the NE is unreachable. This alarm must be cleared manually.	NE DB Backup Failure. [Timed out after 300000ms waiting for 7000's trap.]. Last failure at Tue Aug 14 04:25:23 BST 2012.  NE DB Backup Failure. NE is unreachable. Last failure at Tue Aug 14 04:15:11 BST 2012.

Table 64: PSM Alarms (continued)

Alarm	Description	Example
NE DB restore failure	This alarm is raised when an NE DB restore process fails. The cause of the alarm can be attributed with any number of PSM server or NE issues, e.g. the NE DB restore process might have exceeded the maximum time allowed (300s), communication to the NE was interrupted, or the NE is unreachable. This alarm must be cleared manually.	NE DB Restore Failure. [Timed out after 300000ms waiting for 7000's trap.]. Last failure at Tue Aug 14 04:25:23 BST 2012.  NE DB Restore Failure. NE is unreachable. Last failure at Tue Aug 14 04:15:11 BST 2012.
NE log collection failure	This alarm is raised when an NE Log Collection process fails. The cause of the alarm can be attributed with any number of PSM server or NE issues, e.g. the NE Log Collection process might have exceeded the maximum time allowed (500s), communication to the NE was interrupted, or the NE is unreachable. This alarm must be cleared manually.	Log Collection Failure. NE is unreachable. Last failure at Fri Jul 13 02:00:03 BST 2012.
NE software upgrade failure	This alarm is raised when an NE Software Upgrade process fails. The cause of the alarm can be attributed with any number of server or NE issues, e.g. the NE S/W Upgrade process times out, a failure of one of the upgrade steps on the NE or the NE is unreachable. This alarm must be cleared manually.	
ERPS state change	This alarm is raised when an ERPS ring goes into protecting, pending, forced protecting, or manual protecting state. Although this alarm is raised by PSM, this alarm is also associated with the ERPS service. A change to protecting state is a major alarm, while a change to other states is a minor alarm.	ERPS Ring SUB_ERPS (SVLAN 4089) is in Protection State  ERPS Ring MAIN_RING (SVLAN 200) is in Pending State in Domain Ottawa
ERPS dynamic port	If GVRP has added ports dynamically to any ERPS rings in the network, these ports are removed from view when the ring is visualized. A minor alarm is raised indicating their presence.	ERPS Ring MAIN_RING (SVLAN 200) has Dynamically Added Ports  ERPS Ring MAIN_RING (SVLAN 200) has Dynamically Added Ports in Domain Ottawa
PSM cluster node connection lost	When running with server replication, this alarm is raised if a connection to a member of a server replication cluster is lost. The IP address of the remote member is identified in the alarm. This alarm is cleared once connection to the remote member is re-established.	PSM cluster node 10.53.4.32 connection lost
Replication processing against cluster node failed	When running with server replication, this alarm is raised if the server encounters problems while processing the replication message from another server in the cluster. The IP address of the remote member is identified in the alarm. This alarm can only be cleared manually.	Replication processing against cluster node 10.53.4.32 failed for GROUPS

Table 64: PSM Alarms (continued)

Alarm	Description	Example
Synchronization failed against cluster node	When running with server replication, this alarm is raised if the server fails to synchronize with another server in the cluster. The IP address of the remote member is identified in the alarm. This alarm is cleared when a successful synchronization with the remote member occurs. This alarm can also be cleared manually.	Synchronization failed against cluster node 10.53.4.32

## BTI7800 Alarm Details

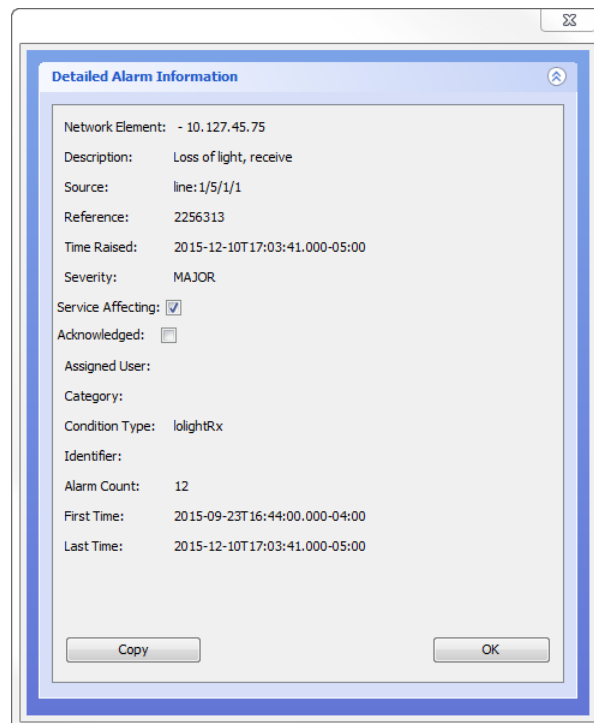
Table 65: BTI7800 Alarm Fields

Detailed Alarm Information fields	Corresponding psmNotificationAlarm objects (SNMP northbound interface)	Description
Network Element	psmNotificationAlarmSysName, psmNotificationAlarmResourceIp	A combination of the system name and the network element IP address.
Description	psmNotificationAlarmDescription	A description of the alarm.
Source	psmNotificationAlarmSource	The component raising the alarm.
Reference	psmNotificationAlarmId	An internal PSM identifier.
Time Raised	psmNotificationAlarmCreateTime	The time the alarm was raised.
Severity	psmNotificationAlarmSeverity	The alarm severity.
Service Affecting	psmNotificationAlarmServiceAffecting	An indication of whether services are affected.
Acknowledged	psmNotificationAlarmAcked	An indication of whether the alarm has been acknowledged.
Assigned User	Not applicable.	The PSM user assigned to this alarm.
Category	psmNotificationAlarmCategory	The category or type of alarm (e.g. SYSTEM, EQPT).
Condition Type	psmNotificationAlarmCodeType	The alarm mnemonic.
Identifier	psmNotificationAlarmIdentifier	Not applicable.
Alarm Count	Not applicable.	The number of times this alarm has been raised (within the time boundaries of the historical alarms report).

