



PRODUCT DOCUMENTATION

BTI 7000 Series Transponder Solutions Guide

Part Number: BT7A73BA
Document Version: 01
Published: March 2017
Type: STANDARD

product release 13.5

Contents

Preface	vii
1.0 Transponder portfolio	1-1
1.1 Transponder modules	1-2
1.2 Transponder module operating temperature ranges	1-3
2.0 Transponder features and supported protocols	2-1
2.1 Dual 2.5G Multiprotocol Transponder features	2-2
2.2 Dual 2.5G Multiprotocol Transponder supported protocols	2-3
2.3 Dual 4G Multiprotocol Transponder features	2-4
2.4 Dual 4G Multiprotocol Transponder supported protocols	2-5
2.5 Dual 10G Multiprotocol Transponder features	2-6
2.5.1 Module temperature monitoring	2-7
2.5.2 Module voltage and fuse monitoring	2-8
2.6 Dual 10G Multiprotocol Transponder supported protocols	2-10
2.7 Dual 10G Multiprotocol Transponder Lite features	2-12
2.8 Dual 10G Multiprotocol Transponder Lite supported protocols	2-13
2.9 10G Multiprotocol Transponder features	2-14
2.10 10G Multiprotocol Transponder supported protocols	2-15
3.0 Transponder applications	3-1
3.1 Reach extension	3-2
3.2 Private Line connectivity	3-3

4.0 Installing Transponder modules, SFPs, and XFPs	4-1
4.1 Installing Transponder modules	4-2
4.2 Installing optical transceivers	4-5
4.3 Installing copper transceivers	4-8
5.0 Management interfaces	5-1
5.1 proNX 900 Node Controller, CLI, TL1, SNMP, and proNX Service Manager	5-2
6.0 Transponder protection architectures	6-1
6.1 Unprotected Wide Area Network (WAN) connectivity	6-2
6.2 Line or WAN protection	6-3
6.3 Client protection	6-4
6.3.1 Client protection set-up considerations	6-5
6.3.2 Restarting Transponder modules in a client protection group	6-5
7.0 Protection switching on Transponder modules	7-1
7.1 Protection switching severity levels	7-2
7.2 Protection switching for line protection	7-3
7.3 Protection switching for client protection	7-6
7.4 Operate protection switching on a Transponder module	7-9
7.5 Release protection switching on a Transponder module	7-10
8.0 Provisioning Transponder modules and ports	8-1
8.1 Autoprovisioning support on Transponder modules	8-2
8.2 Provisioning Transponder modules	8-4
8.2.1 Provision Transponder module settings	8-5
8.2.2 Bulk module provisioning	8-6
8.2.3 Display Transponder module information	8-8
8.2.4 Remove a Transponder module from service	8-9
8.2.5 Restore a Transponder module to service	8-9
8.2.6 Restart a Transponder module	8-10
8.2.7 Delete a Transponder module	8-10
8.3 Provisioning ports on Transponder modules	8-12
8.3.1 Provision port settings on a Transponder module	8-12
8.3.1.1 Wavelengths supported on Tunable XFP BP3AM4TL	8-17
8.3.1.2 Fault Propagation Shutdown and laser status	8-18
8.3.1.3 Monitored type (montype) values and threshold crossing alerts (TCA) for Transponder modules	8-20
8.3.1.4 Physical PMs	8-28
8.3.1.5 Threshold crossing alerts for transceiver ports	8-29
8.3.1.6 Bulk port provisioning	8-29
8.3.2 Display transceiver information	8-32
8.3.3 Display port information for a Transponder module	8-35
8.3.4 Modify port settings on a Transponder module	8-36
8.3.5 Remove a port from service	8-36

8.3.6 Restore a port to service	8-37
8.3.7 Delete a port	8-37
8.3.8 View the Transponder tuning grid	8-38
8.4 General Communications Channel	8-40
8.4.1 Enable the General Communications Channel	8-40
8.4.2 Remove the General Communications Channel from service	8-41
8.4.3 Restore the General Communications Channel to service	8-41
8.4.4 Disable the General Communications Channel	8-42
8.5 Provisioning cross-connections on Transponder modules	8-43
8.5.1 Provision a cross-connection	8-44
8.5.1.1 Supported protocol configurations for 2-Way, 2-Port cross-connections on 10G Transponder modules	8-46
8.5.2 Bulk provision cross-connections	8-48
8.5.3 Display cross-connection information	8-50
8.5.4 Delete a cross-connection	8-51
8.6 Provisioning protection groups on Transponder modules	8-52
8.6.1 Provisioning considerations for line protection groups	8-52
8.6.2 Provision line protection groups on a Transponder module	8-53
8.6.3 Provisioning considerations for client protection groups	8-53
8.6.4 Provision client protection groups on a Transponder module	8-54
8.6.5 Display protection-group information for a Transponder module	8-55
8.6.6 Modify protection-group information for a Transponder module	8-56
8.6.7 Delete a protection group on a Transponder module	8-56

9.0 Transponder port management 9-1

9.1 Retrieving and exporting performance metrics for Transponder modules	9-2
9.1.1 Retrieve and export historical PMs	9-3
9.1.2 Layer 1 Gigabit Ethernet protocol PMs	9-4
9.1.3 SONET PMs	9-4
9.1.4 SDH PMs	9-5
9.1.5 10GELAN PMs	9-7
9.1.6 Layer 1 Fibre Channel protocol PMs	9-10
9.1.7 OTN protocol PMs	9-10
9.1.8 Embedded PM support for 10G Multiprotocol Transponder and Dual 10G Multiprotocol Transponder modules	9-12
9.1.9 Retrieve and export active PMs	9-13
9.2 Monitoring threshold crossing alerts	9-15
9.2.1 Threshold crossing alerts supported on Transponder modules	9-15
9.2.2 Set Performance Monitoring threshold levels	9-17
9.2.3 View threshold crossing alerts	9-17
9.3 Performing loopback tests on transponder modules	9-19
9.4 Loopback on Y-cable client protection groups	9-21
9.5 Perform a loopback test on a Transponder module	9-23
9.6 Transponder module maintenance signals and port timing	9-24
9.6.1 10G and Dual 10G Transponder maintenance signals	9-24
9.6.2 Port timing on 10G and Dual 10G Multiprotocol Transponder modules	9-25
9.7 Laser status control	9-27

10.0 Troubleshooting Transponder modules	10-1
10.1 Alarms and events on Transponder modules	10-2
10.1.1 View alarms or events for a Transponder module	10-2
10.1.2 Transponder module alarms	10-2
11.0 Replacing Transponder modules and transceivers	11-1
11.1 Replacing transponder modules	11-2
11.1.1 System behavior when replacing the Dual 10G Multiprotocol Transponder	11-2
11.1.2 Replacing transponder modules	11-3
11.1.2.1 Replacing a Dual 10G Transponder module in a client protection configuration	11-6
11.2 Replacing optical transceivers	11-7
11.3 Replacing copper transceivers	11-11

Preface

This preface explains who should read this guide, related documentation, and documentation conventions.

Audience

This guide is primarily intended for technicians and network operation center (NOC) staff.

Features of the BTI 7000 Series

For detailed information about this release, see the *BTI 7000 Series Release Notes* for this release.

BTI 7000 Series common equipment

The following table lists the shelves and other common equipment introduced as part of the BTI 7000 Series. For detailed information, see the *BTI 7000 Series Product Guide* and the *BTI 7000 Series Common Equipment Installation Guide*.

BTI 7000 Series common equipment

Equipment	PEC
BTI 7060	BT7A50AA
BTI 7060 with rear access -48V	BT7A50AR
BTI 7060 Cooling Unit (CU)	BT7A52DA, BT7A52EA
BTI 7060 Main Shelf Interface (MSI)	BT7A53BA, BT7A53BB
BTI 7060 Expansion Shelf Interface (ESI)	BT7A54BA
BTI 7060/BTI 7200 System Control Processor (SCP)	BT7A20CA
BTI 7060 AC Power Assembly Kit	BT7A50BA
BTI 7060 AC Power Module	BT7A58AA
BTI 7060 Filler Panel Kit	BT7A55EA

BTI 7000 Series common equipment (Continued)

Equipment	PEC
2U Cover – ANSI	BT7A5070
2U Cover – ETSI	BT7A5071
BTI 7030	BT7A56AA
BTI 7030 Cooling Unit (CU)	BT7A57BA
BTI 7030 Main Shelf Interface (MSI)	BT7A53CA, BT7153CB, BT7A53BB
BTI 7030 System Control Processor (SCP)	BT7A21BA
BTI 7030 AC Power Assembly Kit	BT7A56CA
BTI 7030 AC Power Module	BT7A58BA
1U Cover – ANSI	BT7A5670
1U Cover – ETSI	BT7A5671
BTI 7020	BT7A56BA
BTI 7200	BT7A51AA
BTI 7200 with rear access -48V	BT7A51AR
BTI 7200 Cooling Unit (CU)	BT7A52EA
BTI 7200 Main Shelf Interface (MSI)	BT7A53EA
BTI 7200 Common Communication Module (CCM)	BT7A54EA
BTI 7200 ANSI shelf cover	BT7A5180
BTI 7200 ETSI shelf cover	BT7A5181
BTI 7200 Air Deflector	BT7A59EA
BTI 7200 Installation kit	BT7A5034
BTI 7200 Pack of 5 Mounting Bracket Pairs (7200)	BT7A5035
BTI 7200 Pack of 5 Center Guides	BT7A5036
Single Expansion Shelf Kit (2x 1310 SFP, 1x Dual SM Patch Cord 1.5m)	BP1A58LA-01.5
Single Expansion Shelf Kit (2x 1310 SFP, 1x Dual SM Patch Cord 2m)	BP1A58LA-02

The BTI 7000 Series shelves support a wide range of modules. For the list of modules supported, see the *BTI 7000 Series Product Guide*.

The following table lists the BTI graphical user interface management software suite. For detailed information about each application, refer to the documentation set for the application.

Management software suite

proNX Management Suite
proNX Service Manager (PSM)
proNX 900 Node Controller (proNX 900)

Equipment compliance

The following table provides agency-compliance information for BTI 7000 Series equipment.




Agency	Compliance information
FDA	This equipment is classified by the FDA under IEC 60825, parts 1 and 2, as a Class 1 laser product with a Class 1 hazard rating.
FCC	This equipment complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) This device must accept any interference received, including interference that may cause undesired operation.
Industry Canada	This Class A digital apparatus complies with Canadian ICES-003.

Organization of the BTI 7000 Series documentation

The following guides are contained in the BTI 7000 Series documentation suite.

- *BTI 7000 Series Alarm and Troubleshooting Guide*
- *BTI 7000 Series Command Line Interface Reference Guide*
- *BTI 7000 Series Common Equipment Installation Guide*
- *BTI 7000 Series Dynamic Optical Layer Engineering Guideline*
- *BTI 7000 Series Management Communications Channel Solutions Guide*
- *BTI 7000 Series Multiplexing Solutions Guide*
- *BTI 7000 Series Muxponder Solutions Guide*
- *BTI 7000 Series Operations Solutions Guide*
- *BTI 7000 Series Optical Amplifier and DCM Solutions Guide*
- *BTI 7000 Series packetVX Solutions Guide*
- *BTI 7000 Series Product Guide*
- *BTI 7000 Series SNMP Overview Guide*
- *BTI 7000 Series Test and Turn-up Guide*
- *BTI 7000 Series TLI Reference Guide*
- *BTI 7000 Series Transceiver InformationGuide*
- *BTI 7000 Series Transponder Solutions Guide*
- *BTI 7000 Series Upgrade Guide*
- *BTI 7000 Series Release Notes*
- *BTI 7000 Series Quick Installation Notes (various)*

Documentation conventions

Convention	Description
Note	Means reader take note. Notes contain helpful suggestions or background information.
 Caution	Means reader be careful. Equipment damage or loss of data can result from your actions.
 Warning	Means reader be careful. Harm to yourself or others can result from your actions.
 Laser Warning	Invisible laser radiation can be emitted from the aperture ports of amplifier circuit packs when no fiber cable is connected. Avoid exposure and do not stare into open apertures to avoid permanent eye damage.

Copyright © 2017 Juniper Networks, Inc. ALL RIGHTS RESERVED.

This product is the property of Juniper Networks, Inc. and its licensors, and is protected by copyright. Any reproduction in whole or in part is strictly prohibited. Juniper, Juniper Networks, BTI, BTI SYSTEMS, packetVX, proNX, and The Network You Need are trademarks or registered trademarks of Juniper Networks, Inc. and/or its subsidiaries in the U.S. and/or other countries.

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.

Copyright 2003-2016 BTI Systems, Inc. All rights reserved.

Copyright 1997-2001 Lumos Technologies Inc. All rights reserved.

Unpublished - All rights reserved under the copyright laws of the United States. This software is furnished under a license and use, duplication, disclosure and all other uses are restricted to the rights specified in the written license between the licensee and Lumos Technologies Inc.

Copyright 1998-2006 NuDesign Team Inc. All rights reserved. Copyright 1982-2001 QNX Software Systems Ltd. All rights reserved.

Copyright 1990-2001 Sleepycat Software. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. Redistributions in any form must be accompanied by information on how to obtain complete source code for the DB software and any accompanying software that uses the DB software. The source code must either be included in the distribution or be available for no more than the cost of distribution plus a nominal fee, and must be freely redistributable under reasonable conditions. For an executable file, complete source code means the source code for all modules it contains. It does not include source code for modules or files that typically accompany the major components of the operating system on which the executable file runs. THIS SOFTWARE IS PROVIDED BY SLEEPYCAT SOFTWARE "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT, ARE DISCLAIMED. IN NO EVENT SHALL SLEEPYCAT SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright 1990, 1993, 1994, 1995 The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR

CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright 1995, 1996 The President and Fellows of Harvard University. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED BY HARVARD AND ITS CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL HARVARD OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright 1998 The NetBSD Foundation, Inc. All rights reserved.

This code is derived from software contributed to The NetBSD Foundation by Christos Zoulas. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by the NetBSD Foundation, Inc. and its contributors. 4. Neither the name of The NetBSD Foundation nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED BY THE NETBSD FOUNDATION, INC. AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE FOUNDATION OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright 2003 Maxim Sobolev sobomax@FreeBSD.org. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT

SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright 1995,1996,1997,1998 Lars Fenneberg lf@elemental.net.

Permission to use, copy, modify, and distribute this software for any purpose and without fee is hereby granted, provided that this copyright and permission notice appear on all copies and supporting documentation, the name of Lars Fenneberg not be used in advertising or publicity pertaining to distribution of the program without specific prior permission, and notice be given in supporting documentation that copying and distribution is by permission of Lars Fenneberg. Lars Fenneberg makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

Copyright 1992 Livingston Enterprises, Inc. Livingston Enterprises, Inc. 6920 Koll Center Parkway Pleasanton, CA 94566.

Permission to use, copy, modify, and distribute this software for any purpose and without fee is hereby granted, provided that this copyright and permission notice appear on all copies and supporting documentation, the name of Livingston Enterprises, Inc. not be used in advertising or publicity pertaining to distribution of the program without specific prior permission, and notice be given in supporting documentation that copying and distribution is by permission of Livingston Enterprises, Inc. Livingston Enterprises, Inc. makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

The Regents of the University of Michigan and Merit Network, Inc. 1992, 1993, 1994, 1995. All Rights Reserved. Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies of the software and derivative works or modified versions thereof, and that both the copyright notice and this permission and disclaimer notice appear in supporting documentation. THIS SOFTWARE IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE REGENTS OF THE UNIVERSITY OF MICHIGAN AND MERIT NETWORK, INC. DO NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET LICENSEE'S REQUIREMENTS OR THAT OPERATION WILL BE UNINTERRUPTED OR ERROR FREE. The Regents of the University of Michigan and Merit Network, Inc. shall not be liable for any special, indirect, incidental or consequential damages with respect to any claim by Licensee or any third party arising from use of the software.

Copyright 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved.

License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function. License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work. RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind. These notices must be retained in any copies of any part of this documentation and/or software.

All other product and company names are trademarks or registered trademarks of their respective companies. All of the above-referenced components are not necessarily included in all versions of the product.

1.0 Transponder portfolio

This section identifies the Transponder modules that the BTI 7000 Series supports, and includes software release availability and operating temperature ranges.

- 1.1, “Transponder modules”
- 1.2, “Transponder module operating temperature ranges”

1.1 Transponder modules

Table 1-1 Transponders

Modules	PEC	System software introduced
Dual 2.5G Multiprotocol Transponders		
2.5G Wavelength Regenerator	BP1A42AA	7.1.0
2.5G Wavelength Manager	BP1A43AA	7.1.0
Dual 4G Multiprotocol Transponders		
Dual 4G Multiprotocol Transponder	BT7A41CA	7.2.0
10G Transponders		
Dual 10G Multiprotocol Transponder	BT7A49AA	7.1.0
	BT7A49AA-I02	10.4.1
Dual 10G Multiprotocol Transponder Lite	BT7A49AC	7.2.0
10G Multiprotocol Transponder	BT7A49AB	7.1.0

1.2 Transponder module operating temperature ranges

Table 1-2 Transponder module operating temperature ranges

Module	0°C to +40°C long term	-5°C to +50°C short term	-20°C to +65°C long term
2.5G Wavelength Manager	X	X	X
2.5G Wavelength Regenerator	X	X	X
Dual 4G Multiprotocol Transponder	X	X	
Dual 10G Multiprotocol Transponder	X	X	
Dual 10G Multiprotocol Transponder Lite	X	X	
10G Multiprotocol Transponder	X	X	

Note Short-term refers to a period of not more than 96 consecutive hours and a total of not more than 15 days during a 1-year period (as detailed in GR-63-CORE).

2.0 Transponder features and supported protocols

This section provides information about the features of the Transponder portfolio and the protocols each module supports.

- [2.1, “Dual 2.5G Multiprotocol Transponder features”](#)
- [2.2, “Dual 2.5G Multiprotocol Transponder supported protocols”](#)
- [2.3, “Dual 4G Multiprotocol Transponder features”](#)
- [2.4, “Dual 4G Multiprotocol Transponder supported protocols”](#)
- [2.5, “Dual 10G Multiprotocol Transponder features”](#)
- [2.6, “Dual 10G Multiprotocol Transponder supported protocols”](#)
- [2.7, “Dual 10G Multiprotocol Transponder Lite features”](#)
- [2.8, “Dual 10G Multiprotocol Transponder Lite supported protocols”](#)
- [2.9, “10G Multiprotocol Transponder features”](#)
- [2.10, “10G Multiprotocol Transponder supported protocols”](#)

2.1 Dual 2.5G Multiprotocol Transponder features

The Dual 2.5G Multiprotocol Transponder portfolio offers the following full-featured transponders:

Module	PEC
2.5G Wavelength Regenerator (2.5G WR)	BP1A42AA
2.5G Wavelength Manager (2.5G WM)	BP1A43AA

Features

- Module size: Single slot
- Supported platforms: BTI 7060, BTI 7030, BTI 7200
- Interfaces: 4
- Multiprotocol support. See [2.2, “Dual 2.5G Multiprotocol Transponder supported protocols”](#).
- Pluggable SFP transceivers, including copper SFPs, supported on all ports

Note Copper SFPs are supported only on 2.5G Wavelength Regenerator GE clients

- 850nm, 1310nm, 1550nm, CWDM, DWDM support
- Four optical ports for support of two bidirectional or four unidirectional signal paths
- 3R Regeneration with wavelength protection (2.5G WR only), and 4R reframe (2.5G WM only)
- Optical protection switching sub 50ms
- Client- and line-side loopback
- DWDM interface to any of 36 ITU grid wavelengths
- CWDM interface to all 16 ITU grid wavelengths
- Integrated performance monitoring (15-minute and 24-hour): Optical and Layer 1 PMs
- Extended temperature support (-20°C to +65°C)

2.5G Wavelength Regenerator



2.2 Dual 2.5G Multiprotocol Transponder supported protocols

The following tables list the protocols that are supported on ports on the following Dual 2.5G Multiprotocol Transponder ports, the bit rate at which each protocol operates, and the mapping strategy supported:

- 2.5G Wavelength Regenerator (2.5G WR) – BP1A42AA
- 2.5G Wavelength Manager (2.5G WM) – BP1A43AA

Table 2-1 2.5G Wavelength Regenerator supported protocols, bit rates, and mapping strategies

Protocol	Bit rate	Mapping strategy
OC3	155.52 Mbps	Transparent
OC12	622.08 Mbps	Transparent
OC48	2.488 Gbps	Transparent
OC48FEC	2.666 Gbps	Transparent
STM1	155.52 Mbps	Transparent
STM4	622.08 Mbps	Transparent
STM16	2.488 Gbps	Transparent
Fast Ethernet	125 Mbps	Transparent
Gigabit Ethernet	1.25 Gbps	Transparent
Fibre Channel 1G/FICON 1G	1.062 Gbps	Transparent
Fibre Channel 2G/FICON 2G	2.125 Gbps	Transparent
Fibre Distributed Data Interface (FDDI)	125 Mbps	Transparent
IBM Enterprise Systems Connection (ESCON)	200 Mbps	Transparent

Table 2-2 2.5G Wavelength Manager supported protocols, bit rates, and mapping strategies

Protocol	Bit rate	Mapping strategy
OC3	155.52 Mbps	Section Regen
OC12	622.08 Mbps	Section Regen
OC48	2.488 Gbps	Section Regen
Gigabit Ethernet	1.25 Gbps	Section Regen
STM16	2.488 Gbps	Section Regen

2.3 Dual 4G Multiprotocol Transponder features

The Dual 4G Multiprotocol Transponder (BT7A41CA) is a full-featured transponder.

Features

- Module size: Single slot
- Supported platforms: BTI 7060, BTI 7030 , BTI 7200
- Interfaces: 4
- Multiprotocol support. See [2.4, “Dual 4G Multiprotocol Transponder supported protocols”](#).
- Pluggable SFP transceivers, including copper SFPs, supported on all ports

Note Copper SFPs are supported on GE clients only

- Ethernet fault propagation
- 3R regeneration for all client types
- Automatic protection switching (APS) sub-50ms; APS based on fault detection, including Signal Degrade
- Client- and line-side loopback
- Integrated performance monitoring (15-minute and 24-hour): Physical layer, Ethernet, and FC.

Dual 4G Multiprotocol Transponder



2.4 Dual 4G Multiprotocol Transponder supported protocols

The following table lists the protocols that are supported on Dual 4G Multiprotocol Transponder (BT7A41CA) ports and the bit rate at which each protocol operates.

Table 2-3 Dual 4G Multiprotocol Transponder supported protocols, bit rates, and mapping strategies

Client protocol	Line protocol	Line bit rate	Line mapping
GE, FC1, FC2, FC4	GE	1.25 Gbps	Transparent
	FC1	1.0625 Gbps	Transparent
	FC2	2.125 Gbps	Transparent
	FC4	4.25 Gbps	Transparent

2.5 Dual 10G Multiprotocol Transponder features

BTI supports the Dual 10G Multiprotocol Transponder module (BT7A49AA and BT7A49AA-I02). The functional differences between the versions are listed below.

Features of BT7A49AA

- Module size: Single slot
- Supported platforms: BTI 7060, BTI 7030 , BTI 7200
- Interfaces: 4
- Multiprotocol line rate support. See [2.6, “Dual 10G Multiprotocol Transponder supported protocols”](#).
- XFP versatility, including support for tunable XFPs, and user initiated cold reboot
- Boosted transmission distances through FEC and EFEC
- Ethernet fault propagation
- 3R regeneration for all client types; 4R regeneration for SONET/SDH clients
- Automatic protection switching (APS) sub-50ms; APS based on fault detection, including Signal Degrade
- Embedded GCC0 management channel
- Client- and line-side loopback
- Single module line protection, and redundant module protection options
- Integrated performance monitoring (15-minute and 24-hour): Physical layer, SONET/SDH, Ethernet, and G.709 OTN

Features of BT7A49AA-I02

This version of the module includes all the features listed above, plus the following alarm and performance monitoring (PM) features. For more information about temperature and voltage monitoring refer to [2.5.1, “Module temperature monitoring ”](#) and [2.5.2, “Module voltage and fuse monitoring ”](#).

- Module temperature monitoring, including automatic shutdown if critical temperature is reached
- Module voltage rail and feed fuse monitoring
- PM collection of historical module temperature levels
- Support for 10GELANE/FEC EPV3 Regen

Dual 10G Multiprotocol Transponder



For a list of all the alarms supported on the Dual 10G Multiprotocol Transponder modules refer to [10.1.2, “Transponder module alarms”](#). For detailed information and clearing procedures for these alarms refer to the *BTI 7000 Series Alarm and Troubleshooting Guide*.

2.5.1 Module temperature monitoring

This section describes module-specific temperature monitoring.

Module temperature monitoring is supported on the following Transponder modules:

- Dual 10G Multiprotocol Transponder (BT7A49AA-I02)

Note	Temperature monitoring for modules is not the same as monitoring the temperature of individual pluggable SFPs and XFPs. Temperature monitoring for SFPs and XFPs is part of a port's physical performance metrics (PM).
-------------	---

Temperature thresholds

Temperature monitoring threshold crossing alarms have two levels. The first, high threshold, alerts you to rising temperatures so that you may take action to prevent traffic interruption. The second, shutdown threshold, indicates that module damage may occur. The shutdown temperature is likely to be reached only in case of total cooling unit failure.

For the Dual 10G Multiprotocol Transponder (BT7A49AA-I02) module, the high and shutdown thresholds are 75°C and 80°C respectively.

The threshold values can be viewed in the module inventory. They cannot be changed.

Automatic shutdown

If automatic shutdown is enabled (through the use of the system setting HTAS), then if the shutdown threshold is exceeded, the module is shut down to avoid damage.

The HTAS setting is off by default.

When a module has been shut down due to temperature, the REPLUNITHATS alarm is raised.

Temperature is not monitored while a module is shut down. You can start up a module that has been shut down due to temperature by using the `TL1 INIT-SYS` command with the phase 2 power-on option. Alternatively, the module can be re-seated.

Temperature PMs

The module temperature can be viewed under equipment PMs (`rtrv-pm-eqpt`).

Temperature PMs provide the current and historical temperature readings.

To view PMs, the module must be provisioned.

High temperature automatic shutdown unsupported (HTASUNS) alarm

The high temperature automatic shutdown (HTAS) feature is not supported by all versions of the MSI. In the case of an incompatible MSI, the HTASUNS alarm is raised. To clear the alarm, you can either disable the HTAS feature, or you can replace the MSI with a compatible version. To obtain a compatible MSI, contact your BTI representative.

Temperature monitoring alarms

The following table lists the alarms associated with monitoring the module temperature. For more information about these alarms and alarm clearing procedures, refer to the *BTI 7000 Series Alarm and Troubleshooting Guide*:

Alarm Code	Alarm Name	Problem Description
HTASUNS	High Temperature Automatic Shutdown Unsupported	The HTAS option has been enabled, but the system is not able to support the feature.
REPLUNITHTAS	Circuit Pack High Temperature Automatic Shutdown	The module has exceeded the shutdown temperature threshold and has been shut down because the HTAS feature is enabled.
T-REPLUNIT-HT	Circuit pack exceeded the high temperature threshold.	The module has exceeded the high temperature threshold.
T-REPLUNIT-HTS	Circuit pack exceeded the shutdown temperature threshold.	The module has exceeded the shutdown temperature threshold.

Commands used for module temperature monitoring

This section lists the TL1 commands used for monitoring module temperature. For more information about these commands, refer to the *BTI 7000 Series TL1 Reference Guide*.

Command type	Command	Description
TL1	ED-SYS:BTI7000:: [CTAG]:HTAS=[ON OFF]	Turns the HTAS feature on or off. The default is OFF.
TL1	RTRV-INV: [TID]:[<aid>]:[CTAG]::;	Displays the module high temperature threshold (TEMPHT) and the module high shutdown temperature threshold (TEMPHTS) in degrees Celcius.
TL1	INIT-SYS: [TID]:[<aid>]:[CTAG]::[<2>]:	Restarts the module following a temperature shutdown. The value of the phase parameter is 2.
TL1	RTRV-ALM-ALL: [TID]:[<aid>]:[CTAG]:: [<ntfcncde>], [<condtype>], [<srveff>], [<locn>], [<dirn>], [<tmper>];	Displays all alarms, including the module temperature alarms and severity for the specified condition type (HTASUNS, REPLUNITHTAS, T-REPLUNIT-HT, T-REPLUNIT-HTS).

2.5.2 Module voltage and fuse monitoring

This section describes module-specific voltage and fuse monitoring.

Module voltage and fuse monitoring is supported on the following Transponder modules:

- Dual 10G Multiprotocol Transponder (BT7A49AA-I02)

Voltage monitoring

All supply voltage rails on the module are monitored. If any rail falls below nominal voltage by a preset amount, the module is shut down.

When the module is shut down due to a voltage rail failure, the REPLUNITPWR alarm is raised.

Fuse monitoring

The two 48V feed fuses on the module are monitored. If either of the fuses fails, a feed fuse alarm is raised.

Module operation is not affected if only one fuse fails, unless the system feed for the other side also fails.

A feed fuse alarm indicates that the module should be replaced as soon as possible.

Voltage and fuse monitoring alarms

The following table lists the alarms associated with monitoring the module voltage and fuses. For more information about these alarms and alarm clearing procedures, refer to the *BTI 7000 Series Alarm and Troubleshooting Guide*:

Alarm Code	Alarm Name	Problem Description
FEEDAFUSEFAIL	Circuit pack feed A fuse failure.	The module's fuse for the 48V feed A has failed.
FEEDBFUSEFAIL	Circuit pack feed B fuse failure.	The module's fuse for the 48V feed B has failed.
REPLUNITPWR	Circuit pack power failure.	A voltage rail failure was detected on the module.

Commands used for module voltage monitoring

This section lists the TL1 commands used for monitoring module voltage and fuses. For more information about these commands, refer to the *BTI 7000 Series TL1 Reference Guide*.

Command type	Command	Description
TL1	RTRV-ALM-EQPT : [TID] : [<aid>] : [CTAG] :: [FEEDAFUSEFAIL FEEDBFUSEFAIL REPLUNITPWR]	Displays the module voltage alarms and severity for the specified condition type.

2.6 Dual 10G Multiprotocol Transponder supported protocols

The following table lists the protocols that are supported on Dual 10G Multiprotocol Transponder (BT7A49AA and BT7A49AA-I02) ports and the bit rate at which each protocol operates.

