



## PRODUCT DOCUMENTATION

### *BTI 7000 Series Upgrade Guide - Release 13.5*

**Part Number:** BT7A72BA  
**Document Version:** 01  
**Published:** March 2017  
**Type:** STANDARD

***product release 13.5***



# Contents

---

<b>Preface</b>	<b>v</b>
<b>1.0 BTI 7000 Series overview</b>	<b>1-1</b>
1.1 Supported upgrade paths .....	1-2
1.2 BTI 7000 Series common equipment .....	1-4
1.3 Shelf and module compatibility .....	1-5
1.4 BTI 7000 Series management interfaces .....	1-11
<b>2.0 Upgrading to Release 13.5</b>	<b>2-1</b>
2.1 Upgrade task flow .....	2-2
2.2 Before you upgrade to Release 13.5 .....	2-3
2.3 Set up proNX 900 .....	2-5
2.3.1 Installing proNX 900 Release 13.5 on Microsoft Windows .....	2-5
2.3.2 Installing proNX 900 Release 13.5 on Solaris .....	2-6
2.3.3 Installing proNX 900 Release 13.5 on Linux .....	2-8
2.3.4 Installing proNX 900 Release 13.5 on MAC OS X .....	2-9
2.3.5 Uninstalling proNX 900 on Microsoft Windows .....	2-10
2.3.6 Uninstalling proNX 900 on Solaris .....	2-11
2.3.7 Uninstalling proNX 900 on Linux .....	2-12
2.3.8 Uninstalling proNX 900 on MAC OS X .....	2-12
2.3.9 Troubleshooting installation problems .....	2-13
2.3.10 Logging on to the BTI 7000 Series using proNX 900 over IP network .....	2-13
2.3.11 Logging on to the BTI 7000 Series using proNX 900 over OSI network .....	2-13
2.4 Perform a database backup .....	2-15
2.4.1 Database backup using proNX 900 Node Controller .....	2-15
2.4.2 Database backup using TL1 .....	2-16
2.5 Load, invoke, and commit the system software upgrade .....	2-18

2.5.1 Loading, invoking, and committing the system software upgrade using proNX 900 .....	2-18
2.5.2 Loading, invoking, and committing the system software upgrade using TL1 .....	2-21
2.6 Install and provision equipment .....	2-28
2.7 Auto-upgrade support on modules .....	2-30

---

<b>3.0 Cancelling a system software upgrade</b>	<b>3-1</b>
---	------------

3.1 Cancelling a system software upgrade before committing the load using proNX 900 .....	3-2
3.2 Cancelling a system software upgrade before committing the load using TL1 .....	3-4
3.3 Cancelling a system software upgrade after committing the load using proNX 900 .....	3-7
3.4 Cancelling a system software upgrade after committing the load using TL1 .....	3-9

---

<b>4.0 Useful procedures</b>	<b>4-1</b>
------------------------------	------------

4.1 Determining system software release numbers .....	4-2
4.2 Determining the firmware version .....	4-3
4.3 Database restore using proNX 900 .....	4-6
4.4 Database restore using TL1 .....	4-8
4.5 Establishing a proNX 900 session using Ethernet .....	4-12
4.5.1 Method One: Connecting through the management LAN .....	4-13
4.5.2 Method Two: Connecting through the craft LAN port .....	4-14
4.6 Establishing a TL1 session using RS-232 .....	4-16
4.6.1 RS-232 serial communications .....	4-18

---

<b>5.0 Troubleshooting</b>	<b>5-1</b>
----------------------------	------------

5.1 Check failures .....	5-2
5.2 Load failures .....	5-4
5.3 Invoke failure .....	5-6
5.3.1 Recommended actions for invoke failures .....	5-6
5.4 Commit failure .....	5-8
5.5 Cancel failure .....	5-9
5.5.1 Recommended actions for cancel failures .....	5-9
5.6 Provisioning failure .....	5-10
5.7 Module upgrade failure .....	5-11
5.8 Database recovery failure .....	5-12