Table 65: BTI7800 Alarm Fields (continued)

Detailed Alarm Information fields	Corresponding psmNotificationAlarm objects (SNMP northbound interface)	Description
First Time	Not applicable.	The first time the alarm was raised (within the time boundaries of the historical alarms report).
Last Time	Not applicable.	The last time the alarm was raised (within the time boundaries of the historical alarms report).
Not applicable.	psmNotificationAlarmCleared	The alarm has been cleared.
Not applicable.	psmNotificationAlarmManuallyClearable	The alarm can be cleared manually using PSM.
Not applicable.	psmNotificationAlarmUpdateTime	The time the alarm was last updated. If the alarm has been cleared, then this object indicates the time the alarm was cleared.

Figure 115: BTI7800 Detailed Alarm Information Window (example)



## Installing Net-SNMP

Use this procedure to install Net-SNMP.

The Simple Network Management Protocol (SNMP) is a messaging protocol used by the switch to communicate configuration and status information with a network management system. SNMP messages are exchanged within a SNMP community, which consists of one or more switches and one or more management workstations. Membership in a community is controlled by community strings, which function as passwords for the community. The community strings are embedded in every SNMP packet exchanged between the members of the community to authenticate access to the Management Information Base (MIB) on the switch.

Net-SNMP is a suite of applications used to implement SNMP using IPv4 or IPv6. PSM uses Net-SNMP to deliver functionality offered in the CLI utilities. See “[Setting Utility Executables](#)” on page 280.

For detailed information and Net-SNMP download executables, go to [www.net-snmp.org](http://www.net-snmp.org).

1. Navigate to and download the latest version of Net-SNMP at [www.net-snmp.org/download.html](http://www.net-snmp.org/download.html).
2. Install Net-SNMP following the installation instructions. Use the suggested default settings.
3. To confirm that Net-SNMP is installed, use proNX Service Manager to execute an SNMP ping against a network element.
  - a. Right-click a network element and select **Utilities>Diagnostics>SNMP Ping**.

A command window should pop up with the output of the SNMP ping command:



```

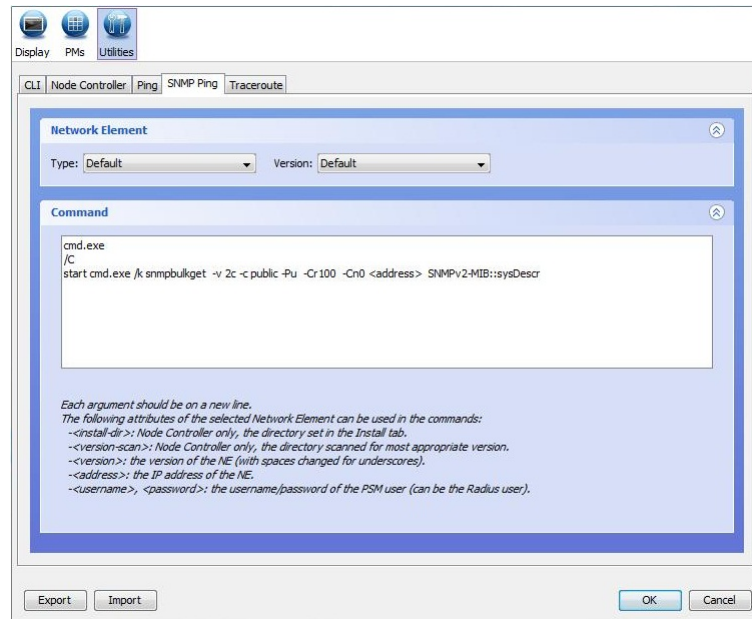
Administrator: C:\Windows\system32\cmd.exe
SNMPv2-MIB::sysDescr.0 = STRING: BTI Systems.;BTI 7000;BTI 7060;9.3.0 C005
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.18070.2.2
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (173902218) 20 days, 3:03:42.18

SNMPv2-MIB::sysContact.0 = STRING: UNKNOWN
SNMPv2-MIB::sysName.0 = STRING: MINGRU2044
SNMPv2-MIB::sysLocation.0 = STRING: BTI
SNMPv2-MIB::sysServices.0 = INTEGER: 5
SNMPv2-MIB::snmpInPkts.0 = Counter32: 2661864
SNMPv2-MIB::snmpOutPkts.0 = Counter32: 2775322
SNMPv2-MIB::snmpInBadVersions.0 = Counter32: 0
SNMPv2-MIB::snmpInBadCommunityNames.0 = Counter32: 18
SNMPv2-MIB::snmpInBadCommunityUses.0 = Counter32: 0
SNMPv2-MIB::snmpInASNParseErrs.0 = Counter32: 0
SNMPv2-MIB::snmpInTooBigs.0 = Counter32: 0
SNMPv2-MIB::snmpInNoSuchNames.0 = Counter32: 0
SNMPv2-MIB::snmpInBadValues.0 = Counter32: 0
SNMPv2-MIB::snmpInReadOnlys.0 = Counter32: 0
SNMPv2-MIB::snmpInGenErrs.0 = Counter32: 0
SNMPv2-MIB::snmpInTotalReqVars.0 = Counter32: 1713647
SNMPv2-MIB::snmpInTotalSetVars.0 = Counter32: 1011
SNMPv2-MIB::snmpInGetRequests.0 = Counter32: 1708586
SNMPv2-MIB::snmpInGetNexts.0 = Counter32: 219
SNMPv2-MIB::snmpInSetRequests.0 = Counter32: 481
SNMPv2-MIB::snmpInGetResponses.0 = Counter32: 0
SNMPv2-MIB::snmpInTraps.0 = Counter32: 0
SNMPv2-MIB::snmpOutTooBigs.0 = Counter32: 0
SNMPv2-MIB::snmpOutNoSuchNames.0 = Counter32: 0
SNMPv2-MIB::snmpOutBadValues.0 = Counter32: 0
SNMPv2-MIB::snmpOutGenErrs.0 = Counter32: 0
SNMPv2-MIB::snmpOutGetRequests.0 = Counter32: 0
SNMPv2-MIB::snmpOutGetNexts.0 = Counter32: 0
SNMPv2-MIB::snmpOutSetRequests.0 = Counter32: 0
SNMPv2-MIB::snmpOutGetResponses.0 = Counter32: 2594664
SNMPv2-MIB::snmpOutTraps.0 = Counter32: 180661
SNMPv2-MIB::snmpEnableAuthenTraps.0 = INTEGER: disabled(2)
SNMPv2-MIB::snmpProxyDrops.0 = Counter32: 0
SNMPv2-MIB::snmpSilentDrops.0 = Counter32: 0
SNMPv2-SMI::enterprises.18070.2.2.1.1.0 = STRING: "9.3.0 C005"
SNMPv2-SMI::enterprises.18070.2.2.1.1.2.0 = INTEGER: 0
SNMPv2-SMI::enterprises.18070.2.2.1.1.3.0 = INTEGER: 0
SNMPv2-SMI::enterprises.18070.2.2.1.1.4.0 = Hex-STRING: 07 DC 07 05 10 15 05 00

SNMPv2-SMI::enterprises.18070.2.2.1.1.5.0 = INTEGER: 304
SNMPv2-SMI::enterprises.18070.2.2.1.1.6.0 = INTEGER: 1
SNMPv2-SMI::enterprises.18070.2.2.1.1.7.0 = IpAddress: 10.1.1.1
SNMPv2-SMI::enterprises.18070.2.2.1.1.8.0 = IpAddress: 0.0.0.0
SNMPv2-SMI::enterprises.18070.2.2.1.1.9.0 = IpAddress: 0.0.0.0
SNMPv2-SMI::enterprises.18070.2.2.1.1.10.0 = INTEGER: 3
SNMPv2-SMI::enterprises.18070.2.2.1.1.11.0 = STRING: "000-00"
SNMPv2-SMI::enterprises.18070.2.2.1.1.12.0 = STRING: "008-00"
SNMPv2-SMI::enterprises.18070.2.2.1.1.13.1.0 = STRING: "001-00"
SNMPv2-SMI::enterprises.18070.2.2.1.1.13.2.0 = INTEGER: 0
SNMPv2-SMI::enterprises.18070.2.2.1.1.13.3.0 = STRING: "N"
SNMPv2-SMI::enterprises.18070.2.2.1.1.13.4.0 = INTEGER: 0
SNMPv2-SMI::enterprises.18070.2.2.1.1.13.5.0 = STRING: "0.0.0.0"
SNMPv2-SMI::enterprises.18070.2.2.1.1.14.0 = INTEGER: 2
SNMPv2-SMI::enterprises.18070.2.2.1.2.1.1.0.1 = INTEGER: 1
SNMPv2-SMI::enterprises.18070.2.2.1.2.1.1.11.1 = STRING: "MS2060"
SNMPv2-SMI::enterprises.18070.2.2.1.2.1.1.12.1 = STRING: "Main Shelf 2060"