Table 2-4 Dual 10G Multiprotocol Transponder supported protocols, bit rates, and mapping strategies

Client protocol	Line protocol	Line bit rate	Line mapping
10GELAN	10GELAN	10.313 Gbps	Transparent
10GELAN	10GELANFEC/EFEC	10.709 Gbps	Semi-transparent G.709 OTN mapping ¹
10GELAN	10GELANFEC/EFEC EPCMF	10.709 Gbps	Semi-transparent G.709 OTN mapping ²
10GELANFEC/EFEC	10GELANFEC/EFEC	10.709 Gbps	Transparent (OTN mapping, OTU regeneration)
10GELANFEC/EFEC EPCMF	10GELANFEC/EFEC EPCMF	10.709 Gbps	Transparent (OTN mapping, OTU regeneration)
10GELAN	OTU2e FEC/EFEC	11.095 Gbps	Transparent (OTN mapping, OTU regeneration)
10GELANFEC/EFEC EPV3	10GELANFEC/EFEC EPV3	10.709 Gbps	Transparent (OTN mapping, OTU regeneration)
Note This protocol is supported only on the BT7A49AA-102.	Note This protocol is supported only on the BT7A49AA-102.		
10GELAN	OTU2EPV3 FEC/EFEC	10.709 Gbps	Transparent (OTN mapping, OTU regeneration)
10GFC	10GFC	10.519 Gbps	Transparent
OC192	OC192	9.953 Gbps	SONET Section regeneration
OC192	OC192FEC/EFEC	10.709 Gbps	SONET Section regeneration (OTN mapping)
OC192FEC	OC192FEC	10.709 Gbps	Transparent (OTN mapping, OTU regeneration)
STM64	STM64	9.953 Gbps	SDH Section regeneration
STM64	STM64FEC/EFEC	10.709 Gbps	SDH Section regeneration (OTN mapping)

Table 2-4 Dual 10G Multiprotocol Transponder supported protocols, bit rates, and mapping strategies (Continued)

Client protocol	Line protocol	Line bit rate	Line mapping
STM64FEC	STM64FEC	10.709 Gbps	Transparent (OTN mapping, OTU regeneration)
ODU1OTU2FEC	ODU1OTU2FEC	10.709 Gbps	Transparent (OTN mapping, OTU regeneration)
OTU2eFEC/EFEC	OTU2eFEC/EFEC	11.095 Gbps	Transparent (OTN mapping, OTU regeneration)

¹Interframe Gap Frames that do not contain a Remote Fault Message are discarded. A client fault will generate a downstream remote fault. The 10G LAN frames are inspected and any errored frame is dropped from the stream

²Interframe Gap Frames that do not contain a Local Fault or Remote Fault Message are discarded. A client fault will generate a downstream local fault. The 10G LAN frames are inspected and any errored frame is dropped from the stream

2.7 Dual 10G Multiprotocol Transponder Lite features

The Dual 10G Multiprotocol Transponder Lite (BT7A49AC) is a transponder that offers a subset of the features of the Dual 10G Multiprotocol Transponder (BT7A49AA).

Features

- Module size: Single slot
- Supported platforms: BTI 7060, BTI 7030, BTI 7200
- Interfaces: 4
- Multiprotocol and line rate support. See [2.8, “Dual 10G Multiprotocol Transponder Lite supported protocols”](#).
- XFP versatility, including support for tunable XFPs, and user initiated cold reboot
- Ethernet fault propagation
- 2R regeneration for all client types (no re-framing)
- Automatic protection switching (APS) sub-50ms; APS based on LOS
- Client- and line-side loopback
- Integrated physical layer performance monitoring (15-minute and 24-hour)

Dual 10G Multiprotocol Transponder Lite



2.8 Dual 10G Multiprotocol Transponder Lite supported protocols

The following table lists the protocols that are supported on Dual 10G Multiprotocol Transponder Lite (BT7A49AC) ports and the bit rate at which each protocol operates. The Dual 10G Multiprotocol Transponder Lite module does not allow protocol conversion between client and line ports.

Table 2-5 Dual 10G Multiprotocol Transponder Lite supported protocols, bit rates, and mapping strategies

Client protocol	Line protocol	Line bit rate	Line mapping
10GFC	10GFC	10.519 Gbps	Transparent
10GELAN	10GELAN	10.313 Gbps	Transparent
10GELANFEC	10GELANFEC	10.709 Gbps	Transparent
10GELANEFEC	10GELANEFEC	10.709 Gbps	Transparent
10GELANFEC EPCMF	10GELANFEC EPCMF	10.709 Gbps	Transparent
10GELANEFEC EPCMF	10GELANEFEC EPCMF	10.709 Gbps	Transparent
OC192	OC192	9.953 Gbps	Transparent
OC192FEC	OC192FEC	10.709 Gbps	Transparent
OC192EFEC	OC192EFEC	10.709 Gbps	Transparent
STM64	STM64	9.953 Gbps	Transparent
STM64FEC	STM64FEC	10.709 Gbps	Transparent
STM64EFEC	STM64EFEC	10.709 Gbps	Transparent
ODU1OTU2FEC	ODU1OTU2FEC	10.709 Gbps	Transparent
OTU2eFEC	OTU2eFEC	11.095 Gbps	Transparent
OTU2eEFEC	OTU2eEFEC	11.095 Gbps	Transparent

2.9 10G Multiprotocol Transponder features

The 10G Multiprotocol Transponder (BT7A49AB) is a full-featured Transponder.

Features

- Module size: Single slot
- Supported platforms: BTI 7060, BTI 7030 , BTI 7200
- Interfaces: 2
- Multiprotocol and line support. See [2.10, “10G Multiprotocol Transponder supported protocols”](#).
- XFPs: Pluggable XFP transceiver on all ports. Tunable XFPs. User initiated reboot.
- Boosted transmission distances via FEC and EFEC
- Ethernet fault propagation
- 3R regeneration for all client types; 4R regeneration for SONET/SDH clients
- Embedded GCC0 management channel
- Client- and line-side loopback
- Optional redundant module protection (does not support single module protection)
- Integrated performance monitoring (15-minute and 24-hour): Physical layer, SONET/SDH, Ethernet, and G.709 OTN (OTU2 and OTU2e)

Figure 2-5 10G Multiprotocol Transponder



2.10 10G Multiprotocol Transponder supported protocols

The following table lists the protocols that are supported on 10G Multiprotocol Transponder (BT7A49AB) ports, the bit rate at which each protocol operates, and the mapping strategy supported.

Table 2-6 10G Multiprotocol Transponder supported protocols, bit rates, and mapping strategies

Client protocol strategy	Line protocol	Line bit rate	Line mapping
10GELAN	10GELAN	10.313 Gbps	Transparent
10GELAN	10GELANFEC/EFEC	10.709 Gbps	Semi-transparent G.709 OTN mapping ¹
10GELAN	10GELANFEC/EFEC EPCMF	10.709 Gbps	Semi-transparent G.709 OTN mapping ²
10GELANFEC	10GELANFEC	10.709	Transparent (OTN mapping, OTU regeneration)
10GELANFEC/EFEC EPCMF	10GELANFEC/EFEC EPCMF	10.709 Gbps	Transparent (OTN mapping, OTU regeneration)
10GFC	10GFC	10.519 Gbps	Transparent
OC192	OC192	9.953 Gbps	SONET Section regeneration
OC192	OC192FEC/EFEC	10.709 Gbps	SONET Section regeneration (OTN mapping)
OC192FEC	OC192FEC	10.709 Gbps	Transparent (OTN mapping, OTU regeneration)
STM64	STM64	9.953 Gbps	SDH Section regeneration
STM64	STM64FEC/EFEC	10.709 Gbps	SDH Section regeneration (OTN mapping)
STM64FEC	STM64FEC	10.709 Gbps	Transparent (OTN mapping, OTU regeneration)
ODU1OTU2FEC	ODU1OTU2FEC	10.709 Gbps	Transparent (OTN mapping, OTU regeneration)
OTU2eFEC/EFEC	OTU2eFEC/EFEC	11.095 Gbps	Transparent (OTN mapping, OTU regeneration)

¹Interframe Gap Frames that do not contain a Remote Fault Message are discarded. A client fault will generate a downstream remote fault. The 10G LAN frames are inspected and any errored frame is dropped from the stream

²Interframe Gap Frames that do not contain a Local Fault or Remote Fault Message are discarded. A client fault will generate a downstream local fault. The 10G LAN frames are inspected and any errored frame is dropped from the stream

3.0 Transponder applications

This section provides information about the applications that Transponder modules support.

- [3.1, “Reach extension”](#)
- [3.2, “Private Line connectivity”](#)

3.1 Reach extension

Ethernet, SONET, SDH and FC reach extension

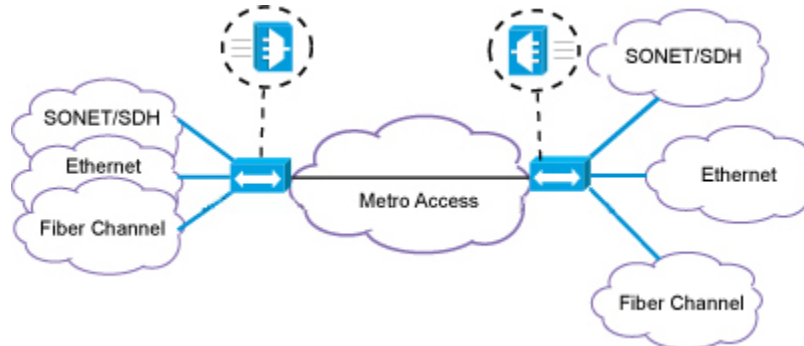
Transponders can provide Optical-Electrical-Optical (OEO) conversion to extend the reach of Ethernet, SONET, SDH, and FC protocols and regenerate optical signals in three domains: power, shape, and time.

Transponders provide in-line regeneration where the physical distance between the source and destination nodes of the optical system exceeds the maximum transmission reach.

Transponder modules can be either collocated with terminal equipment or deployed at intermediate line sites. When a Transponder module is collocated with terminal equipment, it accepts limited-reach 850nm or 1310nm signals and converts them to extended-reach 1550nm or DWDM wavelengths. When deployed at an intermediate line site, the Transponder module can accept and regenerate two bidirectional 1550nm or DWDM wavelengths.

When used to extend the reach of 10GELAN, OC192, and STM64 signals, the Transponder module accepts client interface ports from a router, SONET/SDH ADM or any other terminal device at 850nm, 1310nm, or 1550nm. The signal is regenerated and can be transmitted up to 80km over an optical link, without external amplifiers. With the addition of optical amplifier modules and dispersion compensation modules, signals can be transmitted up to 160km without an intermediate site.

Reach extension

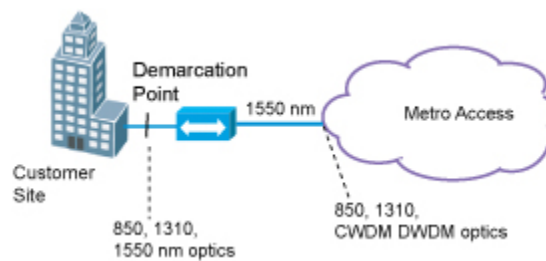


3.2 Private Line connectivity

Transponder modules can be used to provide demarcation of wholesale and enterprise Private Line services. The service interface can be at 850nm, 1310nm, or 1550nm. Client- and line-side loopback provides the ability to isolate the service to the customer boundary during provisioning and fault isolation. Performance monitoring provides measurement to Service Level Agreements (SLAs).

Transponder modules can be deployed on their own or in combination with DWDM multiplexers or amplifiers to extend the service over the fiber network.

Private Line connectivity



4.0 Installing Transponder modules, SFPs, and XFPs

This section provides instructions for installing Transponder modules in supported shelves, and installing SFPs and XFPs in Transponder modules.

- [4.1, “Installing Transponder modules”](#)
- [4.2, “Installing optical transceivers”](#)
- [4.3, “Installing copper transceivers”](#)

4.1 Installing Transponder modules

Use this procedure to install any BTI 7000 Series Transponder module.

What you need

- Slot-head or Phillips screwdriver
- Electrostatic discharge (ESD) wrist strap
- Transponder module
- SFP or XFP transceivers
- Isopropyl alcohol and lint-free pads

Prerequisites



Caution

Use an ESD wrist strap whenever you open the equipment, particularly when you are handling modules as well as SFP and XFP transceivers. To work properly, the wrist strap must make good contact at both ends (that is, with your skin at one end and with the chassis at the other).



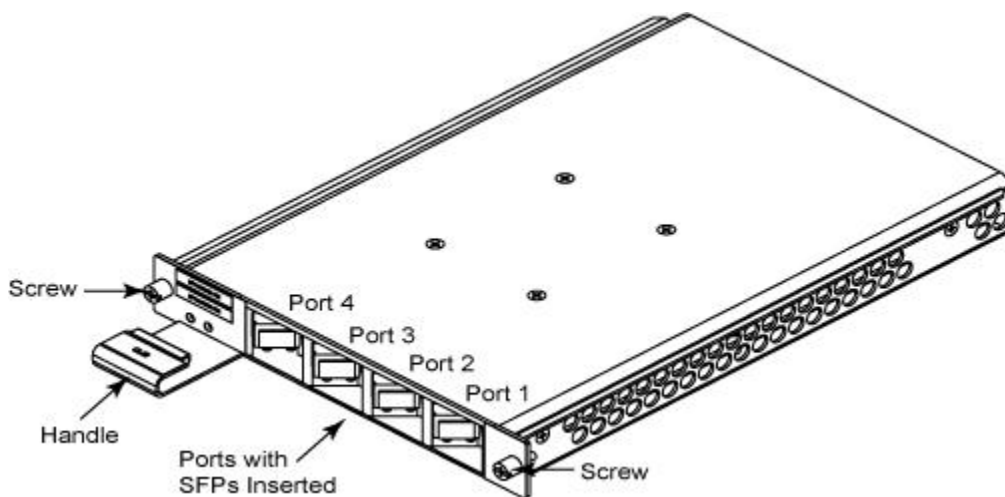
Laser

Invisible laser radiation can be emitted from the aperture ports of various modules when no fiber cable is connected. Avoid exposure and do not stare into open apertures to avoid permanent eye damage.

Key installation features

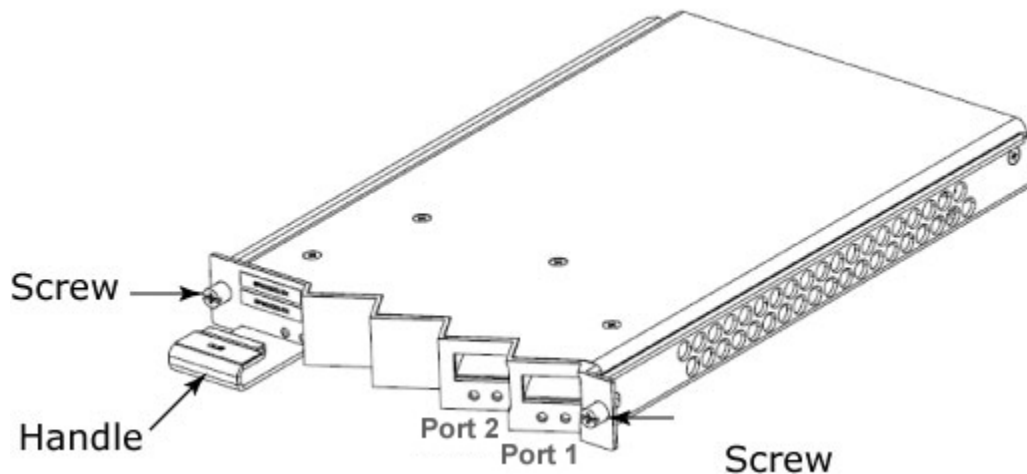
The following figures show Transponder modules and indicate the key features for installing them.

Dual 1G and Dual 2.5G Multiprotocol Transponder modules



Note The following image shows a 10G Multiprotocol Transponder module, but, with the exception of the number of ports, is representative of the Dual 4G Multiprotocol Transponder, the Dual 10G Multiprotocol Transponder, and the Dual 10G Multiprotocol Transponder Lite modules as well.

10G Multiprotocol Transponder module



Installation procedure

Follow these steps to install a Transponder module:

Step 1 Insert the Transponder Module

- a) Align the module to the slot in which it is being inserted.
- b) Carefully push the module straight into the slot.
- c) Push with sufficient pressure until the LEDs come on and the faceplate of the module matches the position of the adjacent module.

Step 2 Attach the Faceplate Screws

- a) Facing the front of the shelf, align the module with its mounting holes.
- b) Using a slot-head or Phillips screwdriver, carefully tighten the two faceplate screws:
 - Partially tighten the center support screw.
 - Partially tighten the other screw.
 - Fully tighten the center support screw.
 - Fully tighten the other screw.

Caution Tighten to a torque that is no more than 4.7 in-lbs.

Step 3 Install the Transceivers

See [4.2, “Installing optical transceivers”](#) for information about installing transceivers, and then return to this procedure

Step 4 Replace the Cables

If any cables were moved to access the module, replace the cables to their original locations.

You have successfully completed this procedure.

4.2 Installing optical transceivers

Use this procedure to install optical small form factor (SFP) or 10 Gb/s (XFP) transceivers.

What you need

- Electrostatic discharge (ESD) wrist strap
- SFP or XFP transceiver
- Isopropyl alcohol and lint-free pads

Prerequisites

To prevent potential damage from electrostatic discharge, observe the following when handling transceivers:

- Do not remove a transceiver from its packaging until you are ready to install it into a module.
- Do not touch any of the pins, connections, or components of a transceiver.
- Always store or transport a transceiver in anti-static packaging.



Caution

Use an ESD wrist strap whenever you open the equipment, particularly when you are handling modules as well as SFP and XFP transceivers. To work properly, the wrist strap must make good contact at both ends (that is, with your skin at one end and with the chassis at the other).



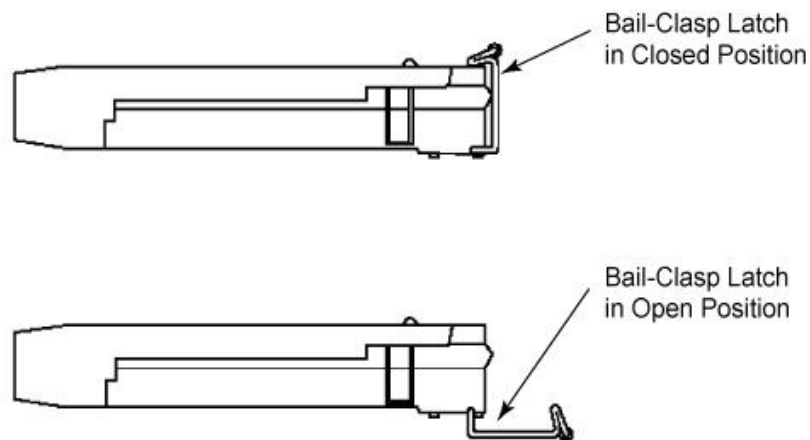
Laser

Invisible laser radiation can be emitted from the aperture ports of various modules when no fiber cable is connected. Avoid exposure and do not stare into open apertures to avoid permanent eye damage.

Transceiver key features

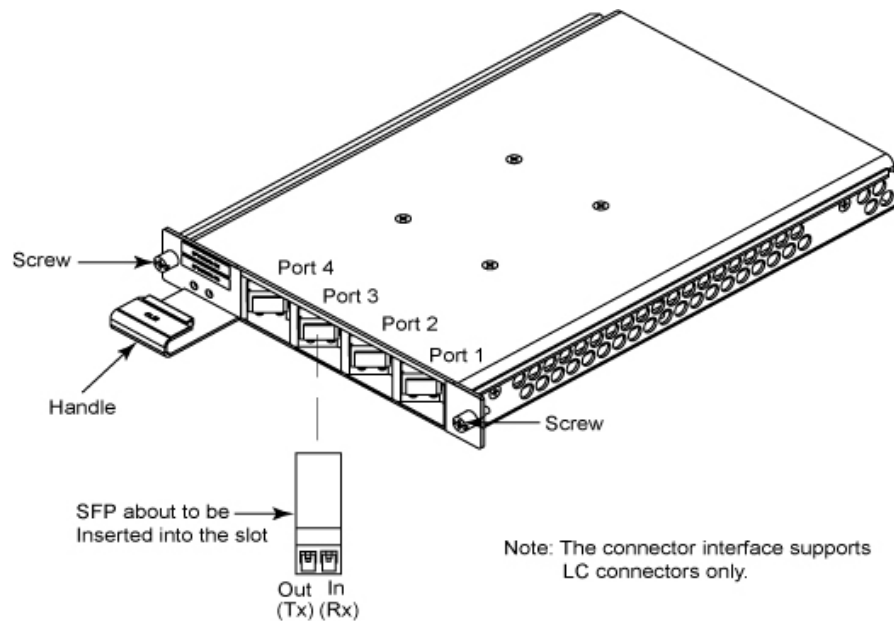
The following figure shows a typical SFP transceiver with a bail-clasp latch.

Figure 4-3 SFP transceiver with a bail-clasp latch



The following figure shows a transceiver about to be inserted into its slot.

Figure 4-4 Transceiver insertion in a generic module



Installation procedure

Step 1 Insert the Transceiver

Note Never insert a transceiver that already has a fiber connected to it. Always fully insert the transceiver first, and then connect the fiber to it.

- a) Hold the transceiver so that the optical connectors face you. On an SFP, the product label is visible. On an XFP, the product label is not visible.
- b) Ensure that the latch is in the closed position.
- c) Align the transceiver to the port in which it is being inserted.
- d) Carefully slide the transceiver straight into the port until it clicks.
 - If the red Fail LED turns on, there is a transceiver fault. To clear the fault, refer to the *Alarm and Troubleshooting Guide*.
 - If the yellow LOS LED turns on, there is no valid modulated signal connected to the transceiver. This condition clears once a valid modulated signal is connected.
- e) Remove the plastic protective cover, if fitted.

Step 2 Clean the Ends of the Fiber Optic Cables

Use lint-free pads with isopropyl alcohol to clean the ends of the fiber optic cables.

Step 3 Connect the Input and Output Optical Cables

Note Before connecting the optical cables to the transceiver, ensure that both the optical cable connectors and the transceiver optical surfaces are clean and that there is no residue on the optical surfaces.

Note The input, or receiver, is on the right side of the transceiver. The output, or transmitter, is on the left side of the transceiver.

- a) Ensure that the latch of the transceiver is in the closed position.
- b) Carefully slide the bottom of the male optical connector along the bottom of the transceiver opening.
- c) Gently push the male optical connector into the transceiver until a distinctive click is heard. Then continue exerting pressure on the connector to ensure a good connection is achieved.

Note A Loss of Signal (LOS) alarm can occur when no coherent modulated signal is connected to the transceiver. To clear an LOS alarm, see the *Alarm and Troubleshooting Guide*.

Important XFPs and DWDM SFPs take about 90 seconds to reach a stable operating temperature. As a result, the REPLUNITFAIL (XFP or SFP Failure) alarm is disabled for 95 seconds after the transceiver is seated. If there is a hardware fault, the REPLUNITFAIL alarm is raised after the 95-second time delay. For more information, see the *Alarm and Troubleshooting Guide*.

You have successfully completed this procedure.

4.3 Installing copper transceivers

Use this procedure to install a copper small form factor (SFP) transceiver with an RJ45 connector.

What you need

- Electrostatic discharge (ESD) wrist strap
- Copper SFP transceiver

Prerequisites

To prevent potential damage from electrostatic discharge, observe the following when handling transceivers:

- Do not remove a transceiver from its packaging until you are ready to install it into a module.
- Do not touch any of the pins, connections, or components of a transceiver.
- Always store or transport a transceiver in anti-static packaging.



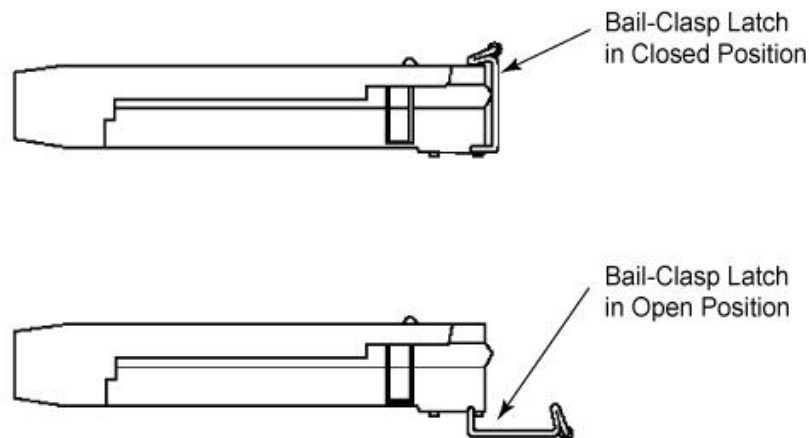
Caution

Use an ESD wrist strap whenever you open the equipment, particularly when you are handling modules as well as SFP and XFP transceivers. To work properly, the wrist strap must make good contact at both ends (that is, with your skin at one end and with the chassis at the other).

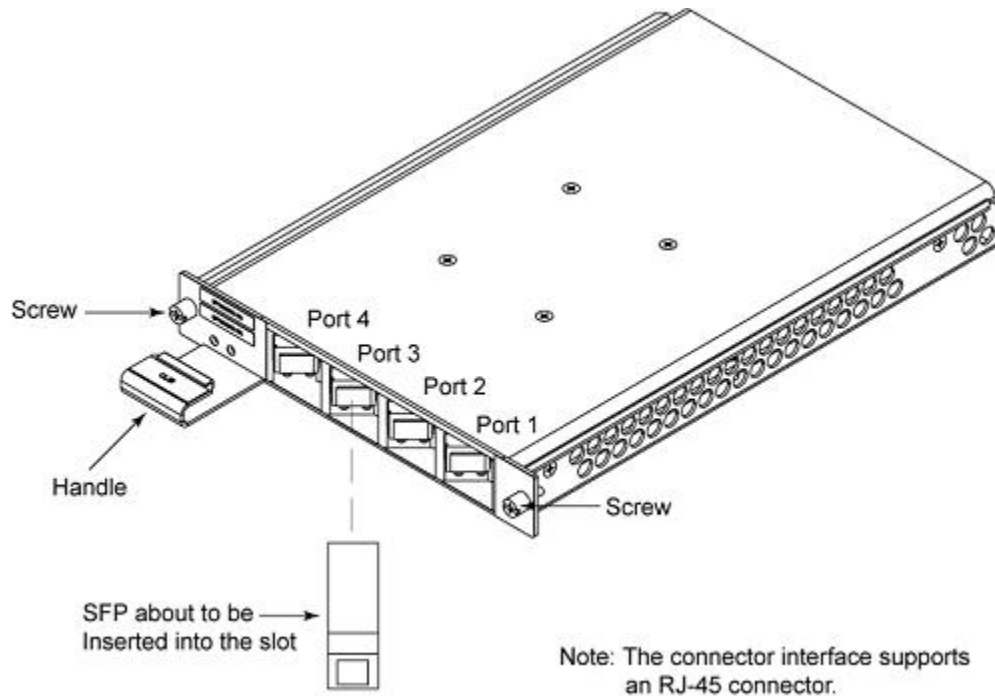
Transceiver key features

The following figure shows a typical SFP transceiver with a bail-clasp latch.

Figure 4-5 SFP transceiver with a bail-clasp latch



The following figure shows a transceiver about to be inserted into its slot.

Figure 4-6 Transceiver insertion in a generic module**Installation procedure**

Note The maximum cable length (CAT5 UTP) is 100 m.

Follow these steps to install a copper SFP transceiver:

Step 1 Insert the Transceiver

Note Never insert a transceiver that already has a CAT5 cable connected to it. Always fully insert the transceiver first, and then connect the CAT5 cable to it.

- a) Hold the transceiver so that the electrical RJ45 connector faces you. On an SFP, the product label is visible.
- b) Ensure that the latch is in the closed position.
- c) Align the transceiver to the port in which it is being inserted.
- d) Carefully slide the transceiver straight into the port until it clicks.
 - If the red Fail LED turns on, there is a transceiver fault. To clear the fault, refer to the *Alarm and Troubleshooting Guide*.
- e) Remove the plastic protective cover, if fitted.

Step 2 Connect an RJ45 cable to each copper SFP transceiver.

Connect an RJ45 cable to each copper SFP transceiver as follows:

- a)** Ensure that the latch of the SFP transceiver is in the closed position
- b)** Push the RJ45 connector into the SFP transceiver until a distinctive click is heard.

Note A Link Down alarm can occur when no signal is connected to the transceiver. To clear a Link Down alarm, refer to the *Alarm and Troubleshooting Guide*.

You have successfully completed this procedure.

5.0 Management interfaces

This section provides a brief overview about each management interface you can use to provision, monitor, and administer Transponder modules.

- [5.1, “proNX 900 Node Controller, CLI, TL1, SNMP, and proNX Service Manager”](#)

5.1 proNX 900 Node Controller, CLI, TL1, SNMP, and proNX Service Manager

proNX 900 Node Controller

proNX 900 Node Controller (proNX 900) provides a graphical user interface you can use to provision, operate, monitor, and troubleshoot all BTI 7000 Series modules. This interface provides a representational view of the physical configuration of each shelf in the network, and the modules in each shelf. For information about using the proNX 900 Node Controller, see the *proNX 900 Node Controller Online Help*.

CLI

The CLI is used to configure, monitor, and maintain packetVX and other modules. The CLI does not support all BTI 7000 Series modules. For information about using CLI commands, see the *CLI Reference Guide*.

TL1

The BTI 7000 Series supports a comprehensive and interactive Transaction Language One (TL1) interface, based on Telcordia standards, including GR-831, GR-199-CORE, and GR-833-Core. For information about using TL1 commands to provision, monitor, and administer BTI 7000 Series modules, see the *TL1 Reference Guide*.

SNMP

The BTI SNMP implementation supports SNMP Version 1 (SNMPv1) as defined in RFCs 1155, 1157, 1212, 1213, and 1215. The SNMP implementation also supports SNMPv2c as defined in RFCs 1901 through 1907. For information about the BTI SNMP implementation, see the *SNMP Overview Guide*.

proNX Service Manager

The proNX Service Manager provides proactive, service-centric management of network resources using tools closely aligned with service providers' own business processes. It is designed to simplify network operations from visualization and activation of services to troubleshooting and supporting end customers. For more information, see the *proNX Service Manager User Guide*.

6.0 Transponder protection architectures

This section describes the protection support on BTI Transponder modules, and includes the following sections:

- 6.1, “Unprotected Wide Area Network (WAN) connectivity”
- 6.2, “Line or WAN protection”
- 6.3, “Client protection”

6.1 Unprotected Wide Area Network (WAN) connectivity

- Architecture providing transmission of a non-resilient client signal between client equipment
- Can be provided by a pair of Transponder modules for a single client signal, or by a Dual Transponder module for two independent clients.
- Failure of client equipment, or a client or line port, or loss of WAN physical connectivity (for example, as a result of a fiber cut) causes the connection to fail

Architecture providing unprotected WAN connectivity



6.2 Line or WAN protection

- Protection architecture providing resilient transmission of a client signal between client equipment
- Integrated bridging of a single client equipment signal to both line ports of a Dual Transponder module provides protection in the event of a loss of a line port or loss of WAN physical connectivity
- Protection switching is based on multiple performance-monitoring parameters (i.e., client-equipment dependent). For information, see 7.1, “[Protection switching severity levels](#)”.
- Provides 50ms protection switching based on tail-end switching between redundant WAN signals
- Requires a Dual Transponder module with protection switching (e.g., 1G Wavelength Regenerator, 2.5G Wavelength Regenerator, Dual 2.5G Multiprotocol Transponder, Dual 4G Multiprotocol Transponder, Dual 10G Multiprotocol Transponder, or Dual 10G Multiprotocol Transponder Lite)
- Line protection is not supported at the same time as client protection on the same Transponder module.
- Line protection can be unidirectional or bidirectional for BT7A49AA-IO2 modules, depending on configuration. Line protection is unidirectional for all other transponder modules.
 - Unidirectional means that the protection switch decision at one end is independent of the protection switch decision at the other end. The transponder at one end can choose one path as its working path, while the transponder at the other end can choose the other path as its working path.
 - Bidirectional means that the protection switch decisions at both ends are matched. Both transponders choose the same path as their working path.