---

<b>Appendix A: Upgrading the network element from a BTI 2060 SCP to a BTI 7060 SCP</b>	<b>A-1</b>
--	------------

---

<b>Appendix B: SCP replacement procedures</b>	<b>B-1</b>
---	------------

---

<b>Appendix C: Downgrading to an earlier system software version</b>	<b>C-1</b>
--	------------

---

# 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)**

<b>Equipment</b>	<b>PEC</b>
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**

<b>proNX Management Suite</b>
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
<b>FDA</b>	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.
<b>FCC</b>	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.
<b>Industry Canada</b>	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
<b>Note</b>	Means reader take note. Notes contain helpful suggestions or background information.
 <b>Caution</b>	Means reader be careful. Equipment damage or loss of data can result from your actions.
 <b>Warning</b>	Means reader be careful. Harm to yourself or others can result from your actions.
 <b>Laser Warning</b>	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 BTI 7000 Series overview

---

This section provides information about the upgrade paths, common equipment, modules, and management interfaces supported by BTI 7000 Series Release 13.5.

- 1.1, “Supported upgrade paths”
- 1.2, “BTI 7000 Series common equipment”
- 1.3, “Shelf and module compatibility”
- 1.4, “BTI 7000 Series management interfaces”

## 1.1 Supported upgrade paths

The following table lists the upgrade paths that are supported by BTI for the BTI 7000 Series.

If you are upgrading from...	you can upgrade to...
6.2	7.2.0 or 7.2.1
7.1.0 <sup>1</sup>	7.2.0, 7.2.1, or 7.3
7.1.1 <sup>1</sup>	7.2.0, 7.2.1, or 7.3
7.1.2 <sup>1</sup>	7.2.0, 7.2.1, or 7.3
7.2.0	7.2.1, 7.3, 8.1, 8.2, 9.1
7.2.x	7.3, 8.1, 8.2, or 9.1
7.3	8.1, 8.2, 9.1 <sup>2</sup> , or 9.3 <sup>2</sup>
8.1	8.2 <sup>2</sup> or 9.1 <sup>2</sup>
8.2	9.1, 9.2, 9.3, 10.3, 11.1
9.1	9.2, 9.3, 10.3, 11.1, 11.2
9.2	9.3, 10.2, 10.3, 11.1, 11.2, 11.3
9.3	10.1, 10.2, 10.3, 11.1, 11.2, 11.3
10.1	10.2 or 10.3
10.2	10.3
8.1.4	10.4 <sup>3</sup>
10.1.3	10.4
10.3	11.1, 11.2, 11.3, 12.1
10.3.5	11.1, 11.2, 11.3, 12.1, 12.2
10.3.6	11.1, 11.2, 11.3, 12.1, 12.2
11.1	11.3, 13.1, 13.2, 13.5
11.2	11.3, 12.1, 12.2, 13.1, 13.2, 13.5
11.3	12.2, 13.2, 13.5
12.1	12.2, 13.1, 13.2, 13.5
12.2	13.1, 13.2, 13.5
13.1	13.2, 13.5
13.2	13.5

<sup>1</sup>This release is discontinued. Although an upgrade from 6.2 to 7.1.x is possible, BTI recommends upgrading to a more recent release to take advantage of the features of these newer releases.

<sup>2</sup>Cancelling this upgrade is not supported, either before or after committing the load.

<sup>3</sup>Cancelling this upgrade after committing the load is not supported.

If the upgrade path you require is not supported, for example, from 7.1.0 to 8.1, you may need to perform a two-step upgrade. Contact BTI Systems customer service to determine the best upgrade path for situations not explicitly stated in the table above.

To downgrade to a release other than the release from which you have upgraded, contact BTI Systems customer service to determine the best downgrade path for your situation. Be aware that this type of downgrade is not hitless and that some modules may have upgrade failure alarms raised on them after the downgrade is complete. Manual intervention may also be required.