```

- b. If this is unsuccessful, confirm the Net-SNMP installation directory is correct in the proNX Service Manager Options dialog.



## Configuring Historical PM Collection on BTI800 Series Network Elements

In order for PSM to retrieve historical PMs from BTI800 Series network elements, you must configure the BTI800 Series network elements to transfer the historical PM counts to the PSM server. Unlike historical PM collection for the other NE types, BTI800 Series network elements store historical PM counts in CSV files that must be transferred to the PSM server.

This procedure is required regardless of whether you are running scheduled or on-demand historical PMs.



**NOTE:** The generated CSV files are named using the NE name. Therefore each BTI800 Series network element must be configured with a unique name to ensure the CSV files that it generates have unique names when placed on the PSM server.



**NOTE:** Ensure the BTI800 Series network element is not also reporting statistics to the SLA Portal. You cannot use both PSM and the SLA Portal to retrieve counts from BTI800 Series network elements at the same time.

The following steps are performed using the CLI on the BTI800 Series network element:

1. Configure the NTP server if one is not already configured.

The following specifies the NTP server to use, and sets the time zone to EST.

```
configure ntp del-server 1
configure ntp add-server <ntp_server_ip>
configure ntp enable
configure timezone est
```

2. Disable any existing PM collection and file transfer.

```
configure pm file-transfer disable
configure pm sys disable
configure pm eth disable
configure pm oam disable
configure pm eservice disable
configure pm eservice last5m disable
configure interface average-rate disable
```

3. Enable Ethernet PM collection.

```
configure pm eth enable
```

4. Configure PM file transfer.

The following configures the BT1800 Series switch to transfer 15-minute and 1-day Ethernet PMs to the PSM server every hour, which is the highest recommended upload frequency. To change/decrease the frequency of the file transfer, change the setting of the **upload-mode** parameter.

```
configure pm file-transfer mode sftp
configure pm file-transfer target <server_ip> <username> <password>
<dest_dir> <sftp_port>
configure pm file-transfer upload-bin group del all
configure pm file-transfer upload-bin group add 15m
configure pm file-transfer upload-bin group add 24h
configure pm file-transfer upload-mode frequency 0 0 60
configure pm file-transfer upload-group add eth
configure pm file-transfer enable
```

where

- <server\_ip> is the IP address of the PSM server.
- <username> and <password> are the login credentials used to log in to the PSM server.
- <dest\_dir> is the destination directory where the historical PM CSV files are to be placed, and consequently where PSM retrieves the historical PM CSV files. This directory is specified relative to the FTP user's home directory, and should be set to **HistoricalPMs/ne800**.
- <sftp\_port> is the port number (typically 22) to use.