Architecture providing line or WAN protection



6.3 Client protection

The BTI 7000 Series provides full client-interface equipment redundancy between the client equipment and two separate BTI 10G Transponder modules: Dual 10G Multiprotocol Transponder—BT7A49AA and BT7A49AA-I02 or 10G Multiprotocol Transponder — BT7A49AB, using a combination of a Y-cable component and redundant transponder.

The Y-cable is a 50/50 passive optical splitter device that supports the following, client side XFP interfaces:

- 1310 nm SR: BP3AM4MS
- 1550 nm IR: BP3AM4LI

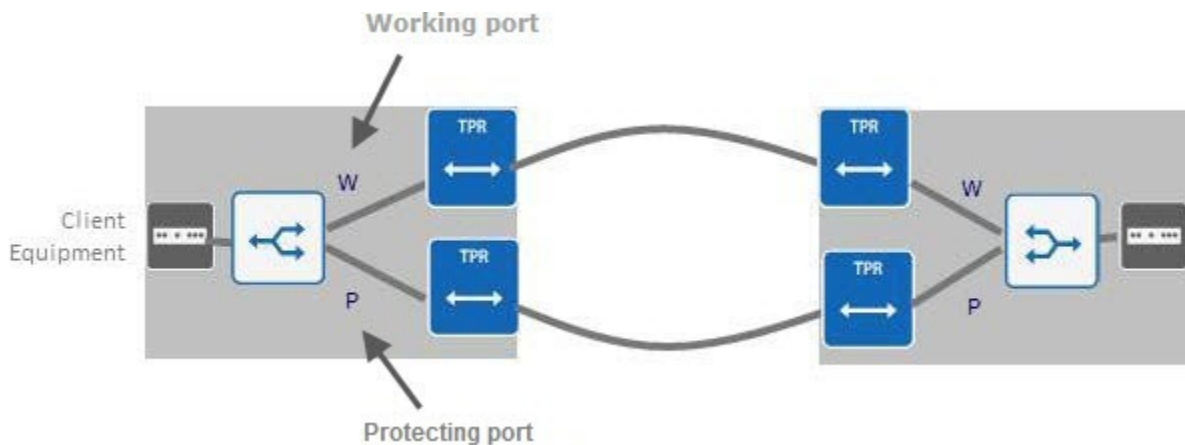
The client ports of each of the transponders are connected by two Y-cable pairs—BT7A57AA:

- One of the Y-cable connectors (combiner end) is terminated onto the CPE transmitter, and the dual cable end (splitter side) terminates to the receiving client port of both the working and protection transponder modules.
- The second Y-cable connector (combiner end) is terminated onto the CPE receiver, and the dual cable end (splitter side) terminates to the transmitting client port of both the working and protection transponder modules.

One client is active (working) and transmits toward the CPE. The other client transmitter (standby) is disabled. Both active and standby clients receive from the CPE. The associated line side port on each module is actively transmitting and receiving. When a fault is detected on the working port, the working port transmitter is automatically turned off and the system switches the transmission to the protecting port. The transmitter on the protecting port turns on, and the port becomes the working client port.

The following example shows a Y-cable set up. The two ports—working and protecting—connected to the transponders make up the protection group. The protection group monitors the optical, OTN and client signal layers on the receiving end.

Figure 6-3 Y-cable client protection set-up



Note Client protection switching is always bidirectional. The transponders at both ends choose the same path as the working path.

6.3.1 Client protection set-up considerations

Following are guidelines that must be considered, before the client equipment is connected to the transponder modules:

- The client ports must be connected to the same transponder module types.
- Client protection cannot be provisioned on a module that is provisioned for line protection.
- When client protection is provisioned, the laser status control must be configured to allow software to control the laser status.
- Protection on ports 1, 2 is independent of ports 3, 4. (Normally, ports 1 and 2 support a single unprotected optical service supporting one client, and ports 3 and 4 support a second optical service supporting a second client.)
- When client protection is provisioned on port 1, 2, ports 3, 4 may be unprotected.
- When using client protection on 1, 2 and 3, 4 the ports must be paired to the protection module in the same matching order.
- Ports 1, 2 on one module cannot be paired to ports 3, 4 on the second module.

Note For additional connection details, refer to "Y-cable for client protection" in the *BTI 7000 Series Common Equipment Installation Guide*.

Software upgrade considerations

Software upgrades on Transponder modules in a client protection group are hitless.

6.3.2 Restarting Transponder modules in a client protection group

The following considerations apply when performing a warm or cold restart on Transponder modules that are members of a client protection group:

Warm restarts

A warm restart of a transponder may be initiated by the user or the upgrade process:

- A warm restart of the working or protecting transponder temporarily disables the fault monitoring of the transceiver ports on the restarted transponder, and disables protection switching.
- The laser on the working client port remains on during the restart. Traffic on this port is not affected.
- The laser on the protecting client port remains off during the restart. Traffic on the working port is not affected.

Cold restarts

A cold restart of a transponder may be initiated by the user, by re-seating the module, or initiated by power cycling the shelf:

- A user-initiated cold restart of the transponder carrying the working client port causes an automatic protection switch to the protecting client port, if it is not locked out or in Out-of-service (OOS) maintenance state. Note that the restart must be performed in the forced (FRCD) command mode.
- A user-initiated cold restart of a transponder carrying the protecting client port is allowed. Note, however, that this type of restart causes a traffic hit—few seconds—on the working client port.

Note To prevent a traffic hit on the working port, use the following procedure to cold restart the transponder carrying the protecting client port.

- 1 Place the transponder in standby mode. It should not be passing traffic.
- 2 Disconnect the y-cable from the transponder carrying the protecting client port, and remove the transponder.

Note If you are performing the restart remotely, verify that the y-cable is disconnected.

- 3 Install the replacement transponder.
- 4 Once the transponder completes booting, reconnect the y-cable.

7.0 Protection switching on Transponder modules

Protection switching is supported for line and client protection groups. Both automatic and manual switching are supported.

For information on line protection switching refer to [7.2, “Protection switching for line protection”](#).

For information on client protection switching refer to [7.3, “Protection switching for client protection ”](#).

7.1 Protection switching severity levels

For the purposes of protection switching, there are two severity levels relevant to input facility faults. They are, in increasing severity:

- Signal Degrade (SD)
- Signal Fail (SF)

When a Signal Degrade is detected on a facility with the administrative state of in-service, it is given a secondary state of abnormal (ANR). When a signal fail is detected on a facility, it is set to the administrative state of OOS-AU.

The following table lists the conditions that result in an Signal Degrade and Signal Fail for the supported protocol types.

Table 7-1 Protection conditions that cause Signal Degrade and Signal Fail faults

Protocols	Signal Degrade	Signal Fail
OC3/STM1, OC12/STM4, OC48/STM16, OC192/STM64	None	LOS, LOF, AIS-L, MS-AIS
GE, FC100, FC200, FC400	None	LOS, LoSync, LF, RF
10GELAN, 10GFC	None	LOS, LoSync, LF, RF
OTN	BER > SDBER	LOS, LOF, ODU2-AIS, GFP (REMOTE_FAULT), LCK, OCI, BDI

Because the protection switching is non-revertive, once an automatic switch occurs, traffic does not switch back to the original facility when the fault that caused the original switch clears.

The following examples illustrate this behavior:

- 1 Protection group A and B start with A working and B protecting, with no faults on either facility. If a signal fail occurs on A, B becomes the working facility and A becomes the protecting facility. If the signal fail clears on A, B remains working and A remains protecting.
- 2 Protection group A and B start with A working and B protecting, with no fault on A and a signal degrade on B. If a signal fail occurs on A, B becomes the working facility. If the signal fail clears on A, another switch occurs, making A the working facility again and B the protecting facility.

7.2 Protection switching for line protection

Line protection switching is supported on the following Transponder modules:

- 1GWavelength Regenerator
- 2.5G Wavelength Regenerator
- 2.5G Wavelength Manager
- Dual 4G Multiprotocol Transponder
- Dual 10G Multiprotocol Transponder
- Dual 10G Multiprotocol Transponder Lite

For information about provisioning protection groups, see [8.6, “Provisioning protection groups on Transponder modules”](#).

Directionality

Line protection can be unidirectional or bidirectional for BT7A49AA-IO2 modules, depending on configuration. Line protection is unidirectional for all other transponder modules.

- Unidirectional means that the protection switch decision at one end is independent of the protection switch decision at the other end. The transponder at one end can choose one path as its working path, while the transponder at the other end can choose the other path as its working path.
- Bidirectional means that the protection switch decisions at both ends are matched. Both transponders choose the same path as their working path. In order for both ends to arrive at the same decision, the near end informs the far end of any switching decision that it makes. For some line protocols, this is accomplished through signaling (e.g. BDI). For other protocols, this is accomplished through 'glitching' the transmit laser. Glitching the laser at the near end causes an LOS at the far end, thereby causing the far end to switch to the other path.

Automatic protection switching

Automatic protection switching occurs when there are facility faults on the working path.

When a qualifying fault occurs, the working port stops receiving and becomes the standby, and the standby port starts receiving and becomes the working port. Refer to the following table for a list of the faults that cause automatic switching in a line protection group. Higher priority faults will cause a switch to a line with a lower priority fault.

Table 7-2 Line fault conditions

Fault Type	Category	Priority
Line RX Fault		
LOS: Loss of signal on the line side of the transponder in receive direction towards client.	Signal Fail	High

Table 7-2 Line fault conditions (Continued)

Fault Type	Category	Priority
LOF: Loss of OTU2 frame that persists for 3ms (as per G.709) on the line side of transponder.	Signal Fail	High
OTU2AIS: Alarm indication signal - OTU2 layer	Signal Fail	High
LCK: A lockout condition exists on the line port at the far end. OCI: An open connection exists at the far end (i.e. a cross connect has been provisioned on the local end but not on the far end). BDI: A backward defect indication has been received on the line side of the transponder.	Signal Fail	High
LoSync: Loss of synchronization on the line side of the transponder in receive direction towards client.	Signal Fail	High
LF, RF: Local fault, remote fault.	Signal Fail	High
AIS-L: Alarm indication signal - line.	Signal Fail	High
Signal degrade alarm: BER > SDBER threshold	Signal Degrade	Low

Note Not all faults apply to all cross connect combinations.

Automatic protection switching considerations

- An automatic protection switch does not switch to a line that has the same or higher priority failure as the working port.
- The SDBER threshold can be set to zero to disable monitoring, and disable switching due to SD fault on a given port in a protection group.
- When a working line port is put into OOS maintenance state, an automatic switch occurs away from that port (unless the protecting port is locked out or OOS).
- If the SCP is removed from the system due to restart or replacement, automatic line protection switching continues to function.

Manual protection switch

A manual protection switch causes the working and protected ports to switch when both ports are free of faults. The following are the rules for a manual protection switch:

- A manual protection switch can operate only on the working port of a protection group.
- A manual protection switch is accepted only if no other protection switch is active and if the protecting port is free of faults.

- When a manual protection switch operates, the working port becomes the protecting port, and the protecting port becomes the working port. No other state changes result.

Forced protection switch

A forced protection switch causes the working and protecting ports to switch even if the protecting port is in a Signal Degrade state.

The following are the rules for a forced protection switch:

- A forced protection switch targets the port in a protection group from which traffic is to be switched away.
- A forced protection switch can be used to switch the working port in a protection group to a port with a signal degrade fault level. It may also be used to switch the working port to protecting, if the protecting port is at the same fault severity as the working port (that is, either in a fault-free state or a signal degrade state).
- A forced protection switch can be used to target the protecting port in a signal degrade or fault-free state. This would not cause a protection switch, but can block an automatic protection switch back to the protecting port that might otherwise occur.
- A forced protection switch is accepted only if there is no lockout protection switch or other forced protection switch active on either port.
- When a forced protection switch operates, the secondary state of the target port goes to FRCD (forced).
- If the working port experiences a signal fail condition while the protecting port is in the forced state, and is not at the Signal Fail severity level, an automatic protection switch to the protecting port occurs, and the forced switch on the protecting port is automatically released.

Lockout protection switch

A lockout protection switch causes the working or protecting port to become protecting and makes the port unavailable for protection. The following are the rules for a lockout switch:

- A lockout protection switch targets the facility in a protection group from which traffic is to be switched away. It can be the working or the protecting port.
- When a lockout protection which is applied to the working port, a protection switch immediately occurs, regardless of the state of the protecting port.
- When a lockout protection switch operates, the secondary state of the target port goes to LKDO (locked out). In this state, the port is not available for protection of the working port.
- A protecting port can also be locked out.
- A lockout protection switch is accepted only when no other lockout switch is active on the protection group.
- A lockout protection switch can be cancelled only when the protection switch on the port in the LKDO secondary state is released.

7.3 Protection switching for client protection

Client port protection provides full equipment redundancy. The service is protected against module, line and client pluggable faults.

During regular operation, the working client port is actively transmitting and the standby client port is turned off. When a qualifying fault occurs:

- The current working client port turns off its transmitting laser. Its status changes to standby and the port becomes the new protecting client port.
- The current protecting client port turns on its transmitting laser. Its status changes to active and the port becomes the new acting client port.

Protection switching is provisioned on the protection group. For information about provisioning protection switching refer to [8.6, “Provisioning protection groups on Transponder modules”](#).

Directionality

Client protection switching is always bidirectional. The transponders at both ends decide on the same path to transmit and receive traffic. In order for both ends to arrive at the same decision, the near end informs the far end of any switching decision that it makes. For some line protocols, this is accomplished through signaling (e.g. BDI). For other protocols, this is accomplished through 'glitching' the transmit laser. Glitching the laser at the near end causes an LOS at the far end, thereby causing the far end to switch to the other path.

Automatic protection switching

Automatic protection switching of client ports occurs when there are working facility faults or client transmitter faults. Removing a transponder module from a client protection group also triggers automatic protection switching.

When a qualifying fault occurs, the working port automatically turns off its transmitting laser and becomes the standby, and the standby port turns on its transmitting laser and becomes the active port. Refer to the following table for a list of the faults that cause automatic switching in a client protection group. Higher priority faults will cause a switch to a client/line pair with a lower priority fault.

Table 7-3 Line and client fault conditions

Fault Type	Category	Priority
Line RX Fault		
LOS: Loss of signal on the line side of the transponder in receive direction towards client.	Signal Fail	High
LOF: Loss of OTU2 frame that persists for 3ms (as per G.709) on the line side of transponder.	Signal Fail	High
OTU2AIS: Alarm indication signal - OTU2 layer	Signal Fail	High

Table 7-3 Line and client fault conditions (Continued)

Fault Type	Category	Priority
LCK: A lockout condition exists on the line port at the far end.	Signal Fail	High
OCI: An open connection exists at the far end (i.e. a cross connect has been provisioned on the local end but not on the far end).		
BDI: A backward defect indication has been received on the line side of the transponder.		
LoSync: Loss of synchronization on the line side of the transponder in receive direction towards client.	Signal Fail	High
LF, RF: Local fault, remote fault.	Signal Fail	High
AIS-L: Alarm indication signal - line.	Signal Fail	High
Signal degrade alarm: BER > SDBER threshold	Signal Degrade	Low
Client RX Fault		
LOS: Loss of signal in receive direction.	Signal Fail	High
LOF: Loss of frame in receive direction.	Signal Fail	High
LoSync: Loss of synchronization in receive direction.	Signal Fail	High
Client TX Fault		
XFP/SFP Failure	Signal Fail	High
XFP/SFP Missing	Signal Fail	High

Note Not all faults apply to all cross connect combinations.

Automatic protection switching considerations

- An automatic protection switch does not switch to a port that has the same or higher priority failure as the working port.
- The SDBER threshold can be set to zero to disable monitoring, and disable switching due to SD fault on a given port in a protection group.
- When a working client port is put into OOS maintenance state, an automatic switch occurs away from that port (unless the protecting port is locked out or OOS).
- If the SCP is removed from the system due to restart or replacement, automatic client protection switching continues to function.

User Invoked protection switching

User invoked protection switching includes three switching options: Manual, Forced, and Lockout.

Manual protection switch

A manual protection switch causes the working and protected port to switch when both ports are free of faults. The following are the rules for a manual protection switch:

- A manual protection switch can operate only on the working port of a protection group.
- A manual protection switch is accepted only if no other protection switch is active and if the protecting port is free of faults.
- When a manual protection switch operates, the working port becomes the protecting port, and the protecting port becomes the working port. No other state changes result.

Forced protection switching considerations

A forced protection switch is used to switch activity even when the standby facility is in signal degrade state.

- A forced protection switch is accepted only if there is no lockout or forced protection switch already active on the protection group.
- A forced protection switch can be applied to the active client port. A protection switch occurs if the standby facility is fault free or in signal degrade.
- A forced protection switch can be applied to the standby client. This does not cause a protection switch. However, it blocks an automatic protection switch to the standby that occurs if the active facility experiences signal degrade. It does not block a protection switch due to signal fail or higher priority switches.
- If a forced protection switch is overridden by a higher priority switch, the forced switch automatically releases. It does not re-occur once the condition, which caused the switch to be overridden, goes away.
- The secondary state of the forced out facility shows FRCD&STDBY.

Lockout protection switching considerations

When a client facility is locked out, it is unavailable for protection:

- A lockout protection switch is accepted only when there is no other lockout switch already active on the protection group.
- A lockout protection switch can be applied to the standby client port.
- A lockout protection switch can be applied to the active client port. A protection switch occurs immediately regardless of the state of the standby client port.
- The secondary state of the locked out facility shows LKDO&STDBY.
- A lockout protection switch can be cancelled using the release command (RLS-PROTNSW-XCVR).
- If the protection group is deleted, lockout is implicitly cancelled.

7.4 Operate protection switching on a Transponder module

Use this procedure to operate a protection switch on a Transponder module.



Prerequisites

- A protection group must be provisioned on the Transponder module.

Operate protection switching

Follow these steps to operate a protection switch on a Transponder module:

- Step 1** In the toolbar, click the System Configuration button.
- Step 2** In the Navigation pane, right-click **Provision Protection Groups**.
- Step 3** In the **Protection groups** dialog for the module, select a protection group, and then click **Protection Switch**.
- Step 4** In the **Operate Switch** dialog, click one of the following option buttons to set the switch command.
- **Manual switch** — to cause the working and protecting ports to switch when both ports are free of faults
 - **Forced switch** — to cause the working and protecting ports to switch even if the protecting port is in a signal degrade state
 - **Lockout** — to cause the working or protecting port to become protecting and make the port unavailable for protection
- Step 5** Select the working or protecting transceiver port from the **onport** list.
- Step 6** In the **Operate protection switch** confirmation dialog, click **Yes**.
- Step 7** In the **Operate Switch** dialog, click **Apply**.

You have successfully completed this procedure.

7.5 Release protection switching on a Transponder module

Use this procedure to release a protection switch on a Transponder module.



Prerequisites

- A protection switch must be provisioned on the Transponder module.

Releasing protection switching

Follow these steps to release a protection switch on a Transponder module:

- Step 1** In the toolbar, click the System Configuration button.
- Step 2** In the Navigation pane, right-click **Provision Protection Groups**.
- Step 3** In the **Protection groups** dialog for the module, select a protection group on which a protection switch is provisioned, and then click **Release**.
- Step 4** In the **Release Switch** confirmation dialog, click **Yes**.

You have successfully completed this procedure.

8.0 Provisioning Transponder modules and ports

This section provides information about provisioning Transponder modules and ports.

- [8.1, “Autoprovisioning support on Transponder modules”](#)
- [8.2, “Provisioning Transponder modules”](#)
- [8.3, “Provisioning ports on Transponder modules”](#)
- [8.4, “General Communications Channel”](#)
- [8.5, “Provisioning cross-connections on Transponder modules”](#)
- [8.6, “Provisioning protection groups on Transponder modules”](#)

8.1 Autoprovisioning support on Transponder modules

Transponder modules support autoprovisioning on the BTI 7000 Series. For detailed information about autoprovisioning, see the *Operations Solutions Guide*.

Note The Dual 10G Multiprotocol Transponder, Dual 10G Multiprotocol Transponder Lite, and 10G Multiprotocol Transponder are always autoprovisioned as AINS, regardless of the system autoprovisioning settings.

When a Transponder module is inserted into a shelf's unprovisioned slot, the module is autoprovisioned with its primary state set to the same value as the AUTOP parameter. Support for autoprovisioning of ports on a Transponder module depends on the type of module.

Only the 2.5G Wavelength Manager supports autoprovisioning of ports; however, only for SONET applications. Autoprovisioning is not supported for SDH applications.

Autoprovisioning support on 2.5G Wavelength Manager ports

When an SFP transceiver is inserted into an unprovisioned 2.5G Wavelength Manager port, the transceiver port is autoprovisioned according to the AUTOP parameter setting as shown in the following table. The port is autoprovisioned with the Wavelength parameter set to the wavelength of the SFP transceiver that is inserted. A REPT^DBCHG system message is sent from the network element indicating that the port is provisioned.

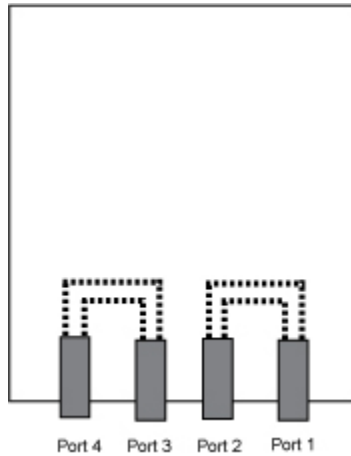
Table 8-1 AUTOP parameter Settings

AUTOP setting	Description
NONE	No autoprovisioning occurs.
IS	The SFP transceiver is autoprovisioned to the OOS-AU,FLT&NALM state.
OOS	The SFP transceiver is autoprovisioned to the OOS-AUMA,FLT state.
AINS	The SFP transceiver is autoprovisioned to the OOS-AU,FLT&AINS state.

Important If an SFP transceiver is inserted into a port of an unprovisioned 2.5G Wavelength Manager module, autoprovisioning of the port does not occur.

Cross-connection pairs on 2.5G Wavelength Manager ports

The following figure shows that each port on a 2.5G Wavelength Manager module is part of a cross-connection pair. Ports 1 and 2 form one cross-connection pair; ports 3 and 4 form another. A given port's mate is the other port in the cross-connection pair. For instance, port 1 is the mate of port 2, and port 2 is the mate of port 1.

Figure 8-1 2.5G Wavelength Manager 2-Way, 2-Port cross-connection pairs**Protocol assignment on 2.5G Wavelength Manager ports**

The protocol that is assigned to a transceiver port on a 2.5G Wavelength Manager module is determined as follows:

- If the mate port is not yet provisioned, or if the mate port is provisioned with the Protocol parameter set to AUTO, the Protocol parameter for the new port is also set to AUTO.
- If the mate port is provisioned to use a valid protocol, the Protocol parameter for the new port is set to the same protocol, and a 2-Way cross-connection is automatically created between the two ports.

When the Protocol parameter for a port is set to AUTO, the 2.5G Wavelength Manager module starts scanning the incoming signal, looking for a valid signal. Once a valid signal, for example, OC48, is found, the Protocol parameter for the transceiver port is also set to OC48. If the mate's transceiver port is still scanning for a signal, the Protocol parameter for the port is set to OC48, and a 2-Way cross-connection is provisioned between the two ports.

Whenever the Protocol parameter changes from AUTO to a supported protocol, a corresponding REPT^DBCHG system message is sent from the network element.

Whenever a 2-Way cross-connection is autoprovisioned, a corresponding REPT^DBCHG system message is sent from the network element.

8.2 Provisioning Transponder modules

Transponder modules may be provisioned before they are physically present in the shelf.

Provisioning settings and custom settings

When you provision a Transponder module, you specify settings such as its name and its Product Equipment Code, and provide brief ID information about the module. You can also provision custom information to record information specific to your environment. For example, you may want to record information about equipment usage, upgrades, and maintenance.

A Transponder module must be provisioned before a port on the module can be provisioned. When a module is physically present in the shelf, the system checks whether the module type matches the provisioned Transponder module type. If the inserted module type does not match the provisioned module type, an equipment mismatch alarm is raised. The alarm clears when the proper module type is inserted or when the provisioning data is updated to resolve the mismatch.

Displaying module information

Once a Transponder module is provisioned, you can view the settings specified when the module was provisioned, as well as inventory information, such as the module's hardware release number and date of manufacture.

Removing and restoring service

A Transponder module should be removed from service before it is deleted, so that alarms are not raised. A module that has been removed from service can be restored to service.

Restarting a module

Transponder modules support warm restarts and cold restarts. A warm restart lets you restart the software on the module. Although a warm restart is not service affecting, you cannot make configuration changes to the module while the warm restart is in process. A cold restart resets the software on the module and is service affecting.

Deleting a module

If you want to change the type of Transponder module that is either preprovisioned or physically present in a shelf, you must first delete it.

This section covers the following topics:

- [8.2.1, “Provision Transponder module settings”](#)
- [8.2.3, “Display Transponder module information”](#)
- [8.2.4, “Remove a Transponder module from service”](#)
- [8.2.5, “Restore a Transponder module to service”](#)
- [8.2.6, “Restart a Transponder module”](#)
- [8.2.7, “Delete a Transponder module”](#)

8.2.1 Provision Transponder module settings

Use this procedure to provision settings for a Transponder module.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

Prerequisites

- Shelf must be provisioned.

Provisioning module settings

Follow these steps to provision settings for a Transponder module:

Step 1 In the toolbar, click the System Configuration button.

Step 2 In the Navigation pane, right-click the slot that includes the module you are provisioning and click **Provision Module**. The **Provision Module** dialog appears.

The following example displays the **Provision Module** dialog as it appears when you first open the dialog. By default, the **Name** and **PEC/CLEI Code** fields show the first entry of the drop-down menu.

Provision Module

Settings Custom Settings

General

Name: C1ADM PEC / CLEI Code: BP1A32AA-01 / WMOAAJXGAA

Shelf Number: 1 ID:

Slot Number: 17

State Management

Initial State: IS

Apply Close Help

Step 3 Select the module that you are provisioning.

Click the **Settings** tab. From the **Name** drop-down menu, select the module type. From the **PEC/CLEI Code** drop-down menu, select the product equipment code (PEC)/Common Language Equipment Identification (CLEI) code for that module. The module shelf and slot numbers are displayed, automatically.

Step 4 Optional. Create an identifier (ID) for the module.

In the **ID** field, enter up to 20 alphanumeric characters.

Step 5 Specify the operational state of the module. From the **Initial State** drop-down menu, choose one of the following:

- **IS** — In Service
- **OOS** — Out of Service

Step 6 Click **Apply**.

Step 7 Option. Click the **Custom Settings** tab, and add additional information about the settings.

Step 8 Click **Close**.

You have successfully completed this procedure.

8.2.2 Bulk module provisioning

Systems that contain many modules of the same type can be provisioned quickly using bulk module provisioning.



Prerequisites

- Expansion shelves must be provisioned.

Note Modules that were provisioned via bulk provisioning must be deleted individually. There is no bulk de-provisioning.

The following table provides information about the bulk module provisioning parameters:

Parameter	Description	Configurable
Product Model	List of all the available products/Short name of module installed. For example, SBA for the Sub-Band Booster Amplifier.	Yes
PEC/CLEI Code	Lists all the Product Equipment Codes (PECs) available for the selected module type. For example, if TPR is selected, the list contains the PEC codes for all the supported TPR modules.	Yes
Initial State	List of initial states for the cards to be provisioned. Values are: <ul style="list-style-type: none"> • OOS (Out of Service) 	Yes

Parameter	Description	Configurable
	<ul style="list-style-type: none"> IS (In Service) - Default 	
Available Slots	Lists the slots within the system that are not provisioned	Yes
Selected Slots	Lists the slots selected to be provisioned with the same attributes as the selected PEC module.	Yes

Use this procedure to bulk provision modules.

Step 1 On the Tools menu, select **Bulk Tools > Bulk Module Provisioning**.

Step 2 In the **Bulk Module Provisioning** dialog, select a module type from the **Product Model** drop-down box.

Step 3 From the **PEC/CLEI Code** drop-down box, select a code for the selected product model.

Step 4 From the **Initial State** drop-down box, select an initial state for the selected PEC.

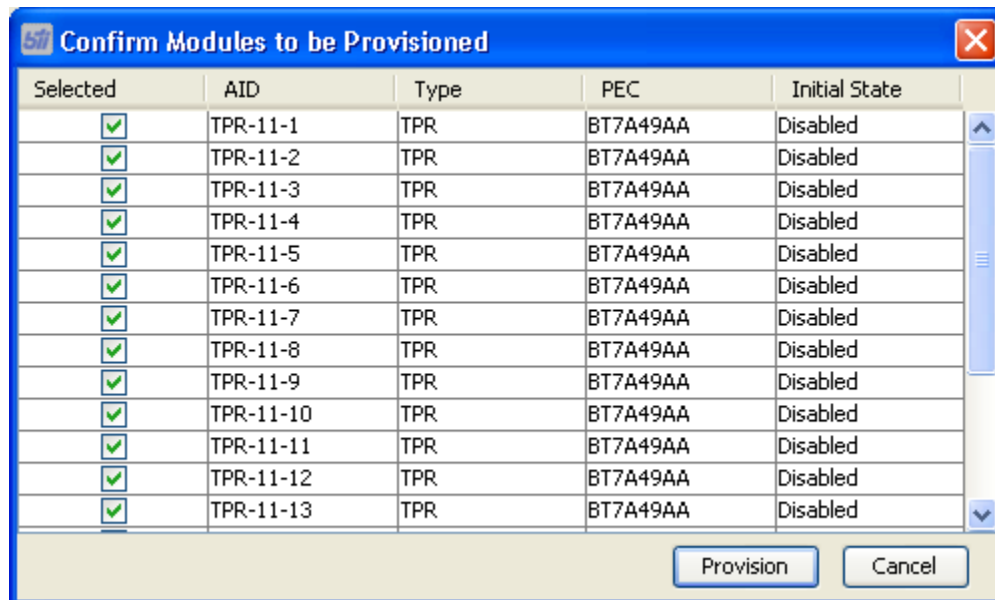
Step 5 In the **Available Slots** list, shift-click to select the slots that are to be provisioned with the PEC attributes selected in step 2.