## 1.2 BTI 7000 Series common equipment

The following table lists the BTI 7000 Series shelves and other common equipment supported in Release 13.5. For detailed information, see the *Product Guide* and the *Common Equipment Installation Guide*.

**Table 1-1 Common equipment supported in Release 13.5**

Equipment	PEC
BTI 7060	BT7A50AA
BTI 7060 with rear access -48V	BT7A50AR
BTI 7060 /BTI 7200 Cooling Unit (CU)	BT7A52DA
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
2U Cover – ANSI	BT7A5070
2U Cover – ETSI	BT7A5071
BTI 7030	BT7A56AA
BTI 7030 Cooling Unit (CU)	BT7A57BA
BTI 7030 Main Shelf Interface (MSI)	BT7A53CA BT7A53CB
BTI 7030 System Control Processor (SCP)	BT7A21BA
BTI 7030 AC Power Assembly Kit	BT7A56CA
BTI 7030 AC Power Module	BT7A58BA
1U Cover – ANSI	BT7A5600
1U Cover – ETSI	BT7A5602
BTI 7020 with ANSI Cover	BT7A56BA
BTI 7200 ANSI	BT7A51AA
BTI 7200 ETSI	BT7A51AB
BTI 7200 with rear access -48V	BT7A51AR
BTI 7200 Main Shelf Interface (MSI)	BT7A53EA
BTI 7200 Common Communication Module (CCM)	BT7A54EA



## 1.3 Shelf and module compatibility

The following tables identify the BTI 7000 Series modules that are supported on shelves that have been upgraded to the BTI 7000 Series platform and on BTI 7000 Series shelves. For information about upgrading Netstender 2060 shelves to the BTI 7000 Series platform, see the *Upgrade Guide — Release 6.2 to Release 7.1.0*.

**Note** The Netstender 1030 shelf cannot be upgraded to support BTI 7000 Series modules.

**Table 1-2 Common equipment**

Module	PEC	Upgraded 2060 Shelf	BTI 7030	BTI 7060	BTI 7200
2060 Cooling Unit (10,000 rpm)	BP1A52CA	Yes	No	No	No
2060 Main Shelf Interface	BP1A53AA <sup>1</sup> BP1A53BA <sup>1</sup>	Yes	No	No	No
2060 Expansion Shelf Interface	BP1A54AA	Yes	No	No	No
2060 Multiport System Control Processor	BP1A20BA	No	No	No	No
1030 Cooling Unit	BP1A57AA	No	No	No	No
1030 System Control Processor	BP1A21AA	No	No	No	No
BTI 7060 Cooling Unit	BT7A52DA	No	No	Yes	No
BTI 7060/BTI 7200 Cooling Unit	BT7A52EA	No	No	Yes	Yes
BTI 7060 Main Shelf Interface	BT7A53BA <sup>1</sup> BT7A53BB	No	No	Yes	No
BTI 7060 Expansion Shelf Interface	BT7A54BA	No	No	Yes	No
BTI 7060/BTI 7200 System Control Processor	BT7A20CA	Yes	No	Yes	Yes
BTI 7030 Cooling Unit	BT7A57BA	No	Yes	No	No
BTI 7030 Main Shelf Interface	BT7A53CA <sup>1</sup> BT7A53CB <sup>1</sup>	No	Yes	No	No

**Table 1-2 Common equipment (Continued)**

<b>Module</b>	<b>PEC</b>	<b>Upgraded 2060 Shelf</b>	<b>BTI 7030</b>	<b>BTI 7060</b>	<b>BTI 7200</b>
BTI 7030 System Control Processor	BT7A21BA	No	Yes	No	No
BTI 7200 ANSI	BT7A51AA	No	No	No	Yes
BTI 7200 ETSI	BT7A51AB	No	No	No	Yes
BTI 7200 with rear access -48V	BT7A51AR	No	No	No	Yes
BTI 7200 Main Shelf Interface (MSI)	BT7A53EA	No	No	No	Yes
BTI 7200 Common Communication Module (CCM)	BT7A54EA	No	No	No	Yes

<sup>1</sup>This module is not field upgradable.