With these settings, the BT1800 Series network element transfers a historical PM CSV file to the PSM server once every hour. The file name includes the name of the NE (or IP address), and the GMT time and date.



**NOTE:** If you are running on-demand historical PMs, be aware of the file transfer frequency. The on-demand historical PM data reflects the counts from the last update.

## PM Counters

PSM supports the retrieval and display of PMs for various interfaces on various equipment.

- [PM Counters for BTI7000 Series Transponders and Muxponders on page 560](#)
- [PM Counters for BTI7000 Series DOL Modules on page 565](#)
- [PM Counters for BTI7000 Series packetVX Modules on page 567](#)
- [PM Counters for BTI718E Modules on page 573](#)
- [PM Counters for BTI800 Series Modules on page 574](#)
- [PM Counters for Optical Interfaces on MX Series and PTX Series Routers and QFX Series Switches on page 576](#)

### PM Counters for BTI7000 Series Transponders and Muxponders

PSM supports the retrieval and display of PMs from BTI7000 Series transponders and muxponders. The actual PMs supported depend on the configuration and the software running on the network element, and might include some of the following:

*Table 66: Physical PMs*

Name (abbreviated)	Description	Units
LBC	The laser bias current.	mA
OPRAvg	The average optical power received on the input.	dBm
OPRMax	The maximum optical power received on the input.	dBm
OPRMin	The minimum optical power received on the input.	dBm
OPR	The instantaneous optical power received on the input.	dBm
OPTAvg	The average optical power transmitted at the output.	dBm
OPTMax	The maximum optical power transmitted at the output.	dBm
OPTMin	The minimum optical power transmitted at the output.	dBm

Table 66: Physical PMs (continued)

Name (abbreviated)	Description	Units
OPT	The instantaneous optical power transmitted at the output.	dBm
SupplyVoltage2	A second supply voltage	mV
SupplyVoltage	The supply voltage	mV
Temp	The temperature measured at the transceiver or port.	Celcius

Table 67: SONET PMs

Name (abbreviated)	Description	Units
<b>Section Layer</b>		
CVS	Coding violations at the section layer.	none
ESS	Errored seconds at the section layer.	seconds
SEFSS	Severely errored framing seconds at the section layer.	seconds
SESS	Severely errored seconds at the section layer.	seconds
UASS	Unavailable seconds at the section layer.	seconds
<b>Line Layer</b>		
CVL	Coding violations at the line layer.	none
ESL	Errored seconds at the line layer.	seconds
SESL	Severely errored seconds at the line layer.	seconds
UASL	Unavailable seconds at the line layer.	seconds
<b>Path Layer</b>		
CVP	Coding violations at the path layer.	none
ESP	Errored seconds at the path layer.	seconds
FCP	Failure count at the path layer.	none
SESP	Severely errored seconds at the path layer.	seconds

*Table 67: SONET PMs (continued)*

Name (abbreviated)	Description	Units
UASP	Unavailable seconds at the path layer.	seconds

*Table 68: SDH PMs*

Name (abbreviated)	Description	Units
<b>Regenerator Section</b>		
RSBBE	Regenerator section background block errors.	none
RSEB	Regenerator section errored blocks.	none
RSES	Regenerator section errored seconds.	seconds
RSOFS	Regenerator section out-of-frame seconds.	seconds
RSSES	Regenerator section severely errored seconds.	seconds
RSUAS	Regenerator section unavailable seconds.	seconds
<b>Multiplex Section</b>		
MSBBE	Multiplex section background block errors.	none
MSEB	Multiplex section errored blocks.	none
MSES	Multiplex section errored seconds.	seconds
MSSSES	Multiplex section severely errored seconds.	seconds
MSUAS	Multiplex section unavailable seconds.	seconds
<b>High Order Path</b>		
HPBBE	High order path background block errors.	none
HPSEB	High order path errored blocks.	none
HPSES	High order path errored seconds.	seconds
HPSSSES	High order path severely errored seconds.	seconds

*Table 68: SDH PMs (continued)*

Name (abbreviated)	Description	Units
HPUAS	High order path unavailable seconds.	seconds

*Table 69: OTN PMs*

Name (abbreviated)	Description	Units
NBITCR64Bit	Bits corrected, 64-bit value.	none
NBITCR	Bits corrected.	none
NBYTCR64Bit	Bytes corrected, 64-bit value.	none
NBYTCR	Bytes corrected.	none
OTNAVGBER	Average BER.	none
OTNBER	Instantaneous BER.	none
OTUBBE	Background block errors at the OTN digital wrapper layer.	none
OTUEB	Errored blocks at the OTN digital wrapper layer.	none
OTUES	Errored seconds at the OTN digital wrapper layer.	seconds
OTUOFS	Out-of-frame seconds at the OTN digital wrapper layer.	seconds
OTUSES	Severely errored seconds at the OTN digital wrapper layer.	seconds
OTUUAS	Unavailable seconds at the OTN digital wrapper layer.	seconds
UNCRCDW	Uncorrectable codewords.	none

*Table 70: GE/FC/10GELAN PMs*

Name (abbreviated)	Description	Units
CV	Coding violations.	none
ES	Errored seconds.	seconds
INVBLK	Invalid blocks.	none

Table 70: GE/FC/10GELAN PMs (continued)

Name (abbreviated)	Description	Units
SES	Severely errored seconds.	seconds
UAS	Unavailable seconds.	seconds
BCST	Valid frames received that were directed to the broadcast address.	none
FCSE	Frames with a bad Frame Check Sequence (FCS) or frames with an alignment error (non-integral number of octets).	none
FRDR	Frames dropped.	none
FRGT	Frames received that were less than 64 octets in length and that had an FCS error or an alignment error.	none
JABR	Frames received longer than the maximum MTU size, including frames with FCS errors or alignment errors.	none
MCST	Valid frames received that were directed to a multicast address.	none
OSIZE	Frames received that were greater than 9600 octets in length, but were otherwise valid.	none
SIZE64	Frames received with the specified length or range (excluding framing bits but including FCS).	none
SIZE65To127	Frames received with the specified length or range (excluding framing bits but including FCS).	none
SIZE128To255	Frames received with the specified length or range (excluding framing bits but including FCS).	none
SIZE256To511	Frames received with the specified length or range (excluding framing bits but including FCS).	none
SIZE512To1023	Frames received with the specified length or range (excluding framing bits but including FCS).	none