Step 6 Click the > arrow between the **Available Slots** and the **Selected Slots** lists.

The selected slots are moved to the **Selected Slots** list.

Step 7 Click **Apply**.

A confirmation dialog displays with a list of the objects that will be created. If required, you can remove individual items from the list. The modules are provisioned with the selected attributes.



Step 8 Click **Provision**.

A progress bar displays. When complete, if any provisioning errors occur, an error status window displays.

8.2.3 Display Transponder module information

Use this procedure to view provisioned and non-provisionable parameters for a Transponder module.

**Prerequisites**

- Transponder module must be physically present in the shelf.

Displaying module information

Follow these steps to view parameters for a Transponder module:

Step 1 In the toolbar, click the **System Configuration** button.

Step 2 In the Navigation pane, right-click a module, and then click **Display Module Inventory**.

The **Display Inventory Information** dialog displays **General**, **Hardware**, **Manufacturing**, and **Testing** parameters for the Transponder module. See the following table.

Step 3 Click **Close**.

You have successfully completed this procedure.

Table 8-2 Module inventory information

Type	Parameter	Description
General	Full Name	Official name of the module
	Name	Short name of the module
	Shelf Number	The shelf in which the module is installed
	Slot Number	The slot in which the module is installed
Hardware	PEC Code	The product equipment code assigned by the manufacturer
	CLEI Code	The Common Language Equipment Identifier number assigned by Telcordia. The CLEI identifies the physical hardware.
	Release Number	The hardware release number
	Serial Number	The serial number of the module
	Firmware	The firmware version of the module
	USI	The USI setting

Table 8-2 Module inventory information (Continued)

Type	Parameter	Description
Manufacturing	Manufacturing Date	The date that the module was manufactured
	Manufacturing Location	The location where the module was manufactured
Testing	Testing Date	The date that the manufacturer tested the module
	Testing Location	The location where the manufacturer tested the module

8.2.4 Remove a Transponder module from service

Use this procedure to remove a Transponder module from service.

Authorization Required Superuser Provisioning Maintenance Surveillance

Prerequisites

- Transponder module must be provisioned and in service.

Removing a module from service

Follow these steps to remove a Transponder module from service:

- Step 1** In the toolbar, click the System Configuration button.
- Step 2** In the Navigation pane, right-click a module, and then click **Provision Module**.
- Step 3** On the **Settings** tab of the **Provision Module** dialog, click the **Remove** button beside the **State** field.
- Step 4** In the **Remove Entity** dialog, click **Yes**.
- Step 5** Click **Close**.

You have successfully completed this procedure.

8.2.5 Restore a Transponder module to service

Use this procedure to restore a Transponder module to service.

Authorization Required Superuser Provisioning Maintenance Surveillance

Prerequisites

- Transponder module must be provisioned and out of service.

Restore a module to service

Follow these steps to restore a Transponder module to service:

Step 1 In the toolbar, click the System Configuration button.

Step 2 In the Navigation pane, right-click a module, and then click **Provision Module**.

Step 3 On the **Settings** tab of the **Provision Module** dialog, click the **Restore** button beside the **State** field.

Step 4 Click **Close**.

You have successfully completed this procedure.

8.2.6 Restart a Transponder module

Use this procedure to restart a Transponder module.



Prerequisites

- Transponder module must be provisioned.

Restarting a Transponder module

Follow these steps to perform a cold or warm restart of a Transponder module:

Step 1 In the toolbar, click the System Configuration button.

Step 2 In the Navigation pane, right-click a module, select **Restart Module**, and then click one of the following:

- **Warm Restart** — to restart the software on the module
- **Cold Restart** — to cycle the power on the module

Step 3 In the **Restart** confirmation dialog, click **Yes**.

You have successfully completed this procedure.

Note A CONTCOM (Control Communications Failure with Circuit Pack) alarm is raised during a cold or warm restart of a Transponder module. For information about this alarm, see the *Alarm and Troubleshooting Guide*.

8.2.7 Delete a Transponder module

Use this procedure to delete a Transponder module.



Prerequisites

- Transponder module must be provisioned and removed from service.

Deleting a module

Follow these steps to delete a Transponder module:

Step 1 In the toolbar, click the System Configuration button.

Step 2 In the Navigation pane, right-click a module, and then click **Delete Module**.

Step 3 In the **Delete Module** confirmation dialog, click **Yes**.

You have successfully completed this procedure.

8.3 Provisioning ports on Transponder modules

When you provision a port on a Transponder module, you must specify the protocol and wavelength. You can also provision custom information to record information specific to your environment. For example, you may want to record information about equipment usage, upgrades, and maintenance.

When a transceiver is physically present in a port, the system checks whether the transceiver type matches the provisioned transceiver type. If the inserted transceiver does not match the provisioned transceiver type, alarm is raised. The alarm clears when the proper transceiver type is inserted or when the provisioning data is updated to resolve the mismatch. If a tunable XFP is installed in the port being provisioned, the XFP tunes to the specified wavelength.

Ports on a provisioned Transponder module may be provisioned before the module is physically present in the shelf.

Ports on transponder modules must be provisioned before loopback tests, cross-connections, or protection groups can be provisioned.

Displaying and modifying port information

Once a Transponder port is provisioned, you can view the settings for provisioned and non-provisionable parameters, and modify provisionable parameters.

Removing and restoring service

A port must be removed from service when a loopback test is to be performed or when the port is to be deleted. A port that has been removed from service can be restored to service.

Deleting a port

You can delete a port when you need to change the transceiver type installed in the port.

This section covers the following topics:

- [8.3.1, “Provision port settings on a Transponder module”](#)
- [8.3.2, “Display transceiver information ”](#)
- [8.3.3, “Display port information for a Transponder module”](#)
- [8.3.4, “Modify port settings on a Transponder module”](#)
- [8.3.5, “Remove a port from service ”](#)
- [8.3.6, “Restore a port to service”](#)
- [8.3.7, “Delete a port ”](#)

8.3.1 Provision port settings on a Transponder module

Use this procedure to provision settings for a transceiver port on a Transponder module.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

Prerequisites

- Transponder module must be provisioned.

Provisioning port settings

Follow these steps to provision port settings on a Transponder module:

Step 1 In the toolbar, click the **System Configuration** icon.

Step 2 In the Navigation pane, highlight the Transponder module that you are configuring and right-click on a port. Click **Provision Transceiver**. The **Provision Transceiver** dialog appears.

The following tabs are available for configuring a Transponder port : **Transceiver**, **Custom Info**, **Performance**, **Thresholds**, **GCC0**.

The following example displays the **Provision Transceiver** dialog with default values, as it appears before you apply new settings. The **Performance** and **Threshold** tabs become available once you apply the Transceiver settings:

The screenshot shows the 'Provision Transceiver' dialog box with the following sections:

- Tabs:** Transceiver (selected), Custom Info, Performance, Thresholds, GCC0.
- Settings:**
 - Protocol: 10 Gigabit Ethernet LAN with Fo...
 - Wavelength (nm:THz:Ch:DOL): 1310 : n/a : n/a : n/a
 - Phy PM Thld Mon: Disabled
 - Fault Propagation Shutdown: Disabled
 - SD Bit Error Rate: 10^-6
 - Loopback: Disabled
 - Vendor Part Number 1:
 - Transceiver PEC: BP3AM4MS
 - Vendor Part Number 2:
 - Tx Trace Id:
 - Vendor Part Number 3:
 - Expected Trace Id:
 - Laser Control: Manual On
 - Rx Trace Id:
- Cross Connects:**

Source	Destination	Direction
- Timers:**
 - Auto-In Service Timer: 0 days 8 hours 0 minutes
 - Active Auto-In Service Timer: <none> [Refresh]
- State Management:**
 - State: OOS-AU, UEQ [Remove] ☐ AIN S
 - Laser Status: OFF
- Buttons:** Apply, Close, Help

Step 3 Specify the settings for the port. See [Table 8-3](#).

Step 4 Click **Apply**.

You have successfully completed this procedure

Table 8-3 Port provisioning parameters

Tab/Parameter	Range of values	Description
Transceiver tab		
Settings		
Protocol	For a list of protocols supported by Transponder modules, see Chapter 2, "Transponder features and supported protocols" .	The protocol to be used. Note The protocol specified must fall within the range of bit rates supported by the transceiver.
Wavelength	0 (copper SFPs, GE clients only) 850nm to 1611nm Note For information about wavelengths supported on a tunable XFP, see 8.3.1.1, "Wavelengths supported on Tunable XFP BP3AM4TL" .	The wavelength to be used
Fault Propagation Shutdown	Enabled Disabled (default) Note When Wavelength = 0, FPSD cannot be enabled. Note When the Protocol parameter is set to 10GELAN, the Fault Propagation Shutdown parameter is Enabled by default. Note Fault Propagation Shutdown must be set to Disabled if Laser Control is set to Manual On or Manual Off .	Enables or disables fault propagation shutdown. For more information, see 8.3.1.2, "Fault Propagation Shutdown and laser status" .
Physical PM Monitoring	Enabled Disabled (default)	Enables or disables monitoring of performance monitoring thresholds for SFP or XFPs with digital diagnostic support. For more information, see 8.3.1.5, "Threshold crossing alerts for transceiver ports" .
Loopback	Terminal Facility	Terminal: The egress port transmits its configured maintenance signal.

Table 8-3 Port provisioning parameters (Continued)

Tab/Parameter	Range of values	Description
	Disabled (default)	<p>Note</p> <p>Terminal loopback cannot operate, if a loopback is operating on either port in the cross-connect (Terminal or Facility).</p> <p>Facility:</p> <ul style="list-style-type: none"> non-OTN protocols: the loopback occurs at the cross-point switch. The signal is still forwarded to the framer to analyze the signal for faults and defects. OTN protocols: the loopback occurs inside the framer, to decode and re-encode the E/FEC. <p>Caution</p> <p>Loopback should be performed when the transceiver port is out-of-service (OOS). The port may still be involved in provisioned cross-connects.</p>
SD Bit Error Rate	For 10G Multiprotocol Transponder, Dual 10G Multiprotocol Transponder, and Dual 4G Multiprotocol Transponder modules: 6 to 10, corresponding to 10^{-6} (high) to 10^{-10} (low)	The signal degrade bit error rate.
Transceiver PEC	Not applicable	The transceiver product equipment code .
Vendor Part Number 1, 2, 3	up to 20 characters	<p>The part numbers provided by the transceiver manufacturer.</p> <p>Note</p> <p>If a vendor part number is entered, the REPLUNITMEA alarm for the transceiver is enabled. Therefore, if the system detects a mismatch between the provisioned vendor part number and the number of the transceiver that is inserted in the port, the REPLUNITMEA alarm is raised.</p>
Tx Trace ID	up to 15 alphanumeric characters	The trace ID to transmit.
Expected Trace ID	up to 15 alphanumeric characters	The trace ID that is expected to be received.
Rx Trace ID (read only)	up to 15 alphanumeric characters	The trace ID that was received.
Laser Control	Auto Manual On Manual Off	<p>The laser status control.</p> <p>Set to Auto to let the software control the laser status. Set to</p>

Table 8-3 Port provisioning parameters (Continued)

Tab/Parameter	Range of values	Description
	Note Laser Control must be set to Auto if Fault Propagation Shutdown is Enabled .	Manual On to turn the laser on, Manual Off to turn the laser off.
Timers		
Auto-In Service Timer	days-hours-minutes	The automatic in-service (AINS) timer for the Transponder module. The default is 08-00.
Active Auto-In Service Timer (read only)	days-hours-minutes	The time remaining on the AINS timer
State Management		
State (read only)	IS OOS AINS	Indicates whether the port is in or out of service. The port defaults to the initial state of the module.
Laser Status (read only)	ON OFF IDLE PRBS REMOTE-FAULT ODU2-AIS AIS-L MS-AIS	Indicates the status of the laser. For more information, see 8.3.1.2, "Fault Propagation Shutdown and laser status" .
Custom Info tab		
Information Settings		
ID1, ID2	up to 32 alphanumeric characters per field	Identifier information about the port or transceiver
Fiber Type	DSF (Dispersion-shifted fiber) NDSF (Non-dispersion-shifted fiber) NZDSF (Non-zero dispersion-shifted fiber)	The fiber type that connects to transceiver. By default, the fiber type is set to <not specified>.
Grid	20 nm 50GHz 100GHz 200GHz	The channel frequency grid.
Custom 1, 2, 3	up to 255 alphanumeric characters for each field	Information specific to the operating environment.
Remote ID	up to 255 alphanumeric characters, in the form of <NE IP Address>-<Shelf>-<Slot>-<Port> For example: 172.1.23.456-21-5-1	The identity of the port at the far end.
Performance tab		
PM Collection Status		

Table 8-3 Port provisioning parameters (Continued)

Tab/Parameter	Range of values	Description
Refresh	5, 10, 30, 60, 300, 900, 3600 seconds	Sets, in seconds, how often to update the statistical information. Toggle the Start/Stop button to enable/disable the PM collection.
Current Status	Not applicable	Indicates whether or not the system is collecting the performance metrics.
Bin Type	15 minute bin 1 day bin Untimed bin	The time period for which to collect the performance metrics.
Physical PMs	The PM types displayed are dependent on the protocol you set, from the options in the Transceiver tab. For a description of PMs supported by each Transponder module refer to 8.3.1.3, “ Monitored type (montype) values and threshold crossing alerts (TCA) for Transponder modules ”.	The performance metrics collected.
Thresholds tab	Default threshold values or configured values. For a list of acceptable range values refer to 8.3.1.3, “ Monitored type (montype) values and threshold crossing alerts (TCA) for Transponder modules ”.	This page is used to monitor and modify the PM threshold values for the provisioned module.

8.3.1.1 Wavelengths supported on Tunable XFP BP3AM4TL

Note This transceiver is manufacture discontinued. Use BP3AM4TF instead.

Table 8-4 DWDM Wavelength Plan

Wavelength (nm)	BTI Channel Numbers	Wavelength (nm)	BTI Channel Numbers
1529.55	E8	1545.32	E4
1530.33	32	1546.12	16
1531.12	31	1546.92	15
1531.90	30	1547.72	14
1532.68	29	1548.51	13
1533.47	28	1549.32	12
1534.25	27	1550.12	11
1535.04	26	1550.92	10
1535.82	25	1551.72	9
1536.61	E7	1552.52	E3
1537.40	E6	1553.33	E2
1538.19	24	1554.13	8

Table 8-4 DWDM Wavelength Plan (Continued)

Wavelength (nm)	BTI Channel Numbers	Wavelength (nm)	BTI Channel Numbers
1538.98	23	1554.94	7
1539.77	22	1555.75	6
1540.56	21	1556.55	5
1541.35	20	1557.36	4
1542.14	19	1558.17	3
1542.94	18	1558.98	2
1543.73	17	1559.79	1
1544.53	E5	1560.61	E1

8.3.1.2 Fault Propagation Shutdown and laser status

Enabling Fault Propagation Shutdown on Transponder modules

When a fault is raised against a pluggable receiver interface, the corresponding transmitting laser at the far end of the link continues to function and can transmit unreliable information.

Fault propagation shutdown (FPSD) provides a means to quickly shut down a transmitting laser and pass the fault to the downstream device when a receiver signal failure occurs. When FPSD is enabled, the transmit laser is shut down in a fault scenario. When FPSD is disabled, the transmitted signal is the maintenance signal pattern for the provisioned protocol. You enable or disable the FPSD parameter when you provision port settings on a Transponder module.

Note If FPSD is enabled, the port laser control parameter must be set to allow software to automatically control the laser.

For information, see [8.3.1, “Provision port settings on a Transponder module”](#).

Laser status

The proNX 900 Node Controller provides laser status information as a read-only attribute. The following table lists the possible laser status values:

Table 8-5 Laser status values

Laser status	Description
ON	The laser is on and a valid signal is being transmitted.
OFF	The laser is shut down; no signal is being transmitted.
IDLE	The laser is transmitting an IDLE signal, as defined in IEEE 802.3ae. Note Applies only to the protocols GE and 10GELAN.
PRBS	The laser is transmitting the PRBS pattern at the provisioned rate. Note This value does not apply to the BT7A49AA-I02.
REMOTE-FAULT	The laser is transmitting the REMOTE-FAULT signal as defined in IEEE 802.3ae.

Table 8-5 Laser status values (Continued)

Laser status	Description
ODU2-AIS	The laser is transmitting OTN G.709-compliant ODU2-AIS. Note This value applies only to OTN protocols.
AIS-L	The laser is transmitting SONET AIS-L (Alarm Indication Signal on the Line). Note This value applies only to SONET protocols.
MS-AIS	The laser is transmitting SDH MS-AIS. Note This value applies only to SDH protocols.
LOCAL-FAULT	The laser is transmitting on the client transmit interface.

Rules for FPSD and laser status

In general, if FPSD is enabled for a transceiver port that is not transmitting a valid signal, the laser status is OFF. However, the following are rules that apply to specific modules:

- For the 1G Wavelength Translator, 1G Wavelength Regenerator, and 2.5G Wavelength Regenerator:
 - If FPSD is ENABLED for a transceiver port that is not transmitting a valid signal, the laser status is OFF.
- For the 2.5G Wavelength Manager:
 - If FPSD is ENABLED for a transceiver port that is not transmitting a valid signal, the laser status is OFF.
 - If FPSD is DISABLED for a transceiver port that is not transmitting a valid signal, and the port is provisioned to use a SONET protocol, the laser status is AIS-L.
 - If FPSD is DISABLED for GE protocol, the laser status is IDLE.
- For 10G Multiprotocol Transponder and Dual 10G Multiprotocol Transponder modules:
 - If FPSD is ENABLED for a transceiver port that is not transmitting a valid signal, the laser status is OFF.
 - If FPSD is DISABLED for a transceiver port that is not transmitting a valid signal, and the port is provisioned to use a SONET protocol, the laser status is AIS-L.
 - If FPSD is DISABLED for a transceiver port that is not transmitting a valid signal, and the port is provisioned to use an SDH protocol, the laser status is MS-AIS.
 - If FPSD is DISABLED for a transceiver port that is not transmitting a valid signal, and the port is provisioned to use the protocol 10GELANFEC/EPCMF, 10GELANEFEC/EPCMF, OC192FEC, OC192EFEC, or STM64FEC, STM64EFEC, the laser status is ODU2-AIS.
 - If FPSD is DISABLED for a GE/FC on a 10G Multiprotocol Transponder, the laser status is PRBS for the line port and Local Fault for the client port.

- If FPSD is DISABLED for a GE/FC on a Dual 10G Multiprotocol Transponder-I02, the laser status is Local-Fault.

8.3.1.3 Monitored type (montype) values and threshold crossing alerts (TCA) for Transponder modules

The following tables describe the protocol Performance Monitoring (PM) types (montype), and list the threshold values that trigger a threshold crossing alert (TCA) on Transponder modules. TCAs are autonomously reported events that signal to the management system that a PM parameter value is reached or exceeds the configured threshold:

- Layer 1 Gigabit Ethernet PMs. See [Table 8-6](#).
- 10GELAN PMs. See [Table 8-7](#).
- SONET PMs. See [Table 8-8](#).
- SDH PMs. See [Table 8-9](#).
- Layer 1 Fibre Channel PMs. See [Table 8-10](#).
- OTN PMs. See [Table 8-11](#).

Table 8-6 Layer 1 Gigabit Ethernet PMs (counters)

PM (montype)	PM threshold default values		Supported modules
	15-minute	1-day	
CV 8B/10B Coding Violations measure the number of 8B/10B coding violations and disparity errors.	382	3820	Dual 4G Multiprotocol Transponder 2.5G Wavelength Manager
ES Errored Seconds measures the number of seconds during which one or more coding violations are detected, or a Loss of Synchronization (LOSYNC) or Loss of Signal (LOS) defect is present.	25	250	Dual 4G Multiprotocol Transponder 2.5G Wavelength Manager
SES Severely Errored Seconds measures the number of seconds during which the number of detected coding violations exceeds the severely errored seconds level (SESLVL), or a Loss of Synchronization (LOSYNC) defect or Loss of Signal (LOS) defect is present. The SESLVL value for Layer 1 Gigabit Ethernet is 1250.	4	40	Dual 4G Multiprotocol Transponder 2.5G Wavelength Manager
UAS Unavailable Seconds measures the number of seconds during which the link was considered unavailable. A link becomes unavailable at the onset of 10 consecutive seconds that qualify as SES, and continues to be unavailable until the onset of 10 consecutive seconds that do not qualify as SES. In seconds that	10	10	Dual 4G Multiprotocol Transponder 2.5G Wavelength Manager

Table 8-6 Layer 1 Gigabit Ethernet PMs (counters)

PM (montype)	PM threshold default values		Supported modules
	15-minute	1-day	
are counted as unavailable, the counting of CV, ES, and SES is inhibited.			

Table 8-7 10GELAN PMs (counters)

PM (montype)	PM threshold default values		Supported modules
	15-minute bin	1-day bin	
INVBLK Invalid Blocks measures the number of invalid 64/66B coding blocks.	382	3820	Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder
ES Errored Seconds measures the number of seconds during which one or more errored blocks/code violations are detected, or LOSYNC (Loss of Synchronization) or LOS (Loss of Signal) is detected.	25	250	Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder
SES Severely Errored Seconds measures the number of detected invalid blocks exceeds the severely errored seconds level (SESLVL), or in which a Loss of Synchronization (LOSYNC) defect or Loss of Frame (LOF) defect is present. The SESLVL value for 10GELAN is 8554.	4	40	Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder
UAS Unavailable Seconds measures the number of seconds during which the link was considered unavailable. A link becomes unavailable at the onset of 10 consecutive seconds that qualify as SES, and continues to be unavailable until the onset of 10 consecutive seconds that do not qualify as SES. In seconds that are counted as unavailable, the counting of In seconds that are counted as unavailable, the counting of INVBLK, ES, and SES is inhibited	10	10	Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder
FCSE-RX Total number of received frames with CRC (Cyclic Redundancy Check) errors measures the number of received frames that had a valid length but had either a bad Frame Check Sequence (FCS Error) or a bad FCS with a non-integral number of OCTETS (alignment errors).	0	0	Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder
FRDR Total number of discarded frames measures the total number of frames dropped due to a lack of resources or other reasons.	0	0	Dual 10G Multiprotocol Transponder

Table 8-7 10GELAN PMs (counters) (Continued)

PM (montype)	PM threshold default values		Supported modules
	15-minute bin	1-day bin	
This number is not necessarily the number of frames dropped, but rather the number of time that dropped frames could be detected.			10G Multiprotocol Transponder
FRGT Total fragmented Frame Count in Receive Direction measures the total number of received frames 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).	0	0	Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder
JABR Total Jabber Frame Count in Receive Direction measures the total number of received frames that were longer than the maximum frame size ¹ (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).	0	0	Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder
BCST Total Broadcast Frame Count in Receive Direction measures the total number of good frames received that were directed to the broadcast address. (This number does not include frames that were directed to the multicast address.)			Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder
MCST Total multicast Frame Count in Receive Direction measures the total number of good frames received that were directed to a multicast address. (This number does not include frames that were directed to the broadcast address.)			Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder
OSIZE Total oversized Frame Count in Receive Direction measures the total number of received frames that were greater than the maximum frame size ¹ in length (excluding framing bits, but including Frame Check Sequence (FCS) octets) but were otherwise well formed.	0	0	Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder
OVER1518 Total over-1518 Frame Count in Receive Direction measures the total number of frames received that were greater than 1518 bytes but not exceeding the maximum frame size ¹ in length (excluding framing bits, but including Frame Check Sequence (FCS) octets).	0	0	Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder
SIZE64			Dual 10G Multiprotocol Transponder

Table 8-7 10GELAN PMs (counters) (Continued)

PM (montype)	PM threshold default values		Supported modules
	15-minute bin	1-day bin	
Total 64 Byte Frame Count in Receive Direction measures the total number of 64 byte frames received (excluding framing bits, but including Frame Check Sequence (FCS) octets).			10G Multiprotocol Transponder
SIZE65-127 Total 65-127 Byte Frame Count in Receive Direction measures the total number of 65-127 byte frames received (excluding framing bits, but including Frame Check Sequence (FCS) octets).			Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder
SIZE128-255 Total 128-255 Byte Frame Count in Receive Direction measures the total number of 128-255 byte frames received (excluding framing bits, but including Frame Check Sequence (FCS) octets).			Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder
SIZE256-511 Total 256-511 Byte Frame Count in Receive Direction measures the total number of 256-511 byte frames received (excluding framing bits, but including Frame Check Sequence (FCS) octets).			Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder
SIZE512-1023 Total 512-1023 Byte Frame Count in Receive Direction measures the total number of 512-1023 byte frames received (excluding framing bits, but including Frame Check Sequence (FCS) octets).			Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder
SIZE1024-1518 Total 1024-1518 Byte Frame Count in Receive Direction measures the total number of 1024-1518 byte frames received (excluding framing bits, but including Frame Check Sequence (FCS) octets).			Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder
TBYC-RX Total Byte Count in Receive Direction measures the total number of bytes of data (including those in bad frames) received (excluding framing bits, but including Frame Check Sequence (FCS) octets).			Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder
TFRC-RX Total Frame Count in Receive Direction measures the total number of frames (bad frames, broadcast frames, and multicast frames) received.			Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder
USIZE Undersized Frames measures the total number of frames received that were less than 64 octets long (excluding framing bits, but including Frame Check Sequence (FCS) octets) and were otherwise well formed.	0	0	Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder

Table 8-7 10GELAN PMs (counters)

PM (montype)	PM threshold default values		Supported modules
	15-minute bin	1-day bin	

¹The maximum frame size on the BT7A49AA and BT7A49AB modules is fixed at 9600 bytes. The maximum frame size on the BT7A49AA-I02 module is fixed at 10200 bytes.

Table 8-8 SONET PMs (counters)

PM (montype)	PM threshold default values		Supporting entities
	15-minute	1-day	
CVS Section Coding Violations measures the number of B1 Bit Interleaved Parity (BIP) errors detected at the section layer.	382	3820	OC3, OC12, OC48, OC192
ESS Section Errored Seconds measures the number of seconds during which one or more B1 Bit Interleaved Parity (BIP) errors were detected or a Severely Errored Frame (SEF) or a Loss of Signal (LOS) defect was present.	25	250	OC3, OC12, OC48, OC192
SEFS-S Section Severely Errored Framing Seconds measures the number of seconds during which a section SEF defect was present.	2	8	OC3, OC12, OC48, OC192
SESS Section Severely Errored Seconds measures number of seconds during which the number of detected B1 Bit Interleaved Parity (BIP) errors exceeds the severely errored seconds level (SESLVL), or a Severely Errored Frame (SEF) or a Loss of Signal (LOS) defect was present. The SESLVL value for SONET section level is as follows: <ul style="list-style-type: none"> • OC3 = 155 • OC12 = 616 • OC48 = 2392 • OC192 = 8554 	4	40	OC3, OC12, OC48, OC192
UAS-S Section Unavailable Seconds measures the number of seconds during which the SONET section is unavailable. A second is considered UAS-S at the onset of 10 consecutive SESS seconds, and is no longer considered UAS-S after 10 consecutive seconds that are not SESS seconds. In seconds that are counted as unavailable, the counting of CVS, ESS and SESS are inhibited.	10	10	OC3, OC12, OC48, OC192

Note For information about SONET protocols supported on Transponder modules, see the *Transponder Solutions Guide*.

Table 8-9 SDH PMs (counters)

PM (montype)	PM threshold default values		Supported entities
	15-minute	1-day	
RS-EB Regenerator Section Errored Blocks measures the number of regenerator section errored blocks. An errored block is one that contains one or more (up to eight per block) B1 Bit Interleaved Parity (BIP) errors.	0	0	STM16, STM64
RS-BBE Regenerator Section Background Block Errors measures the number of errored blocks not occurring during seconds counted as RS-SES seconds.	382	3820	STM16, STM64
RS-ES Regenerator Section Errored Seconds measures the number of seconds during which one or more errored blocks were detected or a Loss of Frame (LOF) or a Loss of Signal (LOS) defect was present.	25	250	STM16, STM64
RS-OFS Regenerator Section out of Frame Seconds measures the number of seconds during which an Out of Frame (OOF) defect was present.	2	8	STM16, STM64
RS-SES Regenerator Section Severely Errored Seconds measures the number of seconds during which the number of detected errored blocks exceeds the severely errored seconds level (SESLVL), or a Loss of Frame (LOF) or Loss of Signal (LOS) defect was present. The SESLVL value for SDH regenerator section is 30% of the nominal block rate.	4	40	STM16, STM64
RS-UAS Regenerator Section Unavailable Seconds measures the number of seconds during which the regenerator section is unavailable. A second is considered RS-UAS at the onset of 10 consecutive RS-SES seconds, and is no longer considered RS-UAS after 10 consecutive seconds that are not RS-SES seconds. In seconds that are counted as unavailable, the counting of RS-EB, RS-BBE, RS-ES, and RS-SES is inhibited.	10	10	STM16, STM64

Note For information about SDH protocols supported on Transponder modules, see the *Transponder Solutions Guide*.

Table 8-10 Layer 1 Fibre Channel PMs (counters)

PM (montype)	PM threshold default values		Supported modules
	15-minute	1-day	
CV 8B/10B Coding Violations measures the number of 8B/10B coding violations and disparity errors.	382	3820	Dual 4G Multiprotocol Transponder
INVBLK Invalid Blocks measures the number of invalid 64/66B coding blocks.	382	3820	Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder
ES Errored Seconds measures the number of seconds during which one or more coding violations are detected, or a Loss of Synchronization (LOSYNC) or Loss of Signal (LOS) defect is present.	25	250	Dual 4G Multiprotocol Transponder Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder
SES Severely Errored Seconds measures the number of seconds during which the number of detected coding violations exceeds the severely errored seconds level (SESLVL), or a Loss of Synchronization (LOSYNC) defect or Loss of Signal (LOS) defect is present. The SESLVL value for Fiber Channel is 1250.	4	40	Dual 4G Multiprotocol Transponder Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder
UAS Unavailable Seconds measures the number of seconds during which the link was considered unavailable. A link becomes unavailable at the onset of 10 consecutive seconds that qualify as SES, and continues to be unavailable until the onset of 10 consecutive seconds that do not qualify as SES.	10	10	Dual 4G Multiprotocol Transponder Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder

Table 8-11 OTN PMs (counters) supported on SONET/SDH line protocols

PM (montype)	PM threshold default values		Supported modules
	15-minute bin	1-day bin	
NUMBITSCR Number of Bits Corrected measures the total number of bits corrected by the Forward Error Correction (FEC) decoder according to the Reed-Solomon RS(255,239) forward error correction scheme.	0	0	Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder
NUMBYTESCR Number of Bytes Corrected measures the total number of bytes corrected by the forward error correction scheme.	0	0	Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder

Table 8-11 OTN PMs (counters) supported on SONET/SDH line protocols (Continued)

PM (montype)	PM threshold default values		Supported modules
	15-minute bin	1-day bin	
Note			
Not supported on line protocols OC192EFEC and STM64EFEC.			
UNCRCDWRD	10	100	Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder
Number of Uncorrectable Code Words measures the total number of errored code words received that could not be corrected by the Forward Error Correction scheme.			
BER			Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder
Bit Error Ratio provides an estimate of the instantaneous Bit Error Ratio of the line by evaluating the ratio of the number of bits corrected to the total bits received over a 10-second time window. Both the instantaneous and average BER values are only valid for relatively low error rates in the signal. If the BER value is reported to be above 10 ⁻³ , it should be disregarded as it is not possible to accurately measure BER values above this level. BER values above this level usually indicate another problem, which should be evident in other PM counts.			
BER-AVG			Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder
Average Bit Error Ratio provides an estimate of the average Bit Error Ratio of the line by evaluating the ratio of the number of bits corrected to the total bits received over the duration of the entire collection interval. Both the instantaneous and average BER values are only valid for relatively low error rates in the signal. If the BER value is reported to be above 10 ⁻³ , it should be disregarded as it is not possible to accurately measure BER values above this level. BER values above this level usually indicate another problem, which should be evident in other PM counts.			
OTU-BBE	382	3820	Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder
OTU-2 Background Block Error measures the number of errored blocks not occurring during seconds counted as OTU-SES seconds.			
OTU-EB	0	0	Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder
OTU-2 Errored Blocks measures the number of frames containing one or more Bit Interleaved Parity (BIP) errors, using the OTU-2 SM BIP-8 byte in the incoming OTN signal. Up to eight BIP-8 errors can be detected per OTU-2 frame. However, regardless of the number of BIP-8 errors detected, a single frame can count for no more than one errored block.			
Note			
EB counting is suspended when either one of the following faults is active on the port: Loss of Signal, Loss of Frame.			