**Table 1-3 Optical Amplifier modules**

<b>Module</b>	<b>PEC</b>	<b>Upgraded 2060 Shelf</b>	<b>BTI 7030</b>	<b>BTI 7060</b>	<b>BTI 7200</b>
DWDM C-Band Pre- Amplifier	BP1A01DA-UC	Yes	Yes	Yes	Yes
DWDM C-Band Booster Amplifier	BP1A02DA-UC	Yes	Yes	Yes	Yes
Optical Line Amplifier	BP1A03AA-SC	Yes	Yes	Yes	Yes
Optical Line Amplifier with mid-stage access	BP1A04BA-SC	Yes	Yes	Yes	Yes
Single Channel and Sub-band Booster Amplifier	BP1A05BB-UC	Yes	Yes	Yes	Yes
Single Channel and Sub-band Pre- Amplifier	BP1A05PB-UC	Yes	Yes	Yes	Yes
DWDM C-Band Low Gain Amplifier (LGA)	BT7A02AA-LC	No	No	Yes	Yes
DWDM C-Band Mid Gain Amplifier (MGA)	BT7A03AA-LC	No	No	Yes	Yes
DWDM C-Band Mid Gain Amplifier with Mid-stage access (MGM)	BT7A04AA-LC	No	No	Yes	Yes

**Table 1-4 Dispersion Compensation modules**

<b>Module</b>	<b>PEC</b>	<b>Upgraded 2060 Shelf</b>	<b>BTI 7030</b>	<b>BTI 7060</b>	<b>BTI 7200</b>
SMF Dispersion Compensation Module 20km	BP1A10CH-UC	Yes	Yes	Yes	Yes
SMF Dispersion Compensation Module 40km	BP1A10CC-SC	Yes	Yes	Yes	Yes
SMF Dispersion Compensation Module 60km	BP1A10CA-SC	Yes	Yes	Yes	Yes
SMF Dispersion Compensation Module 80km	BP1A10CB-SC	Yes	Yes	Yes	Yes
SMF 100 GHz C-Band DCM 40km	BP1A10AA-UC	Yes	Yes	Yes	Yes
SMF 100 GHz C-Band DCM 60km	BP1A10AB-UC	Yes	Yes	Yes	Yes
SMF 100 GHz C-Band DCM 80km	BP1A10AC-UC	Yes	Yes	Yes	Yes

**Table 1-5 Optical Multiplexing modules**

<b>Module</b>	<b>PEC</b>	<b>Upgraded 2060 Shelf</b>	<b>BTI 7030</b>	<b>BTI 7060</b>	<b>BTI 7200</b>
4-Channel CWDM Mux/Demux, Channel 1 - 4	BP1A33BA	Yes	Yes	Yes	Yes
4-Channel CWDM Mux/Demux, Channel 5 - 8	BP1A33BB	Yes	Yes	Yes	Yes
4-Channel CWDM Mux/Demux, Channel 9 - 12	BP1A33BC	Yes	Yes	Yes	Yes
4-Channel CWDM Mux/Demux, Channel 13- 16	BP1A33BD	Yes	Yes	Yes	Yes
Double 1-Channel OADM	BP1A32CA	Yes	Yes	Yes	Yes
32-Channel DWDM Mux/Demux Module 1	BP1A35AA	Yes	Yes	Yes	Yes
32-Channel DWDM Mux/Demux Module 2	BP1A35AB	Yes	Yes	Yes	Yes