Table 70: GE/FC/10GELAN PMs (continued)

Name (abbreviated)	Description	Units
SIZE1024To1518	Frames received with the specified length or range (excluding framing bits but including FCS).	none
SIZEOver1518	Frames received with the specified length or range (excluding framing bits but including FCS).	none
TBYCRX	Total bytes of data received from valid and invalid frames.	none
TBYCTX	Total bytes of data transmitted.	none
TFRCRX	Total frames received including valid and invalid frames, broadcast frames, and multicast frames.	none
TFRCTX	Total frames transmitted.	none
TPFCRX	Total PAUSE frames received.	none
TPFCTX	Total PAUSE frames transmitted.	none
USIZE	Frames received that were less than 64 octets in length, but were otherwise valid.	none

For information on what ports and protocols support these PMs, see the *BTI7000 Series Transponder Solutions Guide* and the *BTI7000 Series Muxponder Solutions Guide*.

## PM Counters for BTI7000 Series DOL Modules

PSM supports the retrieval and display of PMs from BTI7000 Series DOL modules. The actual PMs supported depend on the configuration and the software running on the network element, and might include some of the following:

Table 71: Port PMs

Name (abbreviated)	Description	Units
LossRx	The optical power loss measured on the port in the receive direction. For a line port, this represents the span loss. For a DCM port, this is the DCM loss. For a client port, this is the loss of the receive interconnection fiber.	dBm

Table 71: Port PMs (continued)

Name (abbreviated)	Description	Units
LossTx	The optical power loss measured on the port in the transmit direction. For a line port, this represents the far-end span loss. For a client port, this is the loss of the transmit interconnection fiber.	dBm
OPRAvg	The average optical power received on the input.	dBm
OPRMax	The maximum optical power received on the input.	dBm
OPRMin	The minimum optical power received on the input.	dBm
OPRStdDev	The standard deviation from the average optical power received on the input.	dBm
OPR	The instantaneous optical power received on the input.	dBm
OPTAvg	The average optical power transmitted at the output.	dBm
OPTMax	The maximum optical power transmitted at the output.	dBm
OPTMin	The minimum optical power transmitted at the output.	dBm
OPTStdDev	The standard deviation from the average optical power transmitted on the output.	dBm
OPT	The instantaneous optical power transmitted at the output.	dBm

Table 72: OSC PMs

Name (abbreviated)	Description	Units
CVS	Coding violations at the section layer.	none
ESS	Errored seconds at the section layer.	seconds
OBR	The optical back-reflected power.	dBm
OPR	The instantaneous optical power received on the input.	dBm

*Table 72: OSC PMs (continued)*

Name (abbreviated)	Description	Units
OPT	The instantaneous optical power transmitted at the output.	dBm
SEFSS	Severely errored framing seconds at the section layer.	seconds
SESS	Severely errored seconds at the section layer.	seconds
UASS	Unavailable seconds at the section layer.	seconds

*Table 73: Wavelength Channel PMs*

Name (abbreviated)	Description	Units
OPRMax	The maximum optical power received on the input.	dBm
OPRMin	The minimum optical power received on the input.	dBm
OPR	The instantaneous optical power received on the input.	dBm
OPTMax	The maximum optical power transmitted at the output.	dBm
OPTMin	The minimum optical power transmitted at the output.	dBm
OPT	The instantaneous optical power transmitted at the output.	dBm

For information on what ports and protocols support these PMs, see the *BTI7000 Series Dynamic Optical Layer Engineering Guideline*.

## PM Counters for BTI7000 Series packetVX Modules

PSM supports the retrieval and display of PMs from PVX modules. The actual PMs supported depend on the configuration and the software running on the network element, and might include some of the following:

*Table 74: Physical PMs*

Name (abbreviated)	Description	Units
LBC	The laser bias current.	mA

Table 74: Physical PMs (continued)

Name (abbreviated)	Description	Units
OPRAvg	The average optical power received on the input.	dBm
OPRMax	The maximum optical power received on the input.	dBm
OPRMin	The minimum optical power received on the input.	dBm
OPR	The instantaneous optical power received on the input.	dBm
OPTAvg	The average optical power transmitted at the output.	dBm
OPTMax	The maximum optical power transmitted at the output.	dBm
OPTMin	The minimum optical power transmitted at the output.	dBm
OPT	The instantaneous optical power transmitted at the output.	dBm
SupplyVoltage2	A second supply voltage	mV
SupplyVoltage	The supply voltage	mV
Temp	The temperature measured at the transceiver or port.	Celcius

Table 75: OTN PMs

Name (abbreviated)	Description	Units
NBITCR64Bit	Bits corrected, 64-bit value.	none
NBITCR	Bits corrected.	none
NBYTCR64Bit	Bytes corrected, 64-bit value.	none
NBYTCR	Bytes corrected.	none
OTNAVGBER	Average BER.	none
OTNBER	Instantaneous BER.	none
OTUBBE	Background block errors at the OTN digital wrapper layer.	none

*Table 75: OTN PMs (continued)*

Name (abbreviated)	Description	Units
OTUEB	Errored blocks at the OTN digital wrapper layer.	none
OTUES	Errored seconds at the OTN digital wrapper layer.	seconds
OTUOFS	Out-of-frame seconds at the OTN digital wrapper layer.	seconds
OTUSES	Severely errored seconds at the OTN digital wrapper layer.	seconds
OTUUAS	Unavailable seconds at the OTN digital wrapper layer.	seconds
UNCRCDW	Uncorrectable codewords.	none