Table 8-11 OTN PMs (counters) supported on SONET/SDH line protocols (Continued)

PM (montype)	PM threshold default values		Supported modules
	15-minute bin	1-day bin	
OTU-ES OTU-2 Errored Seconds measures the number of seconds during which one or more errored blocks is detected or a Loss of Frame (LOF), Loss of Signal (LOS), or Trace Identifier Mismatch (TIM) defect is present.	25	250	Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder
OTU-SES OTU-2 Severely Errored Seconds measures the number of seconds during which the number of detected errored blocks exceeds the severely errored seconds level (SESLVL), or a Loss of Frame (LOF), Loss of Signal (LOS), or Trace Identifier Mismatch (TIM) defect was present. The SESLVL value for OTN is 30% of the nominal block rate.	4	40	Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder
OTU-OFS OTU-2 Out of Frame Seconds measures the number of seconds during which a Out of Frame (OOF) defect was present.	2	8	Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder
OTU-UAS OTU-2 Unavailable Seconds measures the number of seconds during which the OTN line is unavailable. A second is considered OTU-UAS at the onset of 10 consecutive OTU-SES seconds, and is no longer considered OTU-UAS after 10 consecutive seconds that are not OTU-SES seconds.	10	10	Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder

8.3.1.4 Physical PMs

Table 8-12 Physical PMs (gauges)

PM (montype)	Supported transceivers
Optical Power Received (OPR MIN, OPR MAX, OPR AVG) Optical Power Received measures the minimum, maximum, and average optical power (dBm) received. Measurements are accurate to ± 3.0 dBm for SFPs; to ± 2.0 dBm for XFPs.	Noncopper SFPs All XFPs
Optical Power Transmitted (OPT MIN, OPT MAX, OPT AVG) Optical Power Transmitted measures the minimum, maximum, and average optical power (dBm) transmitted. Measurements are accurate to ± 3.0 dBm for SFPs; to ± 2.0 dBm for XFPs.	Noncopper SFPs All XFPs
Supply Voltage Supply Voltage measures the supply voltage on the 3.3V supply for SFPs; on the 5.0V supply for XFPs. This PM is not supported on all XFPs and the PM line will contain "NA" instead of "CMPL" or "PRTL".	Noncopper SFPs All XFPs
Supply Voltage 2	All XFPs

Table 8-12 Physical PMs (gauges) (Continued)

PM (montype)	Supported transceivers
Supply Voltage 2 measures the supply voltage on the 3.3V supply. This PM is not supported on all XFPs and the PM line will contain "NA" instead of "CMPL" or "PRTL".	
Temperature	All SFPs
Temperature measures the temperature (°C) of the transceiver.	All XFPs
Tx Bias current	Noncopper SFPs
Laser Bias Current measures the laser bias current (mA).	All XFPs

Note Physical PMs are not supported on SFPs on SCP modules and Expansion Shelf Interface ports.

8.3.1.5 Threshold crossing alerts for transceiver ports

The following threshold crossing alerts (TCAs) are available to most transceiver ports equipped with SFPs or XFPs. For information about threshold crossing alerts for supported protocols, see [9.2, “Monitoring threshold crossing alerts”](#).

Table 8-13 TCAs for transceiver ports equipped with SFPs or XFPs

TCA	Range	Description
OPTLT	Integer	Optical power transmitted low threshold. This value is retrieved from the SFP/XFP and is not provisionable.
OPTHT	Integer	Optical power transmitted high threshold. This value is retrieved from the SFP/XFP and is not provisionable.
OPRLT	Integer	Optical power received low threshold. This value is retrieved from the SFP/XFP and is not provisionable.
OPRHT	Integer	Optical power received high threshold. This value is retrieved from the SFP/XFP and is not provisionable.

These TCAs are available when the digital diagnostics implementation (DDIAGIMP) flag for the transceiver is set to yes (Y) in its inventory entry and the Physical PM Monitor parameter is enabled when the transceiver port settings are provisioned.

8.3.1.6 Bulk port provisioning

Systems that contain many Transponder ports of the same type can be provisioned quickly using bulk port provisioning.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

Prerequisites

- Before you can bulk provision ports, you must provision the modules.
- At least one Master Port must be provisioned and available for port cloning.

The following table provides details about the bulk port provisioning parameters:

Parameter	Description	Configurable
Master Port	Contains a list of provisioned ports available for cloning	Yes
Initial State	List of initial states for the ports to be cloned. Values are: <ul style="list-style-type: none"> • OOS (Out of Service) • IS (In Service) • AINS (Auto-In-Service) 	Yes
Master Port Settings	Contains some of the provisioned parameters of the selected master Port that will be applied to the ports. The following parameters are common to all ports: <ul style="list-style-type: none"> • Protocol • Wavelength • Physical PM Monitoring • Fault Propagation Shutdown • SD Bit Error Rate Additional items for Muxponder ports: <ul style="list-style-type: none"> • Line Mapping • Media Rate 	Yes
Available Ports to Provision	Lists the available unprovisioned ports that are compatible with the selected master port. On Transponder Modules: <ul style="list-style-type: none"> • If the selected master port is a line port, line ports 1 and 3 display. • If the selected master port is a client port, client ports 2 and 4 display. 	Yes
Selected ports	Lists the ports to which you want to apply master port provisioning. When a port is added to this list, it is removed from the Available Ports list.	Yes
Ignore Change Events	Parameter is available only during the provisioning phase. When checked, blocks messages about change notifications such as: <ul style="list-style-type: none"> • a port in the Master Port list has been deleted • a port in the Available Ports list has been provisioned • a port in the Selected Ports list has been provisioned 	Yes

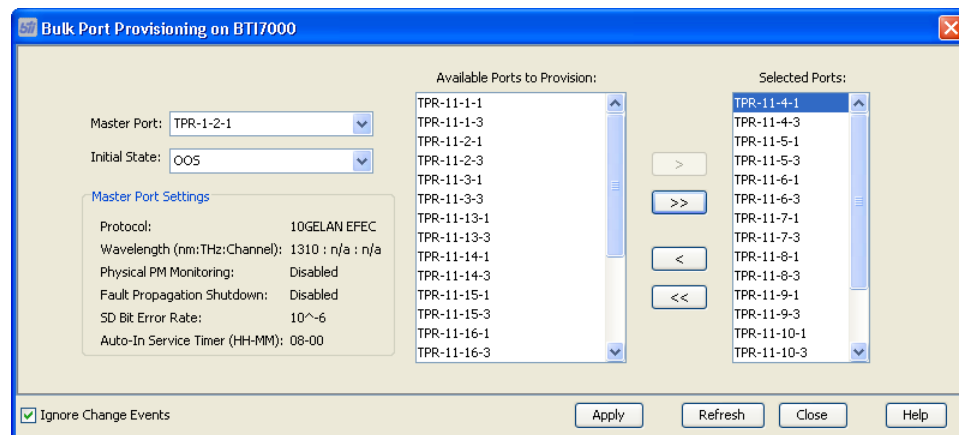
Parameter	Description	Configurable
	<ul style="list-style-type: none"> a card of the Master Port's parent class has been provisioned or deleted 	

Use this procedure to bulk provision ports on Transponder modules.

Step 1 On the Tools menu, select **Bulk Tools > Bulk Port Provisioning**. Alternatively, right-click on Main Shelf graphic on the right and choose **Bulk Port Provisioning**.

You can also right-click on the System or Shelf in the Navigation tree and choose **Bulk Port Provisioning**. When you access bulk port provisioning from the Navigation tree, only the ports specific to the shelf are available.

The Bulk Port Provisioning window displays.



Step 2 From the **Master Port** drop-down box, select a Master port. The settings for the selected Master Port display in the Master Port Settings area.

Step 3 From the **Initial State** drop-down box, select an initial state for the port.

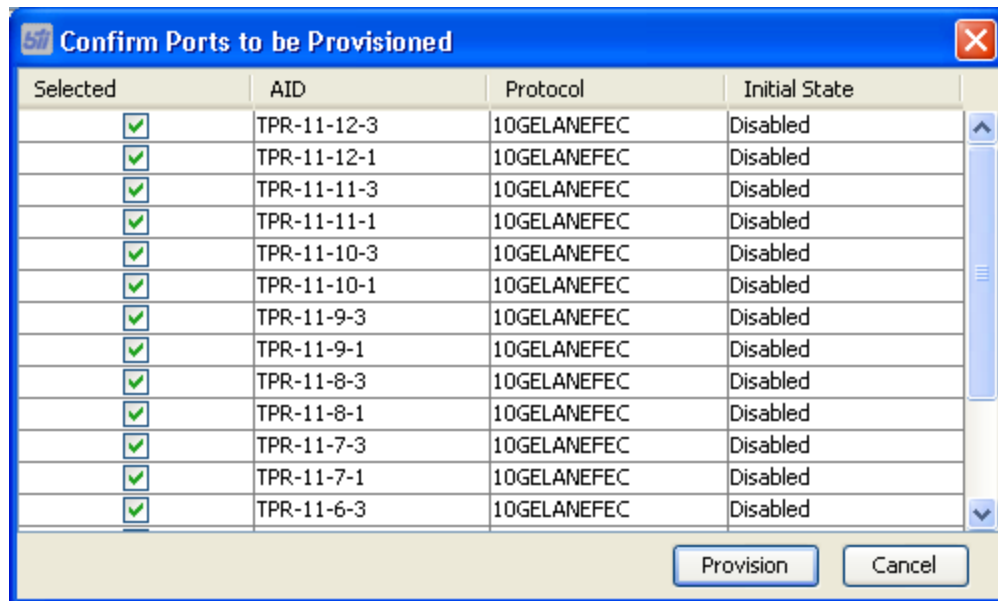
Step 4 In the **Available Ports to Provision** list, shift-click to highlight the ports that are to be provisioned.

Step 5 To move ports:

- Click the Move Right button (>) to move the items selected in the **Available Ports** list to the **Selected Ports** list.
- Click the Move All Right button (>>) to move the entire **Available Ports** list to the **Selected Ports** list.
- Click the Move Left button (<) to move the items selected in the **Selected Ports** list to the **Available Ports** list.
- Click the Move All Left button (<<) to move the entire **Selected Ports** list to the **Available Ports** list.

Step 6 Click **Apply**.

The ports are moved to the **Selected Ports** list and are cloned with the Master port and with the initial state settings. A confirmation window displays with the ports to be provisioned. A confirmation window appears, prompting you to review all the objects that are to be created. You can remove individual items from the list, if required, by unchecking the **Selected** box.



Step 7 Click **Provision**.

8.3.2 Display transceiver information

Use this procedure to view provisioned and non-provisionable parameters for an SFP or XFP transceiver inserted in a port of a module.



Prerequisites

- The SFP or XFP transceiver must be physically present in the port.

Displaying SFP or XFP information

Follow these steps to view inventory information for an SFP or XFP transceiver.

Step 1 In the Navigation pane, right-click a port in which a module is installed, and then click **Display Inventory**.

The **Display Inventory Information** dialog displays **General**, **Characteristic**, and **Vendor** parameters for the SFP transceiver. See [Table 8-14](#).

Step 2 Click **Close**.

You have successfully completed this procedure.

Table 8-14 SFP or XFP transceiver inventory information

Parameter	Range of Values	Description
Full Name	Alphanumeric characters	Full name of the transceiver
Name	Alphanumeric characters	Short name of the transceiver (SFP or XFP)
Shelf Number	Integer	The shelf in which the module is installed
Slot Number	Integer	The slot in which the module is installed
Port Number	Integer	The module port in which the transceiver is inserted
Wavelength	Numeric	<p>The wavelength of the transceiver in nm.</p> <p>Note</p> <p>Some transceivers have a wavelength value that is specified only to the nearest nm, whereas others specify wavelength to the nearest 0.01 nm.</p> <p>Note</p> <p>If a transceiver that does not have a wavelength value specified in its memory is inserted into a module, a REPLUNITUNK alarm is raised against the transceiver.</p>
Minimum Wavelength Note This parameter is supported by a tunable XFP only.	Numeric	The minimum wavelength supported, represented in nm with 0.01 nm resolution.
Maximum Wavelength Note This parameter is supported by a tunable XFP only.	Numeric	The maximum wavelength supported, represented in nm with 0.01 nm resolution.
Wavelength Spacing Note This parameter is supported by a tunable XFP only.	Numeric	The grid spacing in GHz (100GHz, 50GHz)
Reach	Numeric	<p>The maximum transmit distance of the transceiver in kilometers using 9 micron SM fiber.</p> <p>Note</p> <p>If a transceiver that does not have a reach value specified in its memory is inserted</p>

Table 8-14 SFP or XFP transceiver inventory information (Continued)

Parameter	Range of Values	Description
		into a module, a REPLUNITUNK alarm is raised again
Connector Type	LC	The listed transceiver connector type
Digital Diagnostics Implemented	Yes No	The digital diagnostic implementation parameter. When set to Yes, this parameter enables the recording of performance data in historical bins. Note If this parameter is set to No or is not specified in the transceiver's memory, all historical bins are filled with dummy values and marked as invalid.
Tx Fault Implemented	Yes No	The transceiver fault implemented parameter on the transceiver Note The system allows transceivers that do not use this flag to indicate through the inventory table that the installed transceiver will never indicate a transmitter fault.
Signal Encoding	8B10B 4B5B NRZ MANCHESTER SONET_SCRAMBLED	The encoding scheme for the transceiver Note The system does not use the encoding parameter. It is the operating company's responsibility to ensure that both end points of a span use the same encoding.
Minimum bit rate	Integer	The minimum bit rate supported by the transceiver Note If a transceiver inserted in a module port does not have a minimum baud rate value specified in its memory, the system raises a REPLUNITUNK alarm against the transceiver.
Maximum bit rate	Integer	The maximum bit rate supported by the transceiver Note If a transceiver inserted in a module port does not have a maximum baud rate value specified in its memory, the system raises a REPLUNITUNK alarm against the transceiver.
Nominal bit rate	Integer	The nominal bit rate supported by the transceiver

Table 8-14 SFP or XFP transceiver inventory information (Continued)

Parameter	Range of Values	Description
Note If a transceiver inserted in a module port does not have a nominal baud rate value specified in its memory, the system raises a REPLUNITUNK alarm against the transceiver.		
LOS implemented	Yes No	The loss of signal implementation parameter. When set to Yes, this parameter raises the LOS alarm against the transceiver.
Tx Disable Implemented	Yes No	The transceiver disable implemented parameter. When set to Yes, this parameter disables the transmitter of the transceiver when the module is placed in the Out of Service state.
Media	Electrical Optical Unknown	The type of connector used by the transceiver
PEC Code	String	The product equipment code assigned by the manufacturer
Name	Alphanumeric characters	The name of the transceiver's vendor
Part Number	Alphanumeric characters	The part number assigned to the transceiver by the vendor
OUI	Alphanumeric characters	The vendor's organization unique identifier
CLEI Code	String	The Common Language Equipment Identifier number assigned by Telcordia. The CLEI identifies the physical hardware.
Serial Number	Integer	The serial number of the transceiver
Release Number	Alphanumeric characters	The hardware release number
Manufacturing Date	YYYY-MM-DD	The date that the transceiver was manufactured

8.3.3 Display port information for a Transponder module

Use this procedure to view provisioned and non-provisionable parameters for port on a Transponder module.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

Prerequisites

- None

Displaying port information

Follow these steps to view port information for a Transponder module.

Step 1 In the toolbar, click the System Configuration button.

Step 2 In the Navigation pane, right-click a port on a module, and then click **Provision Transceiver**.

The **Provision Transceiver** dialog displays the port parameters on the **Transceiver** tab and the **Custom Info** tab. For information on the port parameters, see [8.3.1, “Provision port settings on a Transponder module”](#).

Step 3 Click **Close**.

You have successfully completed this procedure.

8.3.4 Modify port settings on a Transponder module

Use this procedure to modify provisionable settings for a port on a BTI 7000 Series Transponder module.



Prerequisites

- If the Wavelength parameter is to be modified, the port must be removed from service.

Modifying port settings

Follow these steps to modify provisionable port settings on a Transponder module:

Step 1 In the toolbar, click the System Configuration button.

Step 2 In the Navigation pane, right-click a port on a Transponder module, and then click **Provision Port**.

Step 3 In the **Provision Port** dialog, modify the provisionable parameters for the port. See [8.3.1, “Provision port settings on a Transponder module”](#) for information.

Step 4 Click **Apply**.

You have successfully completed this procedure.

8.3.5 Remove a port from service

Use this procedure to remove a port on a Transponder module from service.



Prerequisites

- Port must be provisioned and in service.

Removing a port from service

Follow these steps to remove a port on a Transponder module from service:

- Step 1** In the toolbar, click the System Configuration button.
- Step 2** In the Navigation pane, right-click a port on a Transponder module, and then click **Provision Transceiver**.
- Step 3** On the **Settings** tab of the **Provision Transceiver** dialog, click the **Remove** button beside the **State** field.
- Step 4** Click **Close**.

You have successfully completed this procedure.

8.3.6 Restore a port to service

Use this procedure to restore a port on a Transponder module to service.

**Prerequisites**

- Port must be provisioned and out of service.

Restore a port to service

Follow these steps to restore a port on a Transponder module to service:

- Step 1** In the toolbar, click the System Configuration button.
- Step 2** In the Navigation pane, right-click a port on a Transponder module, and then click **Provision Transceiver**.
- Step 3** On the **Settings** tab of the **Provision Transceiver** dialog, click the **Restore** button beside the **State** field.
- Step 4** Click **Close**.

You have successfully completed this procedure.

8.3.7 Delete a port

Use this procedure to delete a port on a Transponder module.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

Prerequisites

- Port must be provisioned and removed from service.
- Port must not be in use in a cross-connection or a protection group.

Deleting a port

Follow these steps to delete a port on a Transponder module:

Step 1 In the toolbar, click the System Configuration button.

Step 2 In the Navigation pane, right-click a port on a Transponder module, and then click **Delete Transceiver**.

Step 3 In the **Delete Transceiver** confirmation dialog, click **Yes**.

You have successfully completed this procedure.

8.3.8 View the Transponder tuning grid

The Transponder tuning grid window lets you view a summary of configuration and performance monitoring information by protocol for Transponder ports.

Use this procedure to view the Transponder tuning grid.

Step 1 From the main menu choose **View->View Transponder Tuning Grid**, or

- In the toolbar, click the System Configuration button.
- Right-click on the BTI 7000 Series folder in the left navigation pane.
- From the drop-down menu, choose the **View Transponder Tuning Grid**.
The **Transponder Tuning Grid** window displays.

Field	Description
Port	The port on the Transponder module
Protocol	The Transponder module protocol.
Wavelength	Wavelength frequency can be in nm, THz, or Channel.
OPT (dBm)	Optical power transmitted in dBm.
OPR (dBm)	Optical power received in dBm.
BER	Bit Error Ratio
ES	Errored Seconds
UAS	Unavailable Seconds
State	Indicates the status of the port. Range of values is: <ul style="list-style-type: none"> • OOS-AU - Out of Service–Autonomous

Field	Description
	<ul style="list-style-type: none"> AINS&FLT - Automatic in service, fault secondary state FLT - fault secondary state OOS-AUMA - Out of Service—Autonomous and Management MT&FLT - Maintenance, Fault secondary stat
Vendor	The transceiver manufacturer.

The following table provides the PM points that are available by protocol for the Transponder module.

Protocol	ES	UAS	BER
10GELAN	ES	UAS	n/a
OC192	ESS	UAS-S	n/a
STM64	RS-ES	RS-UAS	n/a
10GFC	ES	UAS	n/a
10GELANFEC	OTU-ES	OTU-UAS	BER
10GLANEFEC	OTU-ES	OTU-UAS	BER
OC192FEC	OTU-ES	OTU-UAS	BER
OC192EFEC	OTU-ES	OTU-UAS	BER
STM64FEC	OTU-ES	OTU-UAS	BER
STM64EFEC	OTU-ES	OTU-UAS	BER
ODU1OTU2FEC	OTU-ES	OTU-UAS	BER

For more information about Transponder PMs, see [9.1, “Retrieving and exporting performance metrics for Transponder modules”](#), and [8.3.1.4, “Physical PMs”](#).

Step 2 Click **Close**.

8.4 General Communications Channel

The BTI 7000 Series uses the general communications channel (defined in ITU-T standard G.709-2003) to form an IP-based network for management communications. Service Providers can use the GCC to manage their networks without impacting customer bandwidth, or using another wavelength on their fibers. BTI uses the GCC0 bytes defined in the OTU2 overhead to form a 1.3 Mb/s channel for management traffic.

GCC0 functionality requires that OSPF be enabled and that the GCC0 exist before the GCC0 itself is enabled on a GCC-capable port of a supporting module. Once the GCC0 is enabled, it can be removed from service when necessary and then restored to service, and it can be disabled. For detailed information about the GCC0, the modules on which it is supported, the applications and configurations it supports, and enabling OSPF, see the *BTI 7000 Series Management Communication Channels Solutions Guide*.

8.4.1 Enable the General Communications Channel

Use this procedure to enable the General Communications Channel on a GCC-capable port on any of the following modules:

- Dual 10G Multiprotocol Transponder
- 10G Multiprotocol Transponder module
- packetVX Integrated Packet Services Module - 24/2



Prerequisites

- The GCC0 must exist and the OSPF must be enabled. See the *Management Communications Channel Solutions Guide* for detailed information.
- The module port must be provisioned to use an OTN protocol.
- The port laser control parameter must be configured to allow software to automatically control the laser status.

Enabling the GCC0

Follow these steps to enable the GCC0:

- Step 1** In the toolbar, click the System Configuration icon. The System Configuration view of the shelf displays in the Navigation pane.
- Step 2** In the Navigation pane, right-click a GCC-capable module, and click **Provision GCC0**. The **Provision <module>** dialog appears.
- Step 3** In the **Provision Port<module>** dialog, click the **GCC0** tab.

Step 4 In the **Settings** area, select one of the following modes. By default, the mode is set at Disabled:

- **Full Rate** — to use the full available bandwidth of 1.3 Mb/s
- **Low Rate** — to limit channel traffic to 192/Kbs

Step 5 Click **Apply**.

You have successfully completed this procedure.

8.4.2 Remove the General Communications Channel from service

Use this procedure to remove the General Communications Channel from service.



Prerequisites

- The GCC0 must be enabled.

Removing the GCC0 from service

Follow these steps to remove the GCC0 from service:

Step 1 In the Navigation pane, right-click a GCC-capable port, and click **Provision GCC0**.

Step 2 In the **Provision<module type> <shelf-slot-port>** dialog, click the **GCC0** tab.

Step 3 In the **State Management** area, click **Remove**.

Step 4 Click **Apply**.

You have successfully completed this procedure.

8.4.3 Restore the General Communications Channel to service

Use this procedure to restore the General Communications Channel to service.



Prerequisites

- The GCC0 must be enabled and removed from service.

Restoring the GCC0 to service

Follow these steps to restore the GCC0 to service:

Step 1 In the Navigation pane, right-click a GCC-capable port on a module, and click **Provision GCC0**.

Step 2 In the **Provision**<module type> <shelf-slot-port> dialogue, click the **GCC0** tab.

Step 3 In the **State Management** area, click **Restore**.

Step 4 Click **Apply**.

You have successfully completed this procedure.

8.4.4 Disable the General Communications Channel

Use this procedure to disable the General Communications Channel.



Prerequisites

- The GCC0 must be enabled.

Disabling the GCC0

Follow these steps to disable the GCC0:

Step 1 In the Navigation pane, right-click a GCC-capable port on a module, and then click **Provision Port**.

Step 2 In the **Provision Port** dialog, click the **GCC0** tab.

Step 3 On the **GCC0** tab, choose **Disabled** from the **GCC0 Mode** list.

Step 4 Click **Apply**.

You have successfully completed this procedure.

8.5 Provisioning cross-connections on Transponder modules

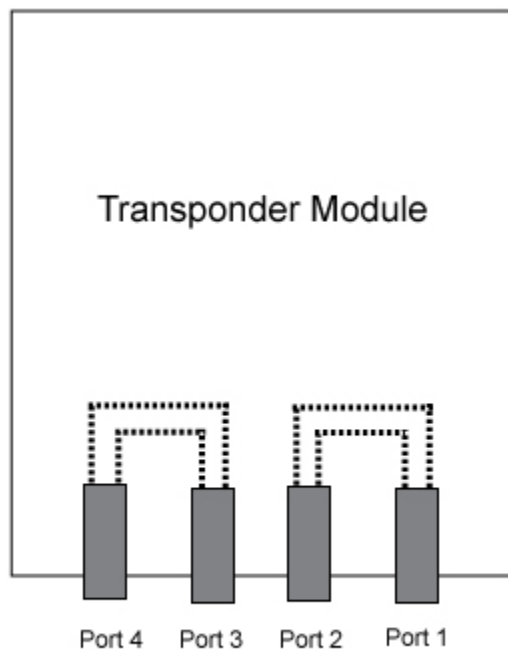
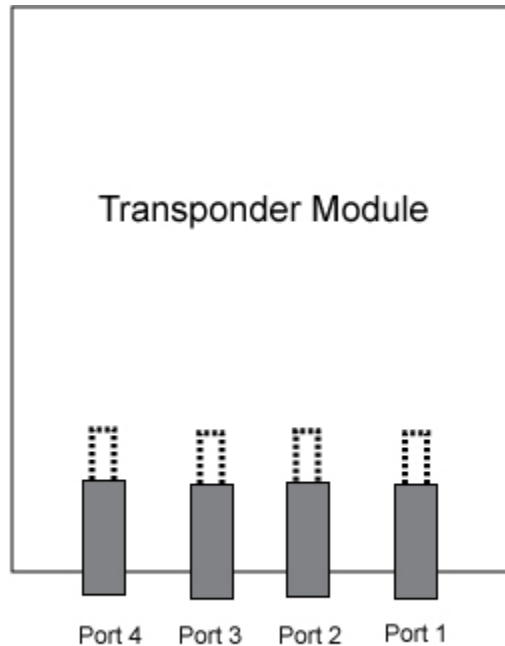
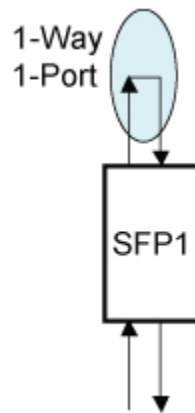
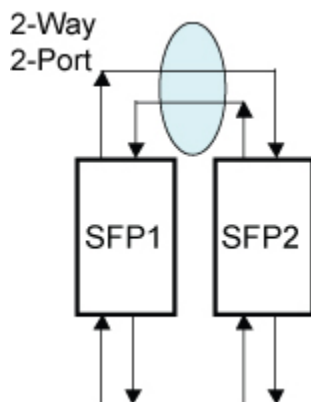
Cross-connections provide connectivity between transceiver ports on a Transponder module. A 1-Way cross-connection is a unidirectional connection, where the source is the receiver side of the transceiver and the destination is the transmitter side of the same transceiver. A 2-Way cross-connection is a bidirectional connection, where the source is the receiver side of one transceiver and the destination is the transmitter side of another transceiver.

The following table identifies the cross-connection configurations that Transponder modules support.

Table 8-15 Supported cross-connection configurations

Cross-connection type	Transponder modules
2-Way, 2-Port	Dual 1G Multiprotocol Transponder modules
	Dual 2.5G Multiprotocol Transponder modules
	Dual 4G Multiprotocol Transponder module
	Dual 10G Multiprotocol Transponder module
	Dual 10G Multiprotocol Transponder Lite module
	10G Multiprotocol Transponder module
1-Way, 1-Port	Dual 1G Multiprotocol Transponder modules
	Dual 2.5G Multiprotocol Transponder modules
	Dual 4G Multiprotocol Transponder module

The following figures illustrate cross-connection configurations supported on Transponder modules.

Cross-connection configurations 1**2-Way, 2-Port Cross-Connections****1-Way, 1-Port Cross-Connections****Cross-connection configurations 2**

This section covers the following topics:

- [8.5.1, “Provision a cross-connection ”](#)
- [8.5.3, “Display cross-connection information”](#)
- [8.5.4, “Delete a cross-connection ”](#)

8.5.1 Provision a cross-connection

Use this procedure to provision a cross-connection that provides transceiver connectivity on a Transponder module.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

Prerequisites

- On Dual 1G, Dual 2.5G Multiprotocol Transponders, and Dual 4G Multiprotocol Transponders, transceiver ports must be provisioned to use the same protocol.

Note For information about 2-Way cross-connections and the protocol configurations that are supported on Dual 10G Multiprotocol Transponders, Dual 10G Multiprotocol Lite Transponders, and 10G Multiprotocol Transponders, see [8.5.1.1, “Supported protocol configurations for 2-Way, 2-Port cross-connections on 10G Transponder modules”](#).