**Table 1-5 Optical Multiplexing modules (Continued)**

<b>Module</b>	<b>PEC</b>	<b>Upgraded 2060 Shelf</b>	<b>BTI 7030</b>	<b>BTI 7060</b>	<b>BTI 7200</b>
32-Channel DWDM Mux/Demux Module 3	BP1A35AC	Yes	Yes	Yes	Yes
32-Channel DWDM Mux/Demux Module 4	BP1A35AD	Yes	Yes	Yes	Yes
32-Channel DWDM Bidirectional Mux/ Demux <sup>1</sup>	BP1A35DA-24 BP1A35DA-42)	No	No	No	No
32-Channel DWDM Bidirectional Mux/ Demux <sup>2</sup>	BP1A35DA-12 BP1A35DA-21	No	No	No	No
2-Channel DWDM OADM	BP1A36AB	Yes	Yes	Yes	Yes
4-Channel DWDM OADM	BP1A36AC	Yes	Yes	Yes	Yes
4-Channel DWDM OADM, BTI Channels E1, E3, E5, E7	BP1A36BC	Yes	Yes	Yes	Yes
CWDM + DWDM Splitter Combiner	BP1A30AA	Yes	Yes	Yes	Yes
1310nm and C-Band Coupler/Splitter	BP1A38AA	Yes	Yes	Yes	Yes
DWDM Bidirectional Coupler/Splitter	BP1A39CA	Yes	Yes	Yes	Yes
Single 50/50 Coupler/ Splitter	BP1A39DA	Yes	Yes	Yes	Yes

<sup>1</sup>Supported on BTI 7020 only.<sup>2</sup>Supported on BTI 7020 only.**Table 1-6 Transponder modules**

<b>Module</b>	<b>PEC</b>	<b>Upgraded 2060 Shelf</b>	<b>BTI 7030</b>	<b>BTI 7060</b>	<b>BTI 7200</b>
2.5G Wavelength Regenerator	BP1A42AA	Yes	Yes	Yes	Yes
2.5G Wavelength Manager	BP1A43AA	Yes	Yes	Yes	Yes
Dual 4G Multiprotocol Transponder	BT7A41CA	Yes	Yes	Yes	Yes

**Table 1-6 Transponder modules (Continued)**

<b>Module</b>	<b>PEC</b>	<b>Upgraded 2060 Shelf</b>	<b>BTI 7030</b>	<b>BTI 7060</b>	<b>BTI 7200</b>
Dual 10G Multiprotocol Transponder	BT7A49AA	Yes	Yes	Yes	Yes
	BT7A49AA-I02	Yes	Yes	Yes	Yes
Dual 10G Multiprotocol Transponder Lite	BT7A49AC	Yes	Yes	Yes	Yes
10G Multiprotocol Transponder	BT7A49AB	Yes	Yes	Yes	Yes

**Table 1-7 Muxponder modules**

<b>Module</b>	<b>PEC</b>	<b>Upgraded 2060 Shelf</b>	<b>BTI 7030</b>	<b>BTI 7060</b>	<b>BTI 7200</b>
2-Port GbE Muxponder (OC-48 with protection)	BP1A46AA	Yes	Yes	Yes	Yes
2-Port GbE Muxponder (STM-16 with protection)	BP1A46BA	Yes	Yes	Yes	Yes
8-Port Multiprotocol Muxponder – SONET	BT7A47JA	No	Yes	Yes	Yes
8-Port Multiprotocol Muxponder – SDH	BT7A47KA	No	Yes	Yes	Yes
8-Port Multiprotocol Muxponder – SDH	BT7A47MA	No	Yes	Yes	Yes
10-port 10G Multiprotocol Muxponder – SONET	BT7A48AA	No	Yes	Yes	Yes
	BT7A48AA-I02	No	Yes	Yes	Yes
10-port 10G Multiprotocol Muxponder – SDH	BT7A48BA	No	Yes	Yes	Yes
	BT7A48BA-I02	No	Yes	Yes	Yes
10-port 10G Multiprotocol Muxponder – SDH CCAT	BT7A48DA	No	Yes	Yes	Yes

**Table 1-8 packetVX modules**

<b>Module</b>	<b>PEC</b>	<b>Upgraded 2060 Shelf</b>	<b>BTI 7030</b>	<b>BTI 7060</b>	<b>BTI 7200</b>
packetVX Integrated Services Module 12/2	BT7A81AA	Yes	Yes	Yes	Yes
packetVX Integrated Services Module 24/2	BT7A81BA	No	No	Yes	Yes