*Table 76: GE/10GE PMs*

Name (abbreviated)	Description	Units
CV	8B/10B coding violations for GE ports.	none
ES	Errored seconds.	seconds
INVBLK	Invalid blocks on 10GE ports.	dBm
SES	Severely errored seconds.	seconds
UASS	Unavailable seconds for GE ports.	seconds

*Table 77: Ethernet L2 PMs*

Name (abbreviated)	Description	Units
BCST	Valid frames received that were directed to the broadcast address.	none
FCSE	Frames with a bad Frame Check Sequence (FCS) or frames with an alignment error (non-integral number of octets).	none
FRDR	Frames dropped.	none
FRGT	Frames received that were less than 64 octets in length and that had an FCS error or an alignment error.	none

Table 77: Ethernet L2 PMs (continued)

Name (abbreviated)	Description	Units
MCST	Valid frames received that were directed to a multicast address.	none
OSIZE	Frames received that were greater than 9600 octets in length, but were otherwise valid.	none
SIZE64	Frames received with the specified length or range (excluding framing bits but including FCS).	none
SIZE65To127	Frames received with the specified length or range (excluding framing bits but including FCS).	none
SIZE128To255	Frames received with the specified length or range (excluding framing bits but including FCS).	none
SIZE256To511	Frames received with the specified length or range (excluding framing bits but including FCS).	none
SIZE512To1023	Frames received with the specified length or range (excluding framing bits but including FCS).	none
SIZE1024To1518	Frames received with the specified length or range (excluding framing bits but including FCS).	none
SIZEOver1518	Frames received with the specified length or range (excluding framing bits but including FCS).	none
TBYCRX	Total bytes of data received from valid and invalid frames.	none
TBYCTX	Total bytes of data transmitted.	none
TFRCRX	Total frames received including valid and invalid frames, broadcast frames, and multicast frames.	none
TFRCTX	Total frames transmitted.	none
TPFCRX	Total PAUSE frames received.	none
TPFCTX	Total PAUSE frames transmitted.	none

*Table 77: Ethernet L2 PMs (continued)*

Name (abbreviated)	Description	Units
USIZE	Frames received that were less than 64 octets in length, but were otherwise valid.	none

*Table 78: LAG PMs*

Name (abbreviated)	Description	Units
INVLACFRRX	The count of invalid Link Access Control frames received on the LAG port.	none
LACPDURX	The total Link Access Control PDUs received on the LAG port.	none
LACPDUTX	The total Link Access Control PDUs transmitted on the LAG port.	none
MRKPDURX	The count of Marker PDUs received on the LAG port.	none
MRKPDUTX	The count of Marker PDUs transmitted on the LAG port.	none
MRKRSPPDURX	The count of Marker Response PDUs received on the LAG port.	none
MRKRSPPDUTX	The count of Marker Response PDUs transmitted on the LAG port.	none

*Table 79: ERPS PMs*

Name (abbreviated)	Description	Units
Blocked	The number of times this port has transitioned to blocked state.	none
EventPduRx	The number of Event PDUs received on this port.	none
EventPduTx	The number of Event PDUs transmitted on this port.	none
Failures	The number of times this port has transitioned to failed state.	none
FsPduRx	The number of FS PDUs received on this port.	none
FsPduTx	The number of FS PDUs transmitted on this port.	none

Table 79: ERPS PMs (continued)

Name (abbreviated)	Description	Units
MsPduRx	The number of MS PDUs received on this port.	none
MsPduTx	The number of MS PDUs transmitted on this port.	none
NrPduRx	The number of NR PDUs received on this port.	none
NrPduTx	The number of NR PDUs transmitted on this port.	none
NrrbPduRx	The number of NRRB PDUs received on this port.	none
NrrbPduTx	The number of NRRB PDUs transmitted on this port.	none
PduDiscard	The number of PDUs discarded on this port.	none
PduRx	The number of PDUs received on this port.	none
PduTx	The number of PDUs transmitted on this port.	none
Recoveries	The number of times this port has recovered from a failed state.	none
SfPduRx	The number of SF PDUs received on this port.	none
SfPduTx	The number of SF PDUs transmitted on this port.	none
Unblocked	The number of times this port has transitioned to unblocked state.	none
VersionDiscard	The number of PDUs version discards on this port.	none

For information on what ports and protocols support these PMs, see the *BT17000 Series packetVX Solutions Guide*.



## PM Counters for BT1718E Modules

PSM supports the retrieval and display of PMs from BT1718E devices. The actual PMs supported depend on the configuration and the software running on the network element, and might include some or all of the following:

**Table 80: Ethernet L2 PMs**

Name (abbreviated)	Description	Units
DropEvts	Total number of dropped packets due to lack of resources or otherwise.  <i>NOTE:</i> This number is not necessarily the number of frames dropped. It is just the number of times that the drop is detected.	none
FcsErrs	Total number of received packets that had a valid length but had either a bad Frame Check Sequence (FCS) or a bad FCS with a non-integral number of octets (alignment errors).	none
Fragments	Total number of received packets that were less than 64 octets long (excluding framing bits, but including Frame Check Sequence (FCS) octets) and had either a bad FCS with a integral number of octets (FCS error) or a bad FCS with a non-integral number of octets (alignment error).	none
Jumbo		none
Oversize	Total number of received packets that were longer than 9600 octets (excluding framing bits, but including Frame Check Sequence (FCS) octets) and had either a bad FCS with an integral number of octets (FCS error) or a bad FCS with a non-integral number of octets (alignment error).	none
Rx5mBps	Last 5 minutes received bytes per second rate.	bytes per second
Rx5mPps	Last 5 minutes received packets per second rate.	packets per second
RxBroadcast	Total number of good packets received that were directed to the broadcast address.	none
RxBytes	Total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets).	none
RxMulticast	Total number of good packets received that were directed to a multicast address.	none
RxPause	Total number of pause frames received.	none
RxPkts	Total number of packets (including bad packets, broadcast packets, and multicast packets) received.	none