Restrictions

The following restrictions, presented in TL1 syntax, should be considered when provisioning cross-connections on Dual 1G, Dual 2.5G and Dual 4G Multiprotocol Transponders:

- WT/WR/WB/TPR-<shelf#>-<slot#>-1,WT/WR/WB/TPR-<shelf#>-<slot#>-1:1WAY
- WT/WR/WB/TPR-<shelf#>-<slot#>-2,WT/WR/WB/TPR-<shelf#>-<slot#>-2:1WAY
- WT/WR/WB/TPR-<shelf#>-<slot#>-3,WT/WR/WB/TPR-<shelf#>-<slot#>-3:1WAY
- WT/WR/WB/TPR-<shelf#>-<slot#>-4,WT/WR/WB/TPR-<shelf#>-<slot#>-4:1WAY
- WT/WR/WB/TPR-<shelf#>-<slot#>-1,WT/WR/WB/TPR-<shelf#>-<slot#>-2:2WAY
- WT/WR/WB/TPR-<shelf#>-<slot#>-3,WT/WR/TPR-<shelf#>-<slot#>-4:2WAY
- Typically, the following restriction, presented in TL1 syntax, should be considered when provisioning cross-connections on a 10G Multiprotocol Transponder:
 - TPR-<shelf#>-<slot#>-1,TPR-<shelf#>-<slot#>-2:2WAY
- Typically, the following restrictions, presented in TL1 syntax, should be considered when provisioning cross-connections on Dual 10G Multiprotocol Transponder and Dual 10G Multiprotocol Transponder Lite modules:
 - TPR-<shelf#>-<slot#>-1,TPR-<shelf#>-<slot#>-2:2WAY
 - TPR-<shelf#>-<slot#>-3,TPR-<shelf#>-<slot#>-4:2WAY
- A cross-connection cannot be modified. To modify a cross-connection, delete it, and then create a new cross-connection.
- Two or more source ports cannot be multiplexed to a single destination port.

Provisioning a cross-connection

Follow these steps to provision a cross-connection on a Transponder module.

Step 1 In the toolbar, click the **System Configuration** button.

Step 2 In the Navigation pane, right-click **Cross Connects** for a Transponder module, and then click **Provision Cross Connects**.

Step 3 In the **Cross Connects** dialog for the module, click the **Add** button.

Step 4 In the **Add Cross Connect** dialog, choose a value from the following lists:

- **Source**
- **Destination**
- **Direction**

Step 5 Click **Apply**.

Step 6 Optionally, repeat steps 1 to 4 for each additional cross-connection that you want to provision, and then click **Close**.

You have successfully completed this procedure.

8.5.1.1 Supported protocol configurations for 2-Way, 2-Port cross-connections on 10G Transponder modules

Note The Dual 10G Multiprotocol Transponder Lite module supports regeneration for all protocols, but does not support protocol translation.

10GELAN cross-connections

Table 8-16 Supported protocol configurations for 10GELAN cross-connections

Line protocol (P1, P3)	Client protocol (P2, P4)	Dual 10G Multiprotocol Transponder Ports	Dual 10G Multiprotocol Lite Transponder Ports	10G Multiprotocol Transponder Ports
10GELAN	10GELAN	1, 2 and/or 3,4	1, 2 and/or 3,4	1, 2
10GELANFEC	10GELAN	1, 2 and/or 3,4	NA	1, 2
10GELANFEC	10GELANFEC	1, 2 and/or 3,4	1, 2 and/or 3,4	1, 2
10GELANEFEC	10GELAN	1, 2 and/or 3,4	NA	1, 2
10GELANEFEC	10GELANEFEC	1, 3	1, 2 and/or 3,4	NA
10GELANFEC EPCMF	10GELAN	1, 2 and/or 3,4	NA	1, 2
10GELANFEC EPCMF	10GELANFEC EPCMF	1, 2 and/or 3,4	1, 2 and/or 3,4	1, 2
10GELANFEC EPCMF	10GELANEFEC EPCMF	1, 2 and/or 3, 4	1, 2 and/or 3,4	1, 2
10GELANEFEC EPCMF	10GELAN	1, 2 and/or 3,4	NA	1, 2
10GELANEFEC EPCMF	10GELANFEC EPCMF	1, 2 and/or 3,4	NA	1, 2

Table 8-16 Supported protocol configurations for 10GELAN cross-connections (Continued)

Line protocol (P1, P3)	Client protocol (P2, P4)	Dual 10G Multiprotocol Transponder Ports	Dual 10G Multiprotocol Lite Transponder Ports	10G Multiprotocol Transponder Ports
10GELANEFEC EPCMF	10GELANEFEC EPCMF	1, 3	1, 3	NA
OTU2eFEC	10GELAN	1, 2 and/or 3,4	NA	1, 2
OTU2eFEC	OTU2eFEC	1, 2 and/or 3,4	1, 2 and/or 3,4	1, 2
OTU2eFEC	OTU2eEFEC	NA	NA	NA
OTU2eEFEC	10GELAN	1, 2 and/or 3,4	NA	1, 2
OTU2eEFEC	OTU2eFEC	1, 2 and/or 3,4	NA	1, 2
OTU2eEFEC	OTU2eEFEC	1, 3	1, 3	NA

Fibre Channel cross-connections**Table 8-17 Supported protocol configurations for Fibre Channel cross-connections**

Line protocol (P1, P3)	Client protocol (P2, P4)	Dual 10G Multiprotocol Transponder Ports	Dual 10G Multiprotocol Lite Transponder Ports	10G Multiprotocol Transponder Ports
10GFC	10GFC	1, 2 and/or 3,4	1, 2 and/or 3,4	1, 2

OC192 cross-connections**Table 8-18 Supported protocol configurations for OC192 cross-connections**

Line protocol (P1, P3)	Client protocol (P2, P4)	Dual 10G Multiprotocol Transponder Ports	Dual 10G Multiprotocol Lite Transponder Ports	10G Multiprotocol Transponder Ports
OC192	OC192	1, 2 and/or 3,4	1, 2 and/or 3,4	1, 2
OC192FEC	OC192	1, 2 and/or 3,4	NA	1, 2
OC192FEC	OC192FEC	1, 2 and/or 3,4	1, 2 and/or 3,4	1, 2
OC192EFEC	OC192	1, 2 and/or 3,4	NA	1, 2
OC192EFEC	OC192FEC	1, 2 and/or 3,4	1, 2 and/or 3,4	1, 2
OC192EFEC	OC192EFEC	1, 3	1, 3	NA

STM64 cross-connections

Table 8-19 Supported protocol configurations for STM64 cross-connections

Line protocol (P1, P3)	Client protocol (P2, P4)	Dual 10G Multiprotocol Transponder Ports	Dual 10G Multiprotocol Lite Transponder Ports	10G Multiprotocol Transponder Ports
STM64	STM64	1, 2 and/or 3,4	1, 2 and/or 3,4	1, 2
STM64FEC	STM64	1, 2 and/or 3,4	NA	1, 2
STM64FEC	STM64FEC	1, 2 and/or 3,4	1, 2 and/or 3,4	1, 2
STM64EFEC	STM64	1, 2 and/or 3,4	NA	1, 2
STM64EFEC	STM64FEC	1, 2 and/or 3,4	1, 2 and/or 3,4	1, 2
STM64EFEC	STM64EFEC	1, 3	1, 3	NA

8.5.2 Bulk provision cross-connections

Use this procedure to quickly bulk provision cross-connections on a Transponder module.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

Prerequisites

- Before you can bulk provision cross-connections, the Transponder ports must be provisioned.
- Cross-connections that were provisioned using the bulk method must be deleted individually via existing interfaces.

Note Only 2-Way connections are supported.

Provisioning a cross-connection

The following table provides information about the bulk cross-connect provisioning parameters:

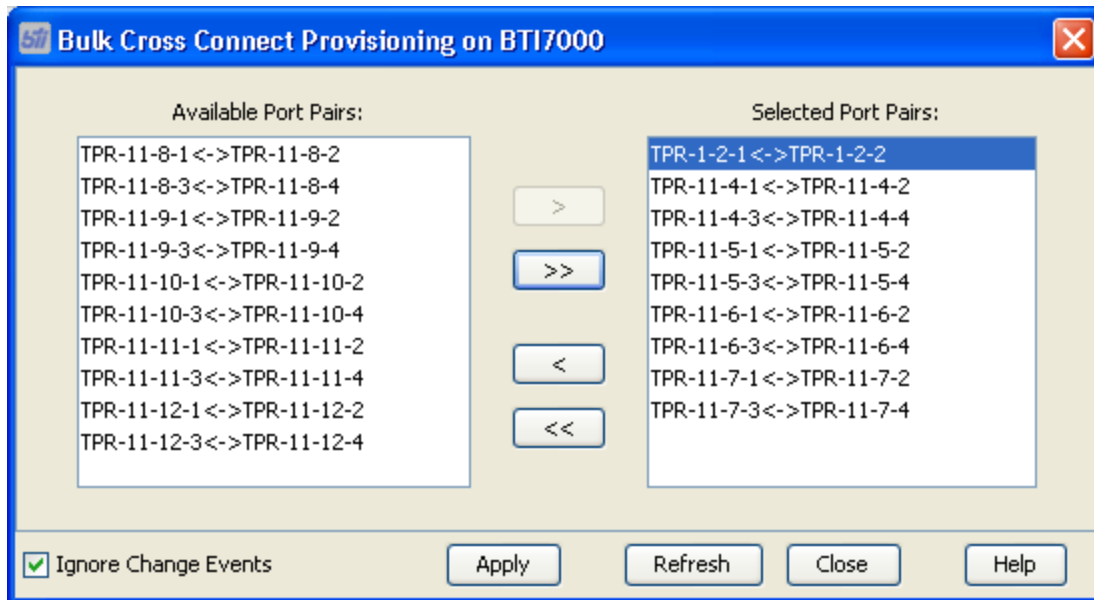
Parameter	Description	Configurable
Available Port Pairs	Lists the pairs of ports that can be cross-connected	Yes
Selected Port Pairs	Lists the port pairs that have been selected to cross-connect	Yes
Ignore Change Events	<p>Parameter is available only during the provisioning phase.</p> <p>When checked, blocks messages about change notifications such as:</p> <ul style="list-style-type: none"> • a cross-connect has been provisioned on one of the items listed on the Available Port Pairs or Selected Port Pairs • one of the ports listed in the Available Port Pairs list is deleted • one of the ports listed in the Selected Port Pairs list is deleted 	Yes

Parameter	Description	Configurable
	<ul style="list-style-type: none"> a Transponder port has been created 	

Follow these steps to bulk provision cross-connections on a Transponder module.

Step 1 On the **Tools** menu, select **Bulk Tools > Bulk Cross-Connect Provisioning**.

The **Bulk Cross-Connect Provisioning** dialog displays.



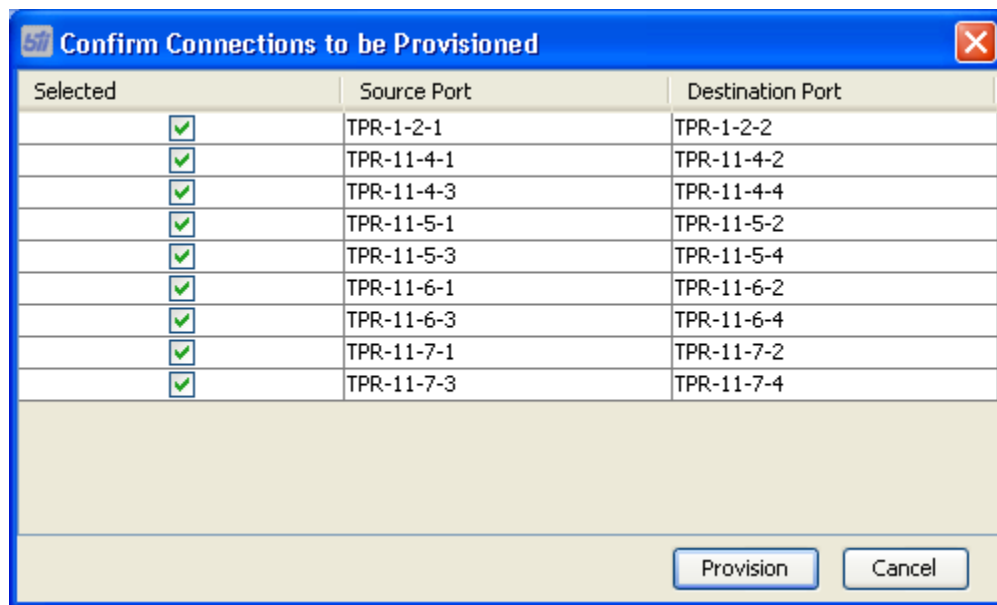
Step 2 In the **Available Port Pairs** panel, shift-click to select the port pairs that you want to cross-connect.

Step 3 To move cross-connects:

- Click the Move Right button (>) to move the items selected in the Available Port Pairs list to the **Selected Port Pairs** list.
- Click the Move All Right button (>>) to move the entire Available Port Pairs list to the **Selected Port Pairs** list.
- Click the Move Left button (<) to move the items selected in the **Selected Port Pairs** list to the **Available Port Pairs** list.
- Click the Move All Left button (<<) to move the entire **Selected Port Pairs** list to the **Available Port Pairs** list.

Step 4 Click **Apply**.

A confirmation window appears, prompting you to review all the objects that will be created. You can remove individual items from the list, if required, by unchecking the Selected box.



Step 5 Click **Provision**.

8.5.3 Display cross-connection information

Use this procedure to view display cross-connection information for a Transponder module.



Prerequisites

- Cross-connection must be provisioned.

Displaying cross-connection information

Follow these steps to display cross-connection information for a Transponder module:

Step 1 In the toolbar, click the System Configuration button.

Step 2 In the Navigation pane, right-click Cross-Connections for a Transponder module, and then click **Provision Cross Connections**.

The **Cross Connects** dialog for the Transponder displays the **Source**, **Destination**, and **Direction** for each cross-connection provisioned on the Transponder module.

Step 3 Click **Close**.

You have successfully completed this procedure.

8.5.4 Delete a cross-connection

Use this procedure to delete a cross-connection on a Transponder module.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

Prerequisites

- Cross-connection must be provisioned.

Deleting a cross-connection

Follow these steps to delete a cross-connection on a Transponder module:

- Step 1** In the toolbar, click the System Configuration button.
- Step 2** In the Navigation pane, right-click **Cross Connection** for a Transponder module, and then click **Provision Cross Connections**.
- Step 3** In the **Cross Connections** dialog for the Transponder module, click a listed cross-connection, and then click **Delete**.
- Step 4** In the **Delete Cross Connect** confirmation dialog, click **Yes**.
- Step 5** Optionally, repeat steps 1 to 3 for each cross-connection that you want to delete, and then click **Close**.

You have successfully completed this procedure.

8.6 Provisioning protection groups on Transponder modules

This topic describes provisioning line and client protection switching groups. For general information on provisioning Transponder modules refer to the *BTI 7000 Series Transponder Solutions Guide*.

- **line protection:** switching is performed between acting and protecting ports within the same Transponder module. In a protection group, one transceiver port on the Transponder module is provisioned as the working port and the other as the protecting port. Because the protection group works as a 1+1 non-revertive switch, the switching algorithm does not place any preference on either port to be the working facility. At any point, either the working or the protecting port can be carrying traffic if both ports are fault free.
- **client protection:** switching is performed between acting and protecting ports on two separate 10 G Transponder modules.

Prerequisites

Before you provision protection groups, you should be familiar with the provisioning considerations for line and client protection groups. Refer to the *BTI 7000 Series Transponder Solutions Guide*.

8.6.1 Provisioning considerations for line protection groups

This section describes provisioning considerations for line ports to be used in a line protection group.

- The Transponder module must support protection switching.
- The working and protecting transceiver ports must be provisioned and must use the same protocol.
- The working port and protecting transceiver ports cannot be involved in an existing protection group.
- The protecting port cannot be involved in a cross-connection provisioned on the module. Therefore, BTI recommends that cross-connections be provisioned on the Transponder module before protection groups are provisioned.
- The setting of the FPSD parameter on the working transceiver port and the protecting transceiver port must be the same; that is, the FPSD parameter on both ports is either enabled or disabled. See [8.3, “Provisioning ports on Transponder modules”](#) for information.
- On 1G Wavelength Regenerator, 2.5G Wavelength Regenerator, and Dual 4G Multiprotocol Transponder modules, typically, the protected port order is as follows:
 - Port 4 protects port 2, or vice versa
 - Port 3 protects port 1, or vice versa
- On Dual 10G Multiprotocol Transponder and Dual 10G Multiprotocol Transponder Lite modules, the protected port order is Port 3 protects port 1, or vice versa.

8.6.2 Provision line protection groups on a Transponder module

Use this procedure to provision line protection groups on a Transponder module.

Before you provision line protection groups, you should be familiar with the provisioning considerations. Refer to the *BTI 7000 Series Transponder Solutions Guide*.



Provisioning protection switching

Follow these steps to provision a line protection group on a Transponder module:

- Step 1** In the toolbar, click the System Configuration button
- Step 2** In the Navigation pane, select the shelf that you are provisioning.
- Step 3** Select the slot that contains the transponder that you are provisioning for protection. Right-click **Protection Groups** and click **Provision Protection Groups**.
The **Provision Transceiver Protection Groups** dialogue appears.
- Step 4** In the **Protection groups** dialog for the module, click **Add**.
- Step 5** In the **Add Protection Group** dialog, select the **Working Port**.

Note A line protection group is created when you select a line port as the **Working Port**.

The protecting transceiver port is automatically selected in the **Protection** list, and the provisioned **Protocol**, **Wavelength**, and **FPSD** parameters for each port appear.

- Step 6** Select the protection switch **Direction**.
Set the direction to UNI (unidirectional) or BI (bidirectional).

Note This option is not available for selection on all transponder modules.

- Step 7** Optionally, enter a name for the protection group in the **Protection ID** field.
- Step 8** Click **Apply**.

You have successfully completed this procedure.

8.6.3 Provisioning considerations for client protection groups

This section describes provisioning considerations for client ports to be used in a Y-cable client protection group. For more information about provisioning ports and protection groups on BTI Transponder modules refer to [8.2, “Provisioning Transponder modules”](#) and [8.6, “Provisioning protection groups on Transponder modules”](#).

Before you begin this procedure you should be familiar with the Transponder supported protocols listed in [Chapter 2, “Transponder features and supported protocols”](#)

- Client ports must be provisioned before they can be included in a protection group:
 - Client ports must be configured with the same supported protocol and the same fault propagation shutdown (FPSD) values. Values for other parameters may be different.
 - The client port number (2 or 4) must be the same for the working and protecting ports.
- Cross-connections:
 - Automatic port switching does not occur, for any reason, until cross-connection is provisioned.
 - The cross-connect must be created on only the provisioned working port.
 - The line port for the client protection group must be associated with the working port.
 - The cross-connect must be a 2WAY type.
 - The line port associated with the protecting port must be provisioned with the same supported protocol
 - The line and client port pairs that can be cross-connected are 1 and 2, and 3 and 4.
- Client port parameters, except protocol and FPSD, may be modified after the port is part of a protection group. Note that the mate client port is not automatically changed.
- The protection switch direction is set to BI and cannot be changed.
- A client port cannot be deleted once it is part of a protection group.
- The secondary state of a client port shows the status of the port, for example, active (WRK), standby (STDBY), forced (FRCD), or locked out (LKDO).
- After client protection is fully provisioned, for example, cross-connect and protection group are created, the protecting line port cannot be deleted. The protecting line port can be deleted after the cross-connect and protection group are deleted.
- Both ports in a protection group can report alarms, conditions, and performance metrics Threshold Crossing Alarms (TCAs), regardless of their status as active or standby.

8.6.4 Provision client protection groups on a Transponder module

Use this procedure to provision client protection groups on a Transponder module.

Before you provision protection groups, you should be familiar with the provisioning considerations. Refer to [8.6.3, “Provisioning considerations for client protection groups”](#).



Provisioning protection switching

Follow these steps to provision a client protection group:

- Step 1** In the toolbar, click the **System Configuration** icon.
- Step 2** In the Navigation pane, select the system and shelf that you are provisioning.
- Step 3** Select the slot that contains the transponder that you are provisioning for client protection. Right-click **Protection Groups** and click **Protection Groups**.
The **Provision Transceiver Protection Groups** dialogue appears.
- Step 4** Click **Add**. The **Provision Protection Group** dialogue appears.
- Step 5** From the **Working Port** field, select the working port from the drop-down menu. From the **Protecting Port** field, select the protecting port from the drop-down menu.

Note A client protection group is created when you select client ports in the **Working Port** and **Protecting Port** fields.

The provisioned **Protocol**, **Wavelength**, and **FPSD** parameters for each port appear. The **Direction** is automatically set to BI.

- Step 6** Option. Enter a name for the protection group in the **Protection ID** field.
- Step 7** Click **Apply**.

You have successfully completed this procedure.

8.6.5 Display protection-group information for a Transponder module

You can view information about each protection group provisioned on a Transponder module, and you can add or change the ID of provisioned protection groups, which can help you identify a specific protection group when more than one is provisioned on a module.



Follow these steps to view protection-group information for a Transponder module:

- Step 1** In the toolbar, click the System Configuration button.
- Step 2** In the Navigation pane, right-click **Protection Groups**, and then click **Provision Protection Groups**.

The **Protection groups** dialog for the module displays the following information for each provisioned protection group:

- **Working** — the working transceiver port
- **Protecting** — the protecting transceiver port
- **Protection ID** — the name of the protection group, if added
- **Protocol** — the protocol used by both transceiver ports
- **FPSD** — the FPSD setting for both transceiver ports

- **Direction** — the protection switch direction (UNI or BI)
- **Working Wavelength** — the wavelength of the working transceiver
- **Protecting Wavelength** — the wavelength of the protecting transceiver

Step 3 Click **Close**.

You have successfully completed this procedure.

8.6.6 Modify protection-group information for a Transponder module

Use this procedure to modify the ID of a protection group on a Transponder module.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

Prerequisites

- A protection group must be provisioned on the Transponder module.

Modify protection-group information

Follow these steps to modify the ID of a protection group on a Transponder module:

Step 1 In the toolbar, click the System Configuration button.

Step 2 In the Navigation pane, right-click **Protection Groups**, and then click **Provision Protection Groups**.

Step 3 In the **Protection groups** dialog for the module, select a protection group, and then click **Edit**.

Step 4 To change the name of the protection group, enter the new name in the **Protection ID** field.

Step 5 To change the name of the protection switch direction, select UNI or BI in the **Direction** field.

Note Not all transponders support changing this option.

Step 6 Click **Apply**.

You have successfully completed this procedure.

8.6.7 Delete a protection group on a Transponder module

When a protection group is no longer required, you can delete it. Use this procedure to delete a protection group on a Transponder module.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

Deleting a protection group

Follow these steps to delete a protection group on a Transponder module:

- Step 1** In the toolbar, click the System Configuration button.
- Step 2** In the Navigation pane, right-click **Protection Groups**, and then click **Provision Protection Groups**.
- Step 3** In the **Protection groups** dialog for the module, select a protection group, and then click **Delete**.

You have successfully completed this procedure.

9.0 Transponder port management

This section provides information about operations for managing ports on Transponder modules.

- [9.1, “Retrieving and exporting performance metrics for Transponder modules”](#)
- [9.2, “Monitoring threshold crossing alerts”](#)
- [9.3, “Performing loopback tests on transponder modules”](#)
- [9.4, “Loopback on Y-cable client protection groups”](#)
- [9.5, “Perform a loopback test on a Transponder module”](#)
- [9.6, “Transponder module maintenance signals and port timing ”](#)
- [9.7, “Laser status control”](#)

9.1 Retrieving and exporting performance metrics for Transponder modules

You can retrieve active and historical performance metrics (PMs) for ports on Transponder modules. The following table lists the supported PM types for each module.

PM type	Supported on
Physical	All Transponder modules
Layer 1 GE	2.5G Wavelength Manager Dual 4G Multiprotocol Transponder
SONET section	2.5G Wavelength Manager Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder
SDH section	2.5G Wavelength Manager Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder
Layer 1 Fibre Channel	Dual 4G Multiprotocol Transponder Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder
10GELAN	Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder
OTN	Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder

This sections covers the following topics:

- [9.1.9, “Retrieve and export active PMs”](#)
- [9.1.1, “Retrieve and export historical PMs”](#)
- [8.3.1.4, “Physical PMs”](#)
- [9.1.2, “Layer 1 Gigabit Ethernet protocol PMs ”](#)
- [9.1.3, “SONET PMs ”](#)
- [9.1.4, “SDH PMs ”](#)
- [9.1.5, “10GELAN PMs ”](#)
- [9.1.6, “Layer 1 Fibre Channel protocol PMs ”](#)
- [9.1.7, “OTN protocol PMs ”](#)
- [9.1.8, “Embedded PM support for 10G Multiprotocol Transponder and Dual 10G Multiprotocol Transponder modules”](#)

9.1.1 Retrieve and export historical PMs

Use this procedure to view historical performance metrics (PMs).



Prerequisites

- The port must be provisioned and a transceiver present in the port.

Retrieving and exporting historical PMs

Follow these steps to retrieve and, if required, export historical PMs:

- Step 1** In the toolbar, click the System Configuration button.
- Step 2** In the Navigation pane, click a port on the module.
- Step 3** On the **View** menu, choose **Performance Monitoring**.
- Step 4** Click the **Historical PM** tab in the **Performance Monitoring** window.
- Step 5** Click one of the following option buttons:
- **15 Min Bins** — to retrieve PMs for the 15-minute period you set using the **From** and **To** lists
 - **1 Day Bin** — to retrieve PMs for the most recent 24-hour period
- Step 6** Select a PM parameter from the **Parameters** list, and then click **Apply**.
The PM data for the parameter appears as a chart report on the **Chart** tab if you specified a 15-minute bin, and as a table report on the **Table** tab if you specified a 1-day bin.
- Note** The chart report provides the actual values and indicates the high and low thresholds for the parameter. Hover text at each collection point on the chart indicates the time and value of the PM. The table report provides the present value for each parameter.
- Step 7** Optionally, click **Export** to save the data retrieved to CSV (.csv) or text (.txt) format.
- Step 8** Repeat steps 4 to 6 for each parameter whose data you want to retrieve and, if required, export.

You have successfully completed this procedure.

9.1.2 Layer 1 Gigabit Ethernet protocol PMs

Table 9-1 Layer 1 Gigabit Ethernet PMs (counters)

PM (montype)	PM threshold default values		Supported modules
	15-minute	1-day	
CV 8B/10B Coding Violations measure the number of 8B/10B coding violations and disparity errors.	382	3820	Dual 4G Multiprotocol Transponder 2.5G Wavelength Manager
ES Errored Seconds measures the number of seconds during which one or more coding violations are detected, or a Loss of Synchronization (LOSYNC) or Loss of Signal (LOS) defect is present.	25	250	Dual 4G Multiprotocol Transponder 2.5G Wavelength Manager
SES Severely Errored Seconds measures the number of seconds during which the number of detected coding violations exceeds the severely errored seconds level (SESLVL), or a Loss of Synchronization (LOSYNC) defect or Loss of Signal (LOS) defect is present. The SESLVL value for Layer 1 Gigabit Ethernet is 1250.	4	40	Dual 4G Multiprotocol Transponder 2.5G Wavelength Manager
UAS Unavailable Seconds measures the number of seconds during which the link was considered unavailable. A link becomes unavailable at the onset of 10 consecutive seconds that qualify as SES, and continues to be unavailable until the onset of 10 consecutive seconds that do not qualify as SES. In seconds that are counted as unavailable, the counting of CV, ES, and SES is inhibited.	10	10	Dual 4G Multiprotocol Transponder 2.5G Wavelength Manager

9.1.3 SONET PMs

SONET protocol PMs are supported on the following Transponder modules.

- 2.5G Wavelength Manager
- Dual 4G Multiprotocol Transponder
- Dual 10G Multiprotocol Transponder
- 10G Multiprotocol Transponder

Table 9-2 SONET PMs (counters)

PM (montype)	PM threshold default values		Supporting entities
	15-minute	1-day	
CVS Section Coding Violations measures the number of B1 Bit Interleaved Parity (BIP) errors detected at the section layer.	382	3820	OC3, OC12, OC48, OC192
ESS Section Errored Seconds measures the number of seconds during which one or more B1 Bit Interleaved Parity (BIP) errors were detected or a Severely Errored Frame (SEF) or a Loss of Signal (LOS) defect was present.	25	250	OC3, OC12, OC48, OC192
SEFS-S Section Severely Errored Framing Seconds measures the number of seconds during which a section SEF defect was present.	2	8	OC3, OC12, OC48, OC192
SESS Section Severely Errored Seconds measures number of seconds during which the number of detected B1 Bit Interleaved Parity (BIP) errors exceeds the severely errored seconds level (SESLVL), or a Severely Errored Frame (SEF) or a Loss of Signal (LOS) defect was present. The SESLVL value for SONET section level is as follows: <ul style="list-style-type: none"> • OC3 = 155 • OC12 = 616 • OC48 = 2392 • OC192 = 8554 	4	40	OC3, OC12, OC48, OC192
UAS-S Section Unavailable Seconds measures the number of seconds during which the SONET section is unavailable. A second is considered UAS-S at the onset of 10 consecutive SESS seconds, and is no longer considered UAS-S after 10 consecutive seconds that are not SESS seconds. In seconds that are counted as unavailable, the counting of CVS, ESS and SESS are inhibited.	10	10	OC3, OC12, OC48, OC192

9.1.4 SDH PMs

SDH protocol PMs are supported on the following Transponder modules.

- 2.5G Wavelength Manager
- Dual 4G Multiprotocol Transponder
- Dual 10G Multiprotocol Transponder
- 10G Multiprotocol Transponder

Table 9-3 SDH PMs (counters)

PM (montype)	PM threshold default values		Supported entities
	15-minute	1-day	
RS-EB Regenerator Section Errored Blocks measures the number of regenerator section errored blocks. An errored block is one that contains one or more (up to eight per block) B1 Bit Interleaved Parity (BIP) errors.	0	0	STM16, STM64
RS-BBE Regenerator Section Background Block Errors measures the number of errored blocks not occurring during seconds counted as RS-SES seconds.	382	3820	STM16, STM64
RS-ES Regenerator Section Errored Seconds measures the number of seconds during which one or more errored blocks were detected or a Loss of Frame (LOF) or a Loss of Signal (LOS) defect was present.	25	250	STM16, STM64
RS-OFS Regenerator Section out of Frame Seconds measures the number of seconds during which an Out of Frame (OOF) defect was present.	2	8	STM16, STM64
RS-SES Regenerator Section Severely Errored Seconds measures the number of seconds during which the number of detected errored blocks exceeds the severely errored seconds level (SESLVL), or a Loss of Frame (LOF) or Loss of Signal (LOS) defect was present. The SESLVL value for SDH regenerator section is 30% of the nominal block rate.	4	40	STM16, STM64
RS-UAS Regenerator Section Unavailable Seconds measures the number of seconds during which the regenerator section is unavailable. A second is considered RS-UAS at the onset of 10 consecutive RS-SES seconds, and is no longer considered RS-UAS after 10 consecutive seconds that are not RS-SES seconds. In seconds that are counted as unavailable, the counting of RS-EB, RS-BBE, RS-ES, and RS-SES is inhibited.	10	10	STM16, STM64

9.1.5 10GELAN PMs

Table 9-4 10GELAN PMs (counters)

PM (montype)	PM threshold default values		Supported modules
	15-minute bin	1-day bin	
INVBLK Invalid Blocks measures the number of invalid 64/66B coding blocks.	382	3820	Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder
ES Errored Seconds measures the number of seconds during which one or more errored blocks/code violations are detected, or LOSYNC (Loss of Synchronization) or LOS (Loss of Signal) is detected.	25	250	Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder
SES Severely Errored Seconds measures the number of detected invalid blocks exceeds the severely errored seconds level (SESLVL), or in which a Loss of Synchronization (LOSYNC) defect or Loss of Frame (LOF) defect is present. The SESLVL value for 10GELAN is 8554.	4	40	Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder
UAS Unavailable Seconds measures the number of seconds during which the link was considered unavailable. A link becomes unavailable at the onset of 10 consecutive seconds that qualify as SES, and continues to be unavailable until the onset of 10 consecutive seconds that do not qualify as SES. In seconds that are counted as unavailable, the counting of In seconds that are counted as unavailable, the counting of INVBLK, ES, and SES is inhibited	10	10	Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder
FCSE-RX Total number of received frames with CRC (Cyclic Redundancy Check) errors measures the number of received frames that had a valid length but had either a bad Frame Check Sequence (FCS Error) or a bad FCS with a non-integral number of OCTETS (alignment errors).	0	0	Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder
FRDR Total number of discarded frames measures the total number of frames dropped due to a lack of resources or other reasons. This number is not necessarily the number of frames dropped, but rather the number of time that dropped frames could be detected.	0	0	Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder
FRGT Total fragmented Frame Count in Receive Direction measures the total number of received frames 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	0	0	Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder

Table 9-4 10GELAN PMs (counters) (Continued)

PM (montype)	PM threshold default values		Supported modules
	15-minute bin	1-day bin	
integral number of octets (FCS error) or a bad FCS with a non-integral number of octets (alignment error).			
JABR Total Jabber Frame Count in Receive Direction measures the total number of received frames that were longer than the maximum frame size ¹ (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).	0	0	Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder
BCST Total Broadcast Frame Count in Receive Direction measures the total number of good frames received that were directed to the broadcast address. (This number does not include frames that were directed to the multicast address.)			Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder
MCST Total multicast Frame Count in Receive Direction measures the total number of good frames received that were directed to a multicast address. (This number does not include frames that were directed to the broadcast address.)			Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder
OSIZE Total oversized Frame Count in Receive Direction measures the total number of received frames that were greater than the maximum frame size ¹ in length (excluding framing bits, but including Frame Check Sequence (FCS) octets) but were otherwise well formed.	0	0	Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder
OVER1518 Total over-1518 Frame Count in Receive Direction measures the total number of frames received that were greater than 1518 bytes but not exceeding the maximum frame size ¹ in length (excluding framing bits, but including Frame Check Sequence (FCS) octets).	0	0	Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder
SIZE64 Total 64 Byte Frame Count in Receive Direction measures the total number of 64 byte frames received (excluding framing bits, but including Frame Check Sequence (FCS) octets).			Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder
SIZE65-127 Total 65-127 Byte Frame Count in Receive Direction measures the total number of 65-127 byte frames received (excluding framing bits, but including Frame Check Sequence (FCS) octets).			Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder
SIZE128-255			Dual 10G Multiprotocol Transponder

Table 9-4 10GELAN PMs (counters) (Continued)

PM (montype)	PM threshold default values		Supported modules
	15-minute bin	1-day bin	
Total 128-255 Byte Frame Count in Receive Direction measures the total number of 128-255 byte frames received (excluding framing bits, but including Frame Check Sequence (FCS) octets).			10G Multiprotocol Transponder
SIZE256-511 Total 256-511 Byte Frame Count in Receive Direction measures the total number of 256-511 byte frames received (excluding framing bits, but including Frame Check Sequence (FCS) octets).			Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder
SIZE512-1023 Total 512-1023 Byte Frame Count in Receive Direction measures the total number of 512-1023 byte frames received (excluding framing bits, but including Frame Check Sequence (FCS) octets).			Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder
SIZE1024-1518 Total 1024-1518 Byte Frame Count in Receive Direction measures the total number of 1024-1518 byte frames received (excluding framing bits, but including Frame Check Sequence (FCS) octets).			Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder
TBYC-RX Total Byte Count in Receive Direction measures the total number of bytes of data (including those in bad frames) received (excluding framing bits, but including Frame Check Sequence (FCS) octets).			Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder
TFRC-RX Total Frame Count in Receive Direction measures the total number of frames (bad frames, broadcast frames, and multicast frames) received.			Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder
USIZE Undersized Frames measures the total number of frames received that were less than 64 octets long (excluding framing bits, but including Frame Check Sequence (FCS) octets) and were otherwise well formed.	0	0	Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder

¹The maximum frame size on the BT7A49AA and BT7A49AB modules is fixed at 9600 bytes. The maximum frame size on the BT7A49AA-I02 module is fixed at 10200 bytes.

9.1.6 Layer 1 Fibre Channel protocol PMs

Table 9-5 Layer 1 Fibre Channel PMs (counters)

PM (montype)	PM threshold default values		Supported modules
	15-minute	1-day	
CV 8B/10B Coding Violations measures the number of 8B/10B coding violations and disparity errors.	382	3820	Dual 4G Multiprotocol Transponder
INVBLK Invalid Blocks measures the number of invalid 64/66B coding blocks.	382	3820	Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder
ES Errored Seconds measures the number of seconds during which one or more coding violations are detected, or a Loss of Synchronization (LOSYNC) or Loss of Signal (LOS) defect is present.	25	250	Dual 4G Multiprotocol Transponder Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder
SES Severely Errored Seconds measures the number of seconds during which the number of detected coding violations exceeds the severely errored seconds level (SESLVL), or a Loss of Synchronization (LOSYNC) defect or Loss of Signal (LOS) defect is present. The SESLVL value for Fiber Channel is 1250.	4	40	Dual 4G Multiprotocol Transponder Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder
UAS Unavailable Seconds measures the number of seconds during which the link was considered unavailable. A link becomes unavailable at the onset of 10 consecutive seconds that qualify as SES, and continues to be unavailable until the onset of 10 consecutive seconds that do not qualify as SES.	10	10	Dual 4G Multiprotocol Transponder Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder

9.1.7 OTN protocol PMs

Table 9-6 OTN PMs (counters) supported on SONET/SDH line protocols

PM (montype)	PM threshold default values		Supported modules
	15-minute bin	1-day bin	
NUMBITSCR Number of Bits Corrected measures the total number of bits corrected by the Forward Error Correction (FEC) decoder according to the Reed-Solomon RS(255,239) forward error correction scheme.	0	0	Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder

Table 9-6 OTN PMs (counters) supported on SONET/SDH line protocols (Continued)

PM (montype)	PM threshold default values		Supported modules
	15-minute bin	1-day bin	
NUMBYTESCR Number of Bytes Corrected measures the total number of bytes corrected by the forward error correction scheme. Note Not supported on line protocols OC192EFEC and STM64EFEC.	0	0	Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder
UNCRCDWRD Number of Uncorrectable Code Words measures the total number of errored code words received that could not be corrected by the Forward Error Correction scheme.	10	100	Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder
BER Bit Error Ratio provides an estimate of the instantaneous Bit Error Ratio of the line by evaluating the ratio of the number of bits corrected to the total bits received over a 10-second time window. Both the instantaneous and average BER values are only valid for relatively low error rates in the signal. If the BER value is reported to be above 10^{-3} , it should be disregarded as it is not possible to accurately measure BER values above this level. BER values above this level usually indicate another problem, which should be evident in other PM counts.			Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder
BER-AVG Average Bit Error Ratio provides an estimate of the average Bit Error Ratio of the line by evaluating the ratio of the number of bits corrected to the total bits received over the duration of the entire collection interval. Both the instantaneous and average BER values are only valid for relatively low error rates in the signal. If the BER value is reported to be above 10^{-3} , it should be disregarded as it is not possible to accurately measure BER values above this level. BER values above this level usually indicate another problem, which should be evident in other PM counts.			Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder
OTU-BBE OTU-2 Background Block Error measures the number of errored blocks not occurring during seconds counted as OTU-SES seconds.	382	3820	Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder
OTU-EB OTU-2 Errored Blocks measures the number of frames containing one or more Bit Interleaved Parity (BIP) errors, using the OTU-2 SM BIP-8 byte in the incoming OTN signal. Up to eight BIP-8 errors can be detected per OTU-2 frame. However, regardless of the number of BIP-8 errors detected, a single frame can count for no more than one errored block.	0	0	Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder

Table 9-6 OTN PMs (counters) supported on SONET/SDH line protocols (Continued)

PM (montype)	PM threshold default values		Supported modules
	15-minute bin	1-day bin	
Note			
EB counting is suspended when either one of the following faults is active on the port: Loss of Signal, Loss of Frame.			
OTU-ES OTU-2 Errored Seconds measures the number of seconds during which one or more errored blocks is detected or a Loss of Frame (LOF), Loss of Signal (LOS), or Trace Identifier Mismatch (TIM) defect is present.	25	250	Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder
OTU-SES OTU-2 Severely Errored Seconds measures the number of seconds during which the number of detected errored blocks exceeds the severely errored seconds level (SESLVL), or a Loss of Frame (LOF), Loss of Signal (LOS), or Trace Identifier Mismatch (TIM) defect was present. The SESLVL value for OTN is 30% of the nominal block rate.	4	40	Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder
OTU-OFS OTU-2 Out of Frame Seconds measures the number of seconds during which a Out of Frame (OOF) defect was present.	2	8	Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder
OTU-UAS OTU-2 Unavailable Seconds measures the number of seconds during which the OTN line is unavailable. A second is considered OTU-UAS at the onset of 10 consecutive OTU-SES seconds, and is no longer considered OTU-UAS after 10 consecutive seconds that are not OTU-SES seconds.	10	10	Dual 10G Multiprotocol Transponder 10G Multiprotocol Transponder

9.1.8 Embedded PM support for 10G Multiprotocol Transponder and Dual 10G Multiprotocol Transponder modules

OC192FEC/STM64FEC Regen

Embedded SONET/SDH protocol PMs are not collected.

OC192/STM64-to-OC192FEC/STM64FEC

Embedded PMs are collected for the egress SONET or SDH signal as it is unwrapped from OTN and reported against the FEC port.

10GELANFEC/10GELANFEC EPCMF Regen

Embedded 10GELAN protocol PMs are not collected.

10GELAN-to-10GELANFEC/EFEC EPCMF and 10GELAN-to-10GELANFEC/EFEC EPV3 Regen

Embedded Layer 2 Ethernet PMs are collected for the egress 10GELAN signal as it is unwrapped from OTN. No BER is calculated.

10GELAN-to-OTU2e FEC/EFEC

Embedded Layer 2 Ethernet PMs are reported for the egress 10GELAN signal.

9.1.9 Retrieve and export active PMs

Use this procedure to retrieve and, if required, export active performance metrics (PMs).

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

Prerequisites

- The port must be provisioned and a transceiver present in the port.

Retrieving and exporting active PMs

Follow these steps to retrieve and, if required, export active PMs:

Step 1 In the toolbar, click the System Configuration button.

Step 2 In the Navigation pane, click a port on the module.

Step 3 On the **View** menu, choose **Performance Monitoring**.

Step 4 Click the **Active PM** tab in the **Performance Monitoring** window.

Step 5 Specify the following settings:

- **Refresh** — to set the frequency that you want the data to be updated (from 5 seconds to 60 minutes)
- **Bin Type** — to set one of the following the bin-storage intervals:
 - 15-Minute Bin
 - 1 Day Bin
 - Untimed (accumulates indefinitely)

Step 6 Select a PM parameter from the **Parameters** list.

You can select two parameters by holding down the Shift key.

Step 7 Click the **Chart** tab or the **Table** tab to have the data presented as either a chart report or a table report.

The chart report provides actual values and indicates the high and low thresholds for a parameter. Hover text at each collection point on the chart indicates the time and value of the PM.

The table report provides the present value for each parameter.

Step 8 Click **Start**.

The PM data for the parameter (or parameters) appears as a report in the format you specified. To view the data in the alternate report format, click the tab for that format.

Note Data can be collected for a maximum of 120 data points at different time intervals (5 seconds to 60 minutes). The proNX 900 Node Controller continuously polls for data at the time interval specified. The scroll bar enables you to view the most recent 120 data points collected.

Step 9 Optionally, click **Export** to save the data retrieved to CSV (.csv) or text (.txt) format.

Step 10 Repeat steps 4 to 8 for each parameter whose data you want to retrieve and, if required, export.

You have successfully completed this procedure.

9.2 Monitoring threshold crossing alerts

When the performance metric (PM) parameter reached or exceeded its preset threshold, threshold crossing alerts (TCAs) are autonomously reported to the management system that the TCAs are supported for each monitored parameter for the configured protocol, for both the current 15-minute and 1-day bins. TCAs are not supported for untimed bins.

When a port is provisioned, default PM threshold values are used. You can modify and view the PM threshold levels on provisioned Transponder ports.

This section covers the following topics:

- [9.2.1, “Threshold crossing alerts supported on Transponder modules”](#)
- [9.2.2, “Set Performance Monitoring threshold levels”](#)
- [9.2.3, “View threshold crossing alerts”](#)

9.2.1 Threshold crossing alerts supported on Transponder modules

The following table lists the 15-minute and 1-day threshold values of the performance monitoring parameters (montype) for Transponder modules. The default 15-minute and 1-day ranges are as follows:

- 15-minute: 0 to 38700
- 15-minute for second-based monitor types: 0 to 899
- 1-day: 0 to 215913600
- 1-day for second-based monitor types: 0 to 86400

Table 9-7 Performance monitoring threshold values

Protocol	Monitored parameter (montype)	15-Minute default	1-Day default
FC	CV (coding violations)	382	3820
	ES (errored seconds)	25	250
	SES (severely errored seconds)	4	40
	UAS (unavailable seconds)	10	10
GE	CV	382	3820
	ES	25	250
	SES	4	40
	UAS	10	10
Layer 1 10GELAN	ES	25	250
	SES	4	40
	UAS	10	10
	INVBLK (invalid block)	382	3820
Layer 2 GE and 10GELAN	FRDR	0	0
	FCSE-RX	0	0

Table 9-7 Performance monitoring threshold values (Continued)

Protocol	Monitored parameter (montype)	15-Minute default	1-Day default
	FRGT	0	0
	OSIZE	0	0
	USIZE	0	0
OTN FEC/EFEC	UNCRCDWRD	10	100
	OTU-EB (errored blocks)	0	0
	Note EB counting is suspended when either one of the following faults is active on the port: Loss of Signal, Loss of Frame.		
	OTU-BBE (background block errors)	382	3820
	OTU-ES (errored seconds)	25	250
	OTU-SES (severely errored seconds)	4	40
	OTU-UAS (unavailable seconds)	10	10
	OTU-OFS (out of frame seconds)	2	8
	NUMBITSCR (number of bits corrected)		
	NUMBYTESCR (number of bytes corrected)		
	Note Does not apply to EFEC.		
	UNCRCDWRD (number of uncorrectable codewords)		
OC3, OC12, OC48, OC192	CVS	382	3820
	ESS	25	250
	SEFS-S	2	8
	SESS	4	40
	UASS	10	10
	CVL	382	3820
	Note OC3, OC12 only.		
	CVL	18336	183360
	Note OC48, OC192 only.		
	ES-L	25	250
	SES-L	4	40
	UAS-L	10	10

Table 9-7 Performance monitoring threshold values (Continued)

Protocol	Monitored parameter (montype)	15-Minute default	1-Day default
STM1, STM4, STM16, STM64	RS-BBE	382	3820
	RS-EB	0	0
	RS-ES	25	250
	RS-SES	4	40
	RS-UAS	10	10
	RS-OFS	2	8
	MS-BBE	21260	212600
	MS-EB	0	0
	MS-ES	87	864
	MS-SES	1	4
	MS-UAS	10	10

9.2.2 Set Performance Monitoring threshold levels

Use this procedure to set performance monitoring (PM) threshold levels on provisioned ports.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

Prerequisites

- The module port must be provisioned.

Setting threshold-crossing-alarm levels

Follow these steps to set PM threshold levels:

- Step 1** In the Navigation pane, right-click a port on the module, and then click **View Transceiver PM**.
- Step 2** Click the **Thresholds** tab of the **Provision Transceiver** dialog.
Values for each threshold are provided on the tab.
- Step 3** Type a value in the field that corresponds to each PM whose level you want to set.
- Step 4** Click **Apply**.

You have successfully completed this procedure.

9.2.3 View threshold crossing alerts

Use this procedure to view threshold crossing alerts for module ports.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

Prerequisites

- The Transponder port must be provisioned.

Viewing threshold crossing alarms

Follow these steps to view threshold crossing alerts for a port:

Step 1 In the Navigation pane, right-click a port on the module, and then click **View Transceiver PM**.

Step 2 Click the **Thresholds** tab of the **Provision Transceiver** dialog.
Values for each threshold crossing alert are provided on the tab.

Step 3 Click **Close**.

You have successfully completed this procedure.

9.3 Performing loopback tests on transponder modules

The BTI 7000 Series supports two types of loopback tests:

- **Facility:** A loopback test performed on the originating end in the transport network.
- **Terminal:** A loopback test performed on the equipment at the receiving end of the network.

Note For a Transponder Lite module, only a Facility loopback test can be performed.

Loopback tests are performed on transceiver ports to test the following:

- The continuity of a link between two sites mitigating the need to travel to the remote site to test the connection.
- The functionality of a transceiver provisioned in a slot at the time the system is installed to ensure that the transceiver is fully operational before it is placed into service.

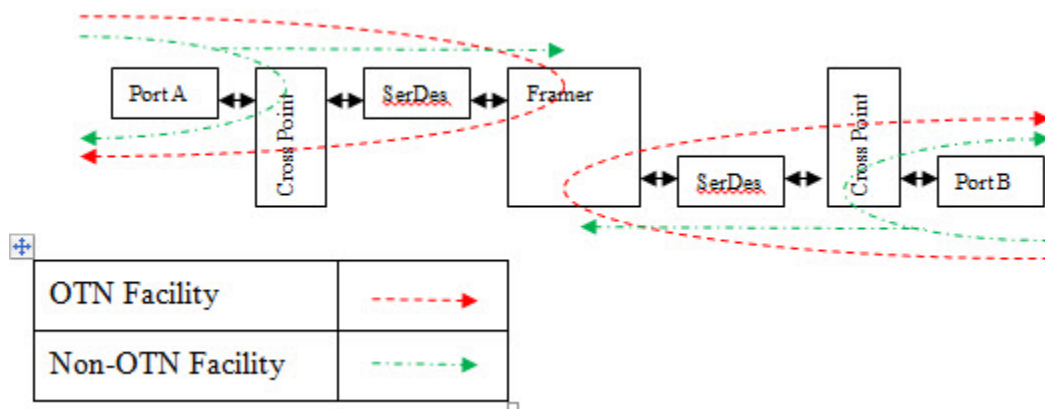
When using OTN protocols, if the input signal is not error-free, the outgoing signal may be modified according to the trace settings and the Fault Proagation Mode for the transceiver port.

If the transceiver port is not set for pass-through, GCC bytes continue to be terminated to maintain the management channel.

Note If a port is in loopback, and a port that can be cross-connected to it is either provisioned or deleted, traffic on the port in loopback can be temporarily affected.

Facility loopback tests on transponder modules

Figure 9-1 Facility loopback



The route the signal follows depends on the protocol that is provisioned.

The following applies for a Facility loopback:

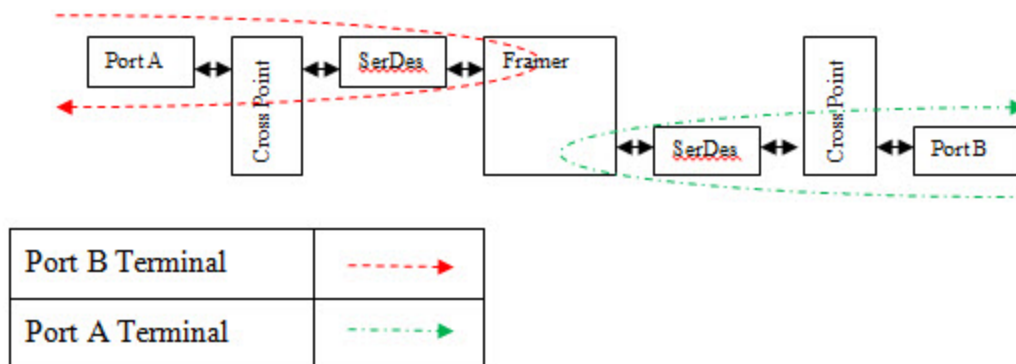
- The transceiver port must be provisioned and out-of-service.
- The route the signal follows through the pack depends on the protocol provisioned.
- If a two-way cross-connect exists, neither port can have a terminal loopback.

For non-OTN protocols, the loopback occurs at the cross-point switch although the signal will still be forwarded to the framer to analyze the signal for faults and defects (LOS, LOF, PMs, etc.).

For OTN protocols, the loopback occurs inside the framer so that the FEC or EFEC is decoded and recoded. This ensures that the looped-back signal can reach back to the sender (without regenerating the FEC, the signal might not reach).

Terminal loopback tests on transponder modules

Figure 9-2 Terminal loopback



The Terminal loopback occurs on the cross-connected port, not the port of the loopback. The figure above shows the route the signal follows in a Terminal loopback.

The following applies for a Terminal loopback:

- The transceiver port must be provisioned and out-of-service.
- A two-way cross-connect must exist.
- Neither port in the cross-connect may have any type of loopback.
- If the transceiver port is in a protection pair:
 - the transceiver port must be in a working (WRK) state.
 - the Standby port must be in an out-of-state management (OOS-MA) or link down (LKDO) state.

Note Terminal loopback cannot be operated if either port in the cross-connect already have a Facility or Terminal loopback.

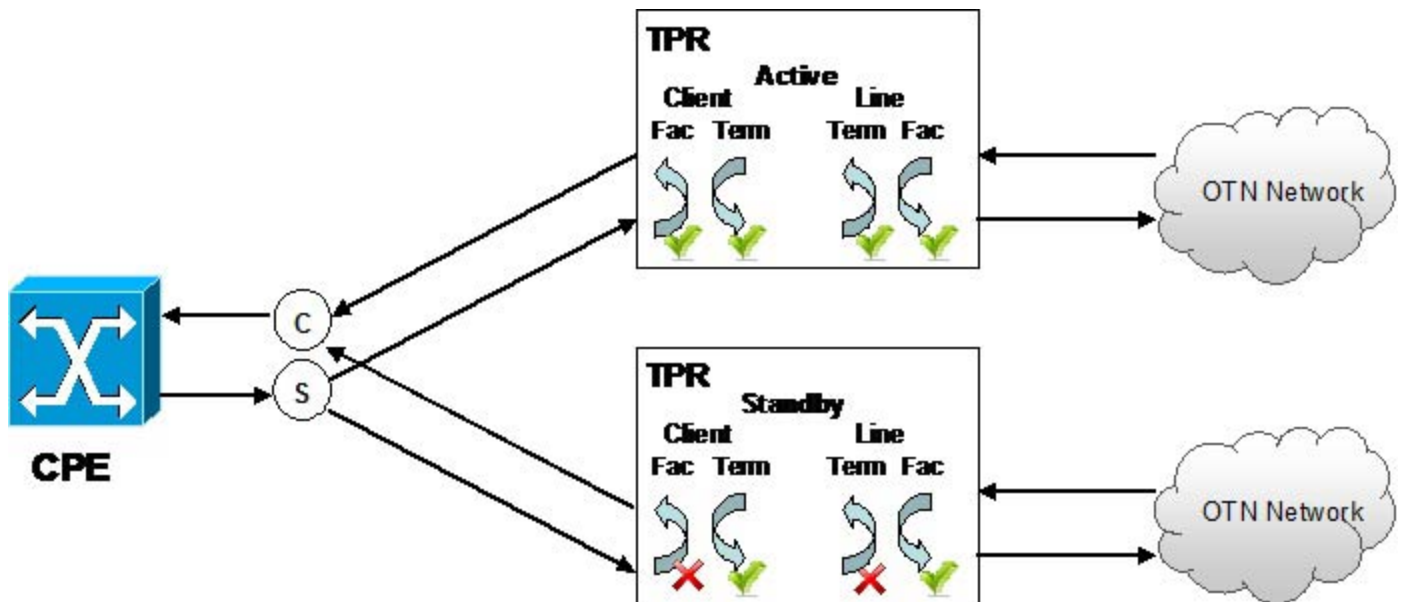
9.4 Loopback on Y-cable client protection groups

This section describes loopback functions for Y-cable client protection groups. For more information about loopback functions for BTI Transponder modules, refer to 9.3, “Performing loopback tests on transponder modules”.

Loopback tests can be performed only when a port is in the Out-of-service (OOS) maintenance state. Loopback operations are not stored in the database, but, recover if the transponder modules are cold or warm restarted. Loopback operations are lost if the SCP is restarted. All loopbacks are released after the SCP finishes booting.

The following figure shows the possible loopbacks in a client protection configuration. Loopbacks not supported are marked with an “x”:

Figure 9-3 Supported client protection loopbacks



Facility loopback considerations

The following Facility loopback considerations apply for Y-cable client protection groups:

- A client port facility loopback can be operated on only the active client port, and only if a lockout protection switch is operated on the standby client port.
- A standby client lockout cannot be released if there is a facility loopback active on the active client port.
- A line port facility loopback can be operated on lines associated with both the active and standby client ports. No lockout is required.

Terminal loopback considerations

The following Terminal loopback considerations apply for Y-cable client protection groups:

- A terminal loopback can operate on the working or protecting client port, or the line port corresponding to the active client port, only if the client port protection group and 2WAY cross-connect is provisioned.
- A protecting client port supports the terminal loopback despite the absence of an explicitly provisioned 2WAY cross-connect between the protecting ports.
- A line port terminal loopback can operate only on the line port associated with the active client port, only if a lockout protection switch is operated on the standby client port.
- A standby client port lockout cannot be released if there is a terminal loopback active on the line port associated with the active client port.
- A client terminal loopback can be operated on both active and standby client ports. No lockout is required.
- A cross-connect provisioned on the working port of a client protection group cannot be deleted, if any of the supported terminal loopbacks are active.

9.5 Perform a loopback test on a Transponder module

Use this procedure to perform a loopback test on a port on a Transponder module.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

Prerequisites

- Port must be provisioned and in the Out-of-Service state.
- The port with which the looped back port is paired must be provisioned to use a compatible protocol, much like it would have to be if it were to be cross-connected to that port. It is recommended that a cross-connect be provisioned between the two ports prior to provisioning the loopback. The system allows you to provision a loopback with incompatible protocols, but traffic will not pass over the loopback.

Note Before you perform a loopback test for a Y-cable client protection group, be sure you are familiar with Y-cable client protection loopback test considerations; refer to the *BTI 7000 Series Transponder Solutions Guide*.

Performing a loopback test

Follow these steps to perform loopback test on a port on a Transponder module:

Step 1 In the toolbar, click the **System Configuration** button.

Step 2 In the Navigation pane, right-click a port on a Transponder module, and then click **Enable Loopback**, and then click one of the following:

- **Facility** — to perform a facility loopback test on a client- or line-side port
- **Terminal** — to perform a terminal loopback test on a client-side port

Note When a loopback is in progress, the letter "L" appears on the port in the graphical representation of the shelf.

Step 3 In the **Enable Loopback** confirmation dialog, click **Yes** to remove the port from service and start the loopback test.

Step 4 Send a test signal through the loopback link using a bit error rate test (BERT) or packet generator test to check for errors or problems on the link.

Step 5 To end the loopback test, right-click the loopback port in the Navigation pane, and then click **Disable Loopback**.

Step 6 In the **Loopback Disabled** confirmation dialog, click **Yes** to restore the port to service.

You have successfully completed this procedure.

9.6 Transponder module maintenance signals and port timing

Maintenance signals and timing behavior on Transponder module ports provide information for effective port management.

This section covers the following topics:

- 9.6.1, “10G and Dual 10G Transponder maintenance signals”
- 9.6.2, “Port timing on 10G and Dual 10G Multiprotocol Transponder modules”

9.6.1 10G and Dual 10G Transponder maintenance signals

Ports on Transponder modules send maintenance signals according to the protocol the port is provisioned to use and the condition that exists at the port. This topic provides information about the maintenance signals.

10GELAN, 10GFC

When a port is provisioned to use 10GELAN or 10GFC, the signal REMOTE-FAULT is sent for ports 2 and 4 (clients), or the signal PRBS is sent for ports 1 and 3 (lines), under the following conditions:

- Port state is Out-of-Service
- No cross-connection exists
- 2-Way cross-connection exists; mate port fault (LOS, LOSYNC, LOF, TIM)
- 2-Way cross-connection exists, mate port receiving a maintenance signal.

OC192, STM64

When a port is provisioned to use OC192 or STM64, the AIS-L or MS-AIS signal, respectively, is sent under the following conditions.

Note The maintenance signal is timed from the module's internal clock, not an incoming signal.

- No cross-connection exists
- 2-Way cross-connection exists; mate port fault (LOS, LOF)
- 2-Way cross-connection exists; mate port receiving AIS-L or MS-AIS (passed through)

When FPSD is enabled on a port, the maintenance signal (AIS-L or MS-AIS) is superseded by laser shutdown. The following tables summarize port and mate port actions according to FPSD setting and port condition.

Table 9-8 OC192 FPSD = OFF, STM64 FPSD = OFF

Port condition	Mate port action	Port action
LOS or LOF	AIS-L/MS-AIS	Not applicable

Table 9-8 OC192 FPSD = OFF, STM64 FPSD = OFF (Continued)

Port condition	Mate port action	Port action
AIS-L or MS-AIS	AIS-L/MS-AIS (pass-through)	Not applicable
OOS	Not applicable	AIS-L/MS-AIS

Table 9-9 OC192/ FPSD = ON, STM64 FPSD = ON

Port condition	Mate port action	Port action
LOS or LOF	Laser Off	Not applicable
AIS-L or MS-AIS	Laser Off	Not applicable
OOS	Not applicable	Laser Off

OTN

When a port is provisioned to use an OTN protocol, the maintenance signal ODU2-AIS is sent under the following conditions.

Note The maintenance signal is timed from the module's internal clock, not an incoming signal.

- Port state is Out-of-Service
- No cross-connection exists
- 2-Way cross-connection exists; mate port fault (LOS, LOF)
- 2-Way cross-connection exists; mate port receiving ODU2-AIS (passed through)
- 2-Way cross-connection exists; mate port receiving OTU2-AIS

Note BTI has implemented ODU2-AIS rather than OTU2-AIS because it maintains OTU2 overhead, including GCC0.

9.6.2 Port timing on 10G and Dual 10G Multiprotocol Transponder modules

When no cross-connections exist on 10G and Dual 10G Multiprotocol Transponders, all ports are timed internally. When a cross-connection is provisioned and the ports are Out-of-Service, the ports are timed internally.

The following table identifies the timing behavior for ports involved in a cross-connection when the ports are In-Service. Timing is through the ports .