Table 80: Ethernet L2 PMs (continued)

Name (abbreviated)	Description	Units
RxUnicast	Total number of unicast packets received on the interface and delivered to a higher-layer protocol.	none
Tx5mBps	Last 5 minutes transmitted bytes per second rate.	bytes per second
Tx5mPps	Last 5 minutes transmitted packets per second rate.	packets per second
TxBroadcast	Total number of packets transmitted that were directed to the broadcast address.	none
TxBytes	Total number of octets of data transmitted on the network (excluding framing bits but including FCS octets).	none
TxMulticast	Total number of packets transmitted that were directed to a multicast address.	none
TxPause	Total number of pause frames transmitted.	none
TxPkts	Total number of packets (including broadcast packets and multicast packets) transmitted.	none
TxUnicast	Total number of packets that higher-layer protocols requested to be transmitted to a unicast address, including those that were discarded or not sent.	none
Undersize	Total number of packets received that were less than 64 octets long (excluding framing bits, but including Frame Check Sequence (FCS) octets) and were otherwise well formed.	none

For information on these PMs, see the *BT1718E Ethernet Access Device Technical Product Guide*.

## PM Counters for BT1800 Series Modules

PSM supports the retrieval and display of PMs from BT1800 Series devices. The actual PMs supported depend on the configuration and the software running on the network element, and might include some or all of the following:

Table 81: Physical PMs

Name (abbreviated)	Description	Units
LBC	Laser Bias Current	mA
OPR	Optical Power Received.	dBm
OPT	Optical Power Transmitted.	dBm

*Table 81: Physical PMs (continued)*

Name (abbreviated)	Description	Units
Temp	Temperature	Celcius
Voltage	Voltage	Volts

*Table 82: GE Layer 1 PMs*

Name (abbreviated)	Description	Units
CV	Coding violations	none
ES	Errored seconds.	seconds
SES	Severely errored seconds.	seconds

*Table 83: Ethernet L2 PMs*

Name (abbreviated)	Description	Units
Discard	Number of received packets discarded.	none
FCS	Number of received packets with CRC error.	none
Fragment	Number of received packets that were less than 64 octets long and had either a bad FCS with an integral number of octets (FCS error) or a bad FCS with a non-integral number of octets (alignment error).	none
Jabber	Number of received packets that were more than 9600 octets long and had either a bad FCS with an integral number of octets (FCS error) or a bad FCS with a non-integral number of octets (alignment error).	none
Oversize	Number of received packets greater than 9600 octets.	none
RXBCAST	Number of broadcast packets received.	none
RXFrame	Number of frames received.	none
RXMCAST	Number of multicast packets received.	none
RXOctet	Number of octets received.	none
RXUCAST	Number of unicast packets received.	none
TXBCAST	Number of broadcast packets transmitted.	none

Table 83: Ethernet L2 PMs (continued)

Name (abbreviated)	Description	Units
TXFrame	Number of frames transmitted.	none
TXMCAST	Number of multicast packets transmitted.	none
TXOctet	Number of octets transmitted.	none
TXUCAST	Number of unicast packets transmitted.	none
Undersize	Number of received packets less than 64 octets.	none

For information on these PMs, see the *BT1800 Series Technical Product Guide*.

## PM Counters for Optical Interfaces on MX Series and PTX Series Routers and QFX Series Switches

PSM supports the retrieval and display of PMs from supported optical interfaces on MX Series and PTX Series routers and QFX Series switches. See “[Nodal Management for Juniper Networks Routers and Switches](#)” on page 257 for the list of supported interfaces.

The actual PMs supported depend on the interface, the configuration, and the software running on the router or switch, and can include some or all of the following:



**NOTE:** When viewing historical PMs for the PMs in Table 84 on page 576, the current values are not displayed.

Table 84: Optics PMs

Name (abbreviated)	Description	Units
CD, CD-Avg, CD-Min, CD-Max	Residual chromatic dispersion, current/average/minimum/maximum	ps/nm
CFO, CFO-Avg, CFO-Min, CFO-Max	Carrier frequency offset, current/average/minimum/maximum	MHz
DGD, DGD-Avg, DGD-Min, DGD-Max	Differential group delay, current/average/minimum/maximum	ps
Pwr-Rx, Pwr-Rx-Avg, Pwr-Rx-Min, Pwr-Rx-Max	Optical power receive, current/average/minimum/maximum	0.01 dBm
Pwr-Tx, Pwr-Tx-Avg, Pwr-Tx-Min, Pwr-Tx-Max	Optical power transmit, current/average/minimum/maximum	0.01 dBm
Q, Q-Avg, Q-Min, Q-Max	Q factor, current/average/minimum/maximum	0.1 dB

**Table 84: Optics PMs (continued)**

Name (abbreviated)	Description	Units
SNR, SNR-Avg, SNR-Min, SNR-Max	Signal-to-noise ratio, current/average/minimum/maximum	0.1 dB
Temp, Temp-Avg, Temp-Min, Temp-Max	Transceiver temperature, current/average/minimum/maximum	°C

**Table 85: OTU PMs**

Name (abbreviated)	Description	Units
FEC-BER-Avg-NearEnd, FEC-BER-Min-NearEnd, FEC-BER-Max-NearEnd	FEC bit error rate, average/minimum/maximum	none
FEC-CorrectedErr-NearEnd	FEC corrected errors	none
FEC-UncorrectedWords-NearEnd	FEC uncorrected words	none
OTU-BBE-NearEnd, OTU-BBE-FarEnd	OTU background block errors, near end, far end	none
OTU-ES-NearEnd, OTU-ES-FarEnd	OTU errored seconds, near end, far end	seconds
OTU-SES-NearEnd, OTU-SES-FarEnd	OTU severely errored seconds, near end, far end	seconds
OTU-UAS-NearEnd, OTU-UAS-FarEnd	OTU unavailable seconds, near end, far end	seconds

**Table 86: ODU PMs**

Name (abbreviated)	Description	Units
ODU-BBE-NearEnd, ODU-BBE-FarEnd	ODU background block errors, near end, far end	none
ODU-ES-NearEnd, ODU-ES-FarEnd	ODU errored seconds, near end, far end	seconds
ODU-SES-NearEnd, ODU-SES-FarEnd	ODU severely errored seconds, near end, far end	seconds
ODU-UAS-NearEnd, ODU-UAS-FarEnd	ODU unavailable seconds, near end, far end	seconds



**NOTE:** PSM displays all counters reported by the router or switch, which might include counters not listed above. Counters not listed above might not be supported. For the definitive list of the supported PM counters, consult the appropriate Juniper Networks documentation for the router or switch.