Table 9-10 Timing behavior on 10G and Dual 10G Multiprotocol Transponder ports

Client protocol (ports 2, 4)	Line protocol (port 1, 3)
10GELAN	10GELANFEC or 10GELANFEC 10GELANFEC EPCMF or 10GELANFEC EPCMF
OC192	OC192FEC or OC192EFEC

Table 9-10 Timing behavior on 10G and Dual 10G Multiprotocol Transponder ports (Continued)

Client protocol (ports 2, 4)	Line protocol (port 1, 3)
STM64	STM64FEC or STM64EFEC
10GELAN	10GELAN
OC192	OC192
STM64	STM64
10GELANFEC	10GELANFEC
10GELANFEC EPCMF	10GELANFEC EPCMF or 10GELANFEC EPCMF
OC192FEC	OC192FEC
STM64FEC	STM64

For synchronous protocols (OTN, SONET, and SDH), when a cross-connected port is receiving a maintenance signal (ODU2-AIS, AIS-L, or MS-AIS), the mate port is transmitting the same signal and uses the same timing that applies if the port is not receiving the maintenance signal. Faults such as LOS or LOF, or receiving OTU-2 AIS result in internally timed maintenance downstream (if applicable). For more information, see [9.6.1, “10G and Dual 10G Transponder maintenance signals”](#).

During a loopback test, timing is recovered from the receiver of the looped back port.

9.7 Laser status control

Laser status control provides the ability for an operator to turn a transmitting laser on or off, and is supported on SFP/XFP ports on transponder and muxponder modules. When the transmitting laser is shut down, the far end port detects the fault and reacts in a way similar to a fiber cut, which may include executing a protection switch.

The operator is not allowed to turn the laser on or off if Fault Propagation Shut Down (FPSD) is enabled on the port, or if the port is part of a client protection group, or on GCC-enabled links. In these situations, the operator must configure the laser control parameter to have the laser automatically controlled by software.

In all other situations, including other protection schemes, the operator is allowed to control the laser status.

10.0 Troubleshooting Transponder modules

This section provides information for troubleshooting issues on Transponder modules.

- [10.1, “Alarms and events on Transponder modules”](#)

10.1 Alarms and events on Transponder modules

The proNX 900 Node Controller allows you to view alarms and events reported on a Transponder module at any time.

If a Transponder module is in the In-Service state or Out-of-Service state, any fault condition pertaining to the module is reported as an autonomous alarm. For information about clearing alarms pertaining to Transponder modules, see the *Alarm and Troubleshooting Guide*.

An event reported on a Transponder module can indicate the module's status, a periodic report of information, or asynchronous command completion information.

For a description of the information provided by the proNX 900 Node Controller about an alarm or event, see the *proNX 900 Node Controller Online Help*.

This section covers the following topics:

- 10.1.1, “View alarms or events for a Transponder module”
- 10.1.2, “Transponder module alarms”

10.1.1 View alarms or events for a Transponder module

Use this procedure to view alarms or events reported on a Transponder module.



Prerequisites

- Transponder module must be provisioned and physically present in the shelf.

Viewing alarms and events

Follow these steps to view alarms and events on a Transponder module:

Step 1 Click one of the following tabs in the **Alarm** pane:

- **Alarms** — to view the list of alarms
- **Events** — to view the list of events
- **Conditions** — to view the list of conditions

Step 2 Double-click an alarm or event to view detailed information about it.

You have successfully completed this procedure.

10.1.2 Transponder module alarms

The following table lists the alarms supported on Transponder modules or ports. For detailed information about these alarms, including procedures for clearing them, see the *BTI 7000 Series Alarm and Troubleshooting Guide*.

Table 10-1 Alarms supported on Transponder modules

Alarm name	Description
FEEDAFUSEFAIL (Circuit pack feed A fuse failure)	The 48V fuse for feed A failed.
FEEDBFUSEFAIL (Circuit pack feed B fuse failure)	The 48V fuse for feed B failed.
HTASUNS (High temperature automatic shutdown unsupported)	The high temperature automatic shutdown option is enabled, but the system is not able to provide the functionality.
INVPROV (Invalid Provisioning)	Invalid provisioning is affecting the system.
LOF (Loss of Frame)	An SFP transceiver detects an errored frame (SEF) defect on the incoming SONET/SDH signal that persists for 2.5 seconds (± 0.5 sec.). An XFP transceiver detects that the OC192 or STM64 32-bit A1-A1-A2-A2 framing bytes sequence cannot be locked onto for 3 ms.
LOL (Loss of Lock)	A Dual 2.5G Multiprotocol Transponder or 1G wavelength regenerator (WR) port is unable to lock on the incoming bit stream.
LOS (WT/WR/TPR Loss of Signal)	An SFP or XFP transceiver has experienced an input power drop that is below the manufacturer's preset threshold.
LOSYNC (Loss of Synchronization)	A transceiver on a transponder detects 16 synchronization block errors in any group of 64 consecutive 64/66B blocks.
LSRMANOFF (Laser control manually turned off)	The port laser control parameter was manually set to OFF.
REPLUNITFAIL (Circuit Pack Failure)	A module failure.
REPLUNITMEA (Circuit Pack Mismatch)	There is a mismatch between the equipment provisioned for the slot and the physical module that is inserted in the slot.
REPLUNITHTAS (Circuit pack high temperature automatic shutdown)	The module temperature is above the high threshold and powered down.
REPLUNITMISS (Circuit Pack Missing)	A module is missing from its slot, or the wrong type module is provisioned for the slot.
REPLUNITPWR (Circuit pack power failure)	Power failure is detected on the module.
SD (Signal Degrade for line-side port)	The SONET/SDH line port has signal degradation.
T-OPR-HT (OPR High Threshold)	The input signal to an optical amplifier or SFP transceiver reached the optical power received (OPR) high threshold.
T-OPR-LT (OPR Low Threshold)	The input signal to an optical amplifier or SFP transceiver reached the optical power received (OPR) low threshold.
T-OPT-HT (OPT High Threshold for amplifiers)	The optical power transmitted (OPT) high threshold is exceeded.
T-OPT-LT (OPT Low Threshold for amplifiers)	The optical power transmitted (OPT) low threshold is crossed.
T-REPLUNIT-HT (Circuit pack high temperature threshold exceeded)	The module temperature is above the high threshold, but, below the shutdown threshold (HTS).
T-REPLUNIT-HTS (Circuit pack temperature shutdown threshold exceeded)	The module temperature is above the shutdown threshold (HTS).

Table 10-1 Alarms supported on Transponder modules (Continued)

Alarm name	Description
WNA (Wavelength Not Achievable)	Tuning failed.

11.0 Replacing Transponder modules and transceivers

This section provides instructions for replacing Transponder modules in supported shelves, and replacing SFPs and XFPs in Transponder modules.

- [11.1, “Replacing transponder modules”](#)
- [11.2, “Replacing optical transceivers”](#)
- [11.3, “Replacing copper transceivers”](#)

11.1 Replacing transponder modules

11.1.1 System behavior when replacing the Dual 10G Multiprotocol Transponder

When replacing one issue of the Dual 10G Multiprotocol Transponder with another issue, the general rule is that higher issues of the module support a superset of hardware functionality when compared to lower issues of that module. There are two situations to consider:

- The new module contains hardware features that require new system software. Full support of the hardware features only occurs on a shelf running the new system software. When you install the new module on a shelf that is running software that pre-dates the software introduction release of that module, the functionality of the new module reverts to the functionality that is supported by the software running on the older system.
- The new module does not contain hardware features that require new system software. In this situation, the new hardware features are supported regardless of the software release of the shelf in which the module is installed.

The behavior of the new module is therefore dictated by which of the above two situations applies. This is depicted in the following table for the Dual 10G Multiprotocol Transponder modules:

Table 11-1 Dual 10G Multiprotocol Transponder replacement

Module issue	Software introduction release	Can be installed in software release	Resulting functionality
BT7A49AA	7.1	Release 7.1 and higher	BT7A49AA
BT7A49AA-I02	11.1	Release 10.3 up to but not including release 11.1	Equivalent to the BT7A49AA
		Release 11.1 and higher	BT7A49AA-I02

The rest of this section provides additional details to the table above:

- For the list of features that each issue supports, see [2.5, “Dual 10G Multiprotocol Transponder features”](#).
- In all supported replacement situations, the inventory displays the PEC of the replacement module once the replacement module is inserted into the shelf. Note that this inventory PEC might be different from the configured equipment PEC.
- **When you install a BT7A49AA-I02 module into an unprovisioned slot**
 - In shelves running release 11.1 or higher, the system auto-provisions the equipment PEC to match the PEC of the inserted module. Full functionality of the BT7A49AA-I02 is supported.
 - In shelves running releases prior to release 11.1, the system auto-provisions the equipment PEC to BT7A49AA. You cannot change the equipment PEC and you cannot enable the new features of the BT7A49AA-I02. In effect, the functionality of the BT7A49AA-I02 module is downgraded to be the same as the functionality of the BT7A49AA module. This situation

arises when you use the BT7A49AA-I02 to spare for the BT7A49AA in shelves running releases prior to release 11.1.

- **When you replace a provisioned BT7A49AA module with a BT7A49AA-I02 module**

- A provisioned BT7A49AA module, in this context, is a module that has been provisioned with a PEC of BT7A49AA.
- In all situations where the original module is already provisioned, the provisioning remains unchanged. This means that the equipment PEC remains configured as the original module PEC.
- In shelves running release 11.1 or higher, you can change the equipment PEC to BT7A49AA-I02 to support the new features of the BT7A49AA-I02. Use the TL1 command **EDT-EQPT** to perform this function. If you do not change the equipment PEC, the functionality of the replacement module is downgraded to be the same as the functionality of the original module.
- In shelves running releases prior to release 11.1, you cannot change the equipment PEC and you cannot enable the new features of the replacement module. In effect, the functionality of the replacement module is downgraded to be the same as the functionality of the original module. This situation arises when you use the BT7A49AA-I02 to spare for the BT7A49AA in shelves running releases prior to release 11.1.

- **When you replace a higher issue provisioned module with a lower issue module**

- The system generates a Circuit Pack Mismatch Alarm (REPLUNITMEA). Configuration settings are not transferred to the replacement module. You will need to deprovision the original module along with all associated services and provision the replacement module. Note that replacing the higher issue module with a lower issue module will take longer and will therefore affect traffic for a longer duration. Only those features supported by the lower issue module are supported after the replacement.

11.1.2 Replacing transponder modules

Use this procedure to replace any BTI 7000 Series transponder module.

What you need

- Slot-head or Phillips screwdriver
- Electrostatic discharge (ESD) wrist strap
- Transponder module
- Replacement SFP or XFP transceivers
- Isopropyl alcohol and lint-free pads

Prerequisites



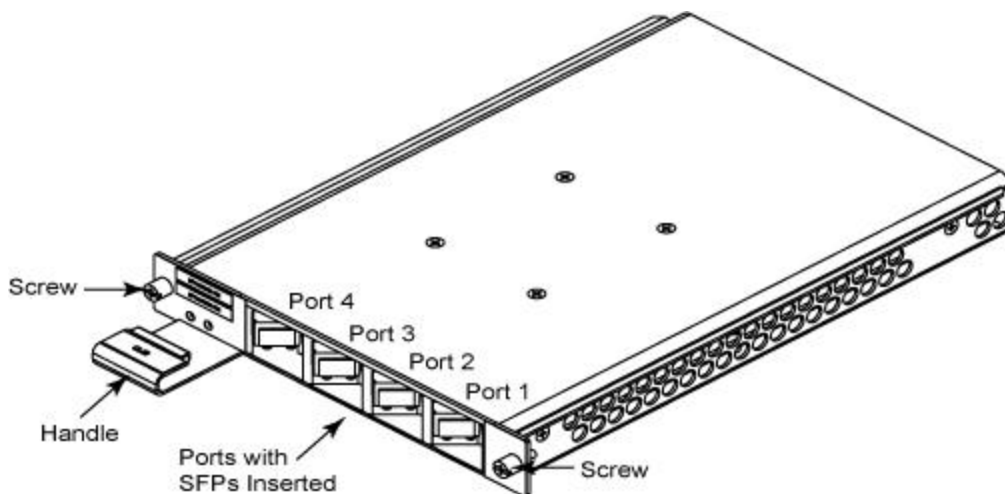
Caution

Use an ESD wrist strap whenever you open the equipment, particularly when you are handling modules as well as SFP and XFP transceivers. To work properly, the wrist strap must make good contact at both ends (that is, with your skin at one end and with the chassis at the other).

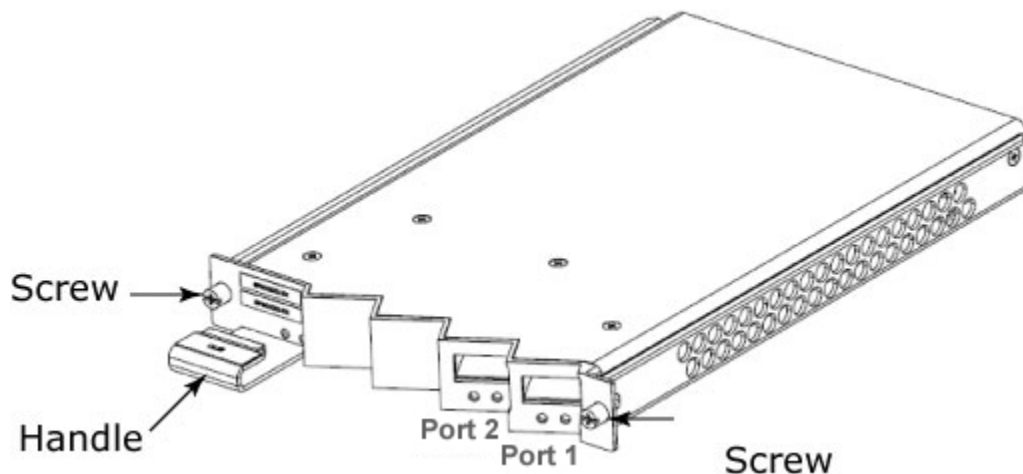
Key module replacement features

The following figures show the Transponder modules and indicate the key features for replacing them.

Dual 1G and Dual 2.5G Multiprotocol Transponder module



10G Multiprotocol Transponder module



Replacement procedure

Follow these steps to replace a Transponder module.

Note The following steps describe how to replace a Transponder module that is not part of a client protection (y-cable) configuration. For information on hitless replacement procedures for replacing a dual 10G transponder module that serves as a standby for client protection refer to the next section, "Replacing a dual 10G Transponder module in a client protection configuration."

Step 1 Reroute Traffic

Caution Failure to reroute traffic can result in lost data. Select an alternate route for the traffic that passes through the module. Transfer traffic to this alternate route before proceeding with this procedure.

Step 2 Move the Cables

Shelf cables may need to be moved aside to get clear access to the module. The cables rest on the handles that are at the front of the module.

Step 3 Disconnect the Cables

Disconnect the optical cables from the ports on the faceplate of the module.

Note Ensure that the optical ports on the module and the optical cables are protected with protective caps while disconnected.

Step 4 Loosen the Faceplate Screws

- a) Facing the front of the shelf, locate the faceplate screws.
- b) Using a slot-head or Phillips screwdriver, loosen the screws.

Step 5 Remove the Module

- a) Grasp the handles on the front of the module and firmly pull the module straight out.

Note An equipment missing alarm appears once you remove the module.

- b) Place the module on a flat work surface.

Step 6 Replace the Module

- a) Align the replacement module with the slot in which the module is being inserted.
- b) Carefully push the module straight into the slot.

Step 7 Replace the Faceplate Screws

- a) Facing the front of the shelf, align the module with its mounting holes.
- b) Using a slot-head or Phillips screwdriver, carefully tighten the faceplate screws:
 - Partially tighten the center support screw.
 - Partially tighten the other screw.
 - Fully tighten the center support screw.

- Fully tighten the other screw.

Caution Tighten to a torque that is no more than 4.7 in-lbs.

Step 8 Replace the SFP or XFP Transceivers

Step 9 Reconnect Optical Cables

Clean the optical cables then reconnect them to their original positions.

Note If you loop excess fiber around the fiber management spool, allow sufficient slack for the fiber management spool to move freely.

Step 10 Replace Cables

If any cables were moved to access the module, replace the cables to their original locations.

You have successfully completed this procedure.

11.1.2.1 Replacing a Dual 10G Transponder module in a client protection configuration

The BTI Dual 10G Transponder module can be used for client protection. Use this procedure to perform a hitless replacement of a Dual 10G Transponder that serves as the standby module on the protecting port.

Note This procedure is used if the module is physically replaced or re-seated.

Step 1 Verify that the module you are replacing/re-seating is the standby module and is not actively carrying traffic.

Using the RTRV-XCVR command, view the states of both the working and protecting client ports. The state of the protecting port must indicate STBY (standby).

Step 2 Remove or re-seat the module:

- a) If you are replacing the module, disconnect the cables and remove the module from the shelf. Refer to steps 2 to 5, above, in the section "Replacement procedure." Or,
- b) If you need to only re-seat the module, release the module from the slot.

Step 3 Install the replacement module, or re-seat the module into the slot.

To install the module, refer to steps 6 and 7, above.

Step 4 Wait until the module completes the booting process, and the red LEDs are off.

Step 5 Reconnect the cables.

To reconnect the cables refer to steps 9 and 10, above.

You have successfully completed this procedure.

11.2 Replacing optical transceivers

Use this procedure to replace optical small form factor (SFP) or 10 Gb/s (XFP) transceivers.

What you need

- Electrostatic discharge (ESD) wrist strap
- Replacement transceiver
- Isopropyl alcohol and lint-free pads

Prerequisites

To prevent potential damage from electrostatic discharge, observe the following when handling transceivers:

- Do not remove a transceiver from its packaging until you are ready to install it into a module.
- Do not touch any of the pins, connections, or components of a transceiver.
- Always store or transport a transceiver in anti-static packaging.



Invisible laser radiation can be emitted from the aperture ports of various modules when no fiber cable is connected. Avoid exposure and do not stare into open apertures to avoid permanent eye damage.

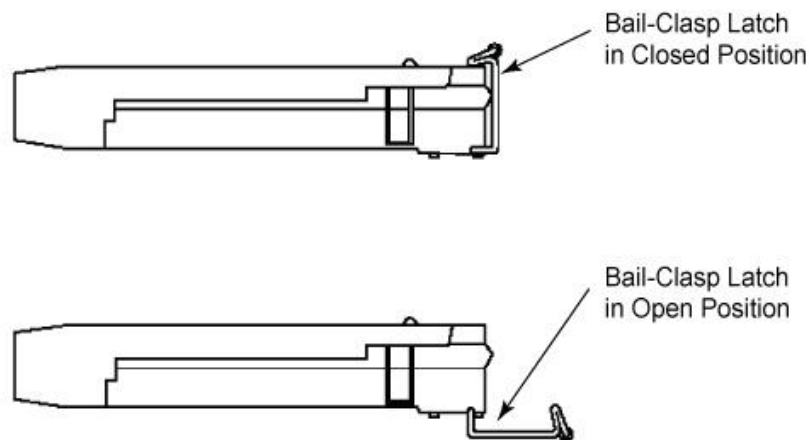


Use an ESD wrist strap whenever you open the equipment, particularly when you are handling modules as well as SFP and XFP transceivers. To work properly, the wrist strap must make good contact at both ends (that is, with your skin at one end and with the chassis at the other).

Transceiver key features

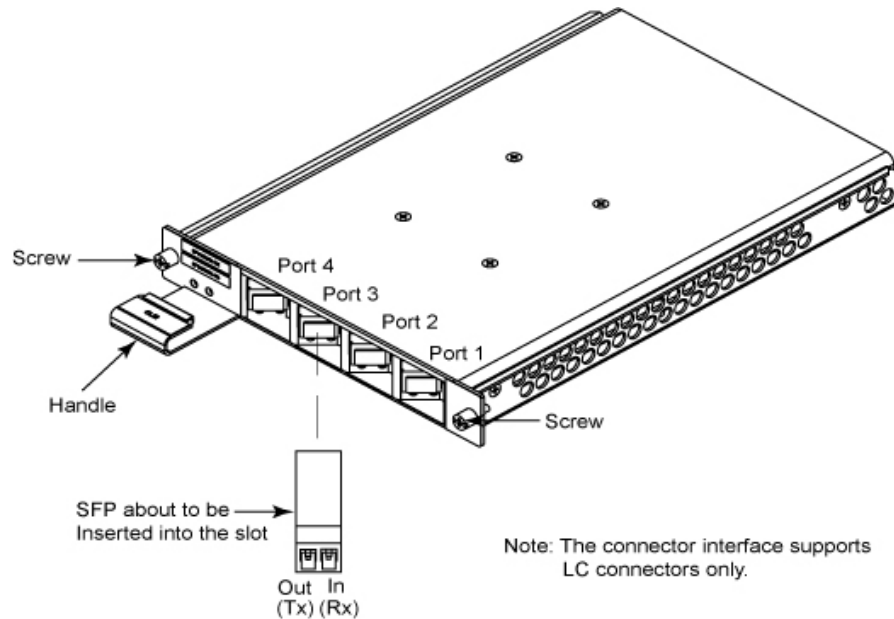
The following figure shows a typical SFP transceiver with a bale-clasp latch.

SFP transceiver with a bale-clasp latch



The following figure shows an SFP transceiver about to be inserted into its slot in a generic module.

Transceiver insertion



Replacement procedure

Follow these steps to replace a transceiver:

Step 1 Reroute Traffic

Caution Failure to reroute traffic can result in lost data. Select an alternate route for the traffic that passes through the module. Transfer traffic to this alternate route before proceeding with this procedure.

Step 2 Remove the Transceiver Port from Service

Remove the port from service.

Step 3 Move the Cables

Shelf cables may need to be moved aside to get clear access to the transceiver. The cables rest on the handles that are at the front of the circuit pack.

Step 4 Disconnect the Optical Cables

Disconnect the optical cables from the optical ports of the transceiver. Label the cables transmit and receive so that you can reconnect them to the correct ports later in this procedure.

Note Ensure that the optical ports on the transceiver and the optical cables are protected with protective caps while disconnected.

Step 5 Disengage the Latch Handle

Facing the front of the shelf, locate the latch handle on the transceiver. For a bale-clasp latch, pull the latch handle down until it is at a 90-degree angle to the transceiver.

Step 6 Remove the Transceiver

- a) Grasp the latch handle on the transceiver and firmly pull the transceiver straight out.

Note If the transceiver port is provisioned, an alarm (REPLUNITMISS) appears and the red LED turns on once you remove the transceiver.

- b) Place the transceiver into anti-static packaging and then lay it on a flat work surface.

Step 7 Insert the Replacement Transceiver

- a) Hold the transceiver so that the optical connectors face you. On an SFP, the product label will be visible. On an XFP, the product label is not visible.
- b) Ensure that the latch handle is in the closed position. For a bale-clasp latch, this is in the upright position.
- c) Align the transceiver to the port in which it is being inserted.
- d) Carefully slide the transceiver straight into the port until it clicks.

Note If the port is provisioned and the replacement transceiver has the same the wavelength, the REPLUNITMISS alarm clears.

Note If the port is provisioned, but the replacement transceiver has a different wavelength, the mismatch alarm (REPLUNITMEA) appears and the red LED turns on.

- e) Remove the plastic protective cover, if fitted.

Step 8 Clean the Ends of the Fiber Optic Cables

Use lint-free pads with isopropyl alcohol to clean the ends of the fiber optic cables.

Step 9 Connect the Optical Cables

Note Before connecting the optical cables to the transceiver, ensure that both the optical cable connectors and the optical surfaces are clean and that there is no residue on the optical surfaces.

Connect the input and output optical cables to the transceiver as follows:

- a) Ensure that the latch handle (or bale) of the transceiver is in the closed (up) position.
- b) Carefully slide the bottom of the male optical connector along the bottom of the transceiver opening.
- c) Gently push the male optical connector into the opening until a distinctive click is heard. Then continue exerting pressure on the connector to ensure a good connection is achieved.

Step 10 Restore the Transceiver Port to Service

Important XFPs and DWDM SFPs take about 90 seconds to reach a stable operating temperature. As a result, the REPLUNITFAIL (SFP or XFP Failure) alarm is disabled for 95 seconds after a transceiver is seated. If there is a transceiver hardware fault, the REPLUNITFAIL alarm is raised subsequent to the 95-second time delay.

Step 11 Replace the Cables

If any cables were moved to access the transceiver, replace the cables to their original locations.

You have successfully completed this procedure.

11.3 Replacing copper transceivers

Use this procedure to replace copper (electrical) small form factor pluggable (SFP) transceivers.

What you need

- Electrostatic discharge (ESD) wrist strap
- Replacement SFP transceiver

Prerequisites

To prevent potential damage from electrostatic discharge, observe the following when handling transceivers:

- Do not remove a transceiver from its packaging until you are ready to install it into a module.
- Do not touch any of the pins, connections, or components of a transceiver.
- Always store or transport a transceiver in anti-static packaging.

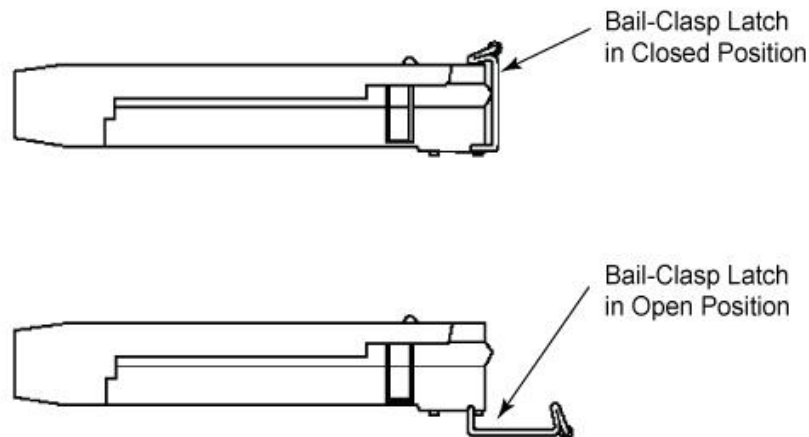


Caution

Use an ESD wrist strap whenever you open the equipment, particularly when you are handling modules as well as SFP and XFP transceivers. To work properly, the wrist strap must make good contact at both ends (that is, with your skin at one end and with the chassis at the other).

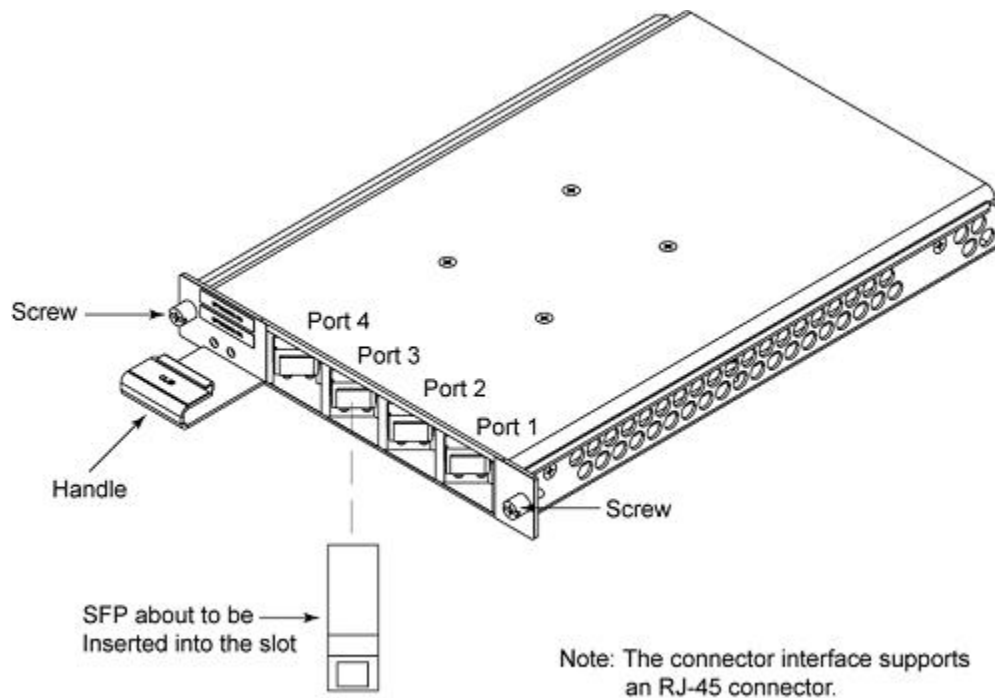
The following figure shows a typical SFP transceiver with a bale-clasp latch.

Figure 11-5 SFP Transceiver key features



The following figure shows a copper SFP transceiver about to be inserted into its slot in a generic module.

Figure 11-6 Copper SFP insertion into a generic module



To prevent potential damage from electrostatic discharge, observe the following when handling SFP transceivers:

- Do not remove an SFP transceiver from its packaging until you are ready to install it into a module.
- Do not touch any of the pins, connections, or components of an SFP transceiver.
- Always store or transport an SFP transceiver in anti-static packaging.

Procedure

Step 1 Reroute Traffic

Important Failure to reroute traffic can result in lost data. Select an alternate route for the traffic that passes through the SFP transceiver and then transfer traffic to the alternate route before proceeding with this procedure.

Step 2 Remove SFP port from service

Step 3 Move Cables

Shelf cables may need to be moved aside to get clear access to the SFP transceiver. The cables rest on the handles that are at the front of the module.

Step 4 Disconnect Cable

Disconnect the electrical cable from the electrical (RJ45) port of the SFP transceiver.

Step 5 Disengage Latch Handle

Facing the front of the module, locate the latch handle on the SFP transceiver. For a bale-clasp latch, pull the latch handle down until it is at a 90-degree angle to the transceiver.

Step 6 Remove Transceiver

- a) Grasp the latch handle on the SFP transceiver and firmly pull the transceiver straight out.

Note If the SFP transceiver port is provisioned, an SFP missing alarm (REPLUNITMISS) appears and the red LED turns on once you remove the transceiver.

- b) Place the SFP transceiver into anti-static packaging and then lay it on a flat work surface.

Step 7 Insert the SFP Replacement Transceiver

- a) Hold the SFP transceiver so that the RJ45 connector faces you and the product label is visible.
- b) Ensure that the latch handle is in the closed position. For a bale-clasp latch, this is in the upright position.
- c) Carefully slide the SFP transceiver straight into the port until it clicks.

Note If you are going from an optical to an electrical SFP, provision a wavelength with a value of 0.

- d) Remove the plastic protective cover, if fitted.

Step 8 Connect an RJ45 Cable to the Transceiver

Connect an RJ45 cable to each electrical SFP transceiver as follows:

- a) Ensure that the latch of the SFP transceiver is in the closed position
- b) Push the RJ45 connector into the SFP transceiver until a distinctive click is heard.

Note A Link Down alarm can occur when no signal is connected to the transceiver. To clear a Link Down alarm, refer to the *Alarm and Troubleshooting Guide*.

Step 9 Restore SFP Port to Service**Step 10 Replace Cables**

If any cables were moved to access the SFP transceiver, replace the cables to their original locations.

You have successfully completed this procedure.



Part Number:
Document Version:
Published:
Type:

BT7A73BA
01
March 2017
STANDARD

product release 13.5