## Regular Expressions

Regular expressions (regex) is a highly descriptive language commonly used to search through a set of data. There are different variants of regex but most share a similar syntax.

This section describes regex in the context of PSM. PSM allows you to use regular expressions to control how entries in the **Network** tree are categorized.

A regular expression is created using one or more constructs. The expression is then compared against a set of data, which, in the case of a branch in the **Network** tree, is the set of entries or names in that branch. The simplest way to envision this is to imagine a scanner that scans through the set of names one character at a time looking for matches to the given expression.<sup>1</sup>



**NOTE:** <sup>1</sup> In reality, the regex engine uses algorithmic methods to look for matches.

*Table 87: Common Regex Constructs*

Construct	Description	Example
<b>Characters and character classes</b>		
<i>char</i>	Literal. Matches if the specified <i>char</i> matches the character at the current position in the data set.	<b>a</b> matches <b>abc</b>
<b>.</b> (dot)	Wildcard. Matches any single character at the current position in the data set. Does not match if there is no character at the current position (e.g. at the end of a name).	<b>ab.d</b> matches <b>abcd</b> and <b>abdd</b>
<b>[chars]</b>	Character class. Matches if any single <i>char</i> within the square parentheses matches the character at the current position in the data set.  The characters in the parentheses can be a list of characters or a range of characters, or a negation.	<b>[a]</b> matches <b>abc</b>  <b>[abc]</b> matches <b>abc</b> , <b>abc</b> , and <b>abc</b>  <b>[a-zA-Z]</b> matches any lowercase or uppercase letter  <b>[^a0-9]</b> matches any character that is not an <b>a</b> or a digit
<b>\w</b>	Word character, shorthand for <b>[a-zA-Z0-9_]</b> .	<b>\w</b> matches <b>!@#-a-%\$#</b>

Table 87: Common Regex Constructs (continued)

Construct	Description	Example
<code>\d</code>	Digit character, shorthand for <code>[0-9]</code> .	<code>\d</code> matches <code>abc2def</code>

<code>\</code> (backslash)	<p>Escape character.</p> <p>When immediately preceding one of the following special characters, <code>[\^\$. ?*+(){}]</code> outside a character class, the <code>\</code> suppresses the special character's meaning, and the special character is treated as a literal.</p> <p>When immediately preceding one of the following special characters, <code>^-]</code> inside a character class, the <code>\</code> suppresses the special character's meaning, and the special character is treated as a literal.</p>	<code>\.com</code> outside a character class matches <code>mycompany.com</code>
----------------------------	---	---

Construct	Description	Example
-----------	-------------	---------

**Anchors**

<code>^</code> (caret)	<p>Match at the start of the string or after a newline.<sup>1</sup></p> <p><b>NOTE:</b> A starting <code>^</code> inside a character class is a negation.</p> <p><b>NOTE:</b> <sup>1</sup>Each name in the branch is separated by the newline character.</p>	<p>If the string is <code>network_subnet</code>, then:</p> <p><code>^net</code> matches <code>network_subnet</code></p>
------------------------	--	---

<code>\$</code> (dollar)	Match at the end of the string or before a newline.	<p>If the string is <code>network_subnet</code>, then:</p> <p><code>net\$</code> matches <code>network_subnet</code></p>
--------------------------	---	--

Construct	Description	Example
-----------	-------------	---------

**Quantification**

<code>*</code> (asterisk)	Match the preceding item 0 or more times, as many times as possible (greedy match).	<p><code>om*</code> matches <code>optical</code></p> <p><code>om*</code> matches <code>commissioning</code></p>
<code>+</code>	Match the preceding item 1 or more times, as many times as possible (greedy match).	<code>om+</code> matches <code>commissioning</code>
<code>?</code>	Match the preceding item 0 or 1 time, as many times as possible (greedy match).	<p><code>om?</code> matches <code>optical</code></p> <p><code>om?</code> matches <code>commissioning</code></p>

Table 87: Common Regex Constructs (continued)

Construct	Description	Example
<b>Groupings</b>		
<i>(expression1 expression2 ...)</i>	Alternation. Matches if any of the <i>expressions</i> matches.	<b>(aaa bbb)</b> matches <b>aaa</b> or <b>bbb</b>
<i>(?&lt;=lb_expression)expression</i>	<p>Lookbehind. Matches if the main expression and the preceding lookbehind expression match. The part of the match due to <i>lb_expression</i> is not included in the matched result. The matched result consists of the match resulting from <i>expression</i> only.</p> <p>This is useful when you want to search for a string and you want to exclude the first part of that string from the matched result itself.</p>	<p><b>(?&lt;=www.)\w*\com</b> matches <b>www.mycompany.com</b></p> <p>The resulting matched string is <b>mycompany.com</b>.</p>
<i>expression(?=la_expression)</i>	<p>Lookahead. Matches if the main expression and the following lookahead expression match. The part of the match due to <i>la_expression</i> is not included in the matched result. The matched result consists of the match resulting from <i>expression</i> only.</p> <p>This is useful when you want to search for a string and you want to exclude the latter part of that string from the matched result itself.</p>	<p><b>\w*(?=)</b> matches <b>john@mycompany.com</b></p> <p>The resulting matched string is <b>john</b>.</p>