**Table 1-8 packetVX modules (Continued)**

<b>Module</b>	<b>PEC</b>	<b>Upgraded 2060 Shelf</b>	<b>BTI 7030</b>	<b>BTI 7060</b>	<b>BTI 7200</b>
packetVX Integrated Services Module 24/4	BT7A81CA	No	No	Yes	Yes
packetVX Integrated Services Module 80	BT7A81GA	No	No	Yes	Yes

**Table 1-9 Dynamic Optical Layer modules**

<b>Module</b>	<b>PEC</b>	<b>Upgraded 2060 Shelf</b>	<b>BTI 7030</b>	<b>BTI 7060</b>	<b>BTI 7200</b>
DWDM Line Amplifier (DLA2)	BT7A06CA	No	Yes	Yes	Yes
2DROADM-on-a-blade (ROB2)	BT7A07AA	No	No	Yes	Yes
40-channel 4D ROADM-on-a-blade (ROB4)	BT7A07BA	No	No	Yes	Yes
96-channel 4D ROADM-on-a-blade (ROB4)	BT7A07CA	No	No	Yes	Yes

## 1.4 BTI 7000 Series management interfaces

---

The BTI 7000 Series supports standard communication interfaces over serial, IP, and OSI connections, including Telcordia Transaction Language One (TL1), and CLI. In addition, the BTI 7000 Series provides proNX 900 Node Controller (proNX 900), a graphical craft management interface, for management of individual NEs.

As an option, you can use proNX Service Manager (PSM) to upgrade more than one network element at a time. PSM is a service-centric network management system designed to simplify network operations from visualization and activation of services to network element database backups and software upgrades. With PSM, you can distribute NE software to multiple network elements outside of a maintenance window, and then upgrade these network elements using a centralized GUI.

The main tasks in this Upgrade Guide are described using both proNX 900-based procedures and TL1-based procedures.

For information about the management interfaces that the BTI 7000 Series supports, refer to the following documentation:

- *proNX 900 Node Controller Online Help*
- *TL1 Reference Guide*
- *BTI 7000 Series and packetVX Command Line Reference Guide*
- *proNX Service Manager User Guide*





## 2.0 Upgrading to Release 13.5

---

This section provides information about upgrading the system software from Release 11.1, 11.2, 11.3, 12.1, 12.2, 13.1, or 13.2 to Release 13.5. For information about other upgrade paths, contact your BTI representative.

## 2.1 Upgrade task flow

---

The following list identifies the order of tasks in the process for upgrading a system from Release 11.1, 11.2, 11.3, 12.1, 12.2, 13.1, or 13.2 to Release 13.5.

- 1 Perform a database backup. For information, see [2.4, “Perform a database backup”](#).
- 2 Install release Release 13.5 of the proNX 900. You can use Release 13.5 of the proNX 900 to perform the upgrade if desired.
- 3 Load, invoke, and commit the system software upgrade.
- 4 Install and provision new shelves and modules, and if necessary, replace common equipment such as the Cooling Unit. For information, see the *Common Equipment Installation Guide*, the *Operations Solutions Guide*, and the solutions guide for the particular module portfolio.

## 2.2 Before you upgrade to Release 13.5

The following is a check list to be reviewed before upgrading the system software from Release 11.1, 11.2, 11.3, 12.1, 12.2, 13.1, or 13.2 to Release 13.5.

- Reference the release notes for Release 13.5 to determine if there is information about upgrading the system software.
- Reference the "Troubleshooting" chapter of the solutions guide for each module type on your system to determine if there is information about a system software upgrade.
- The management network is operating at an acceptable performance level.
- There are no CONTCOM alarms on the system. See the *Alarm and Troubleshooting Guide* for information about clearing a CONTCOM alarm.
- The location to which the database is to be backed up has enough space to store the data.

**Note** A fully configured BTI 7000 Series main shelf and its log files can create a backup file of several megabytes in size. For more information, see [2.4, "Perform a database backup"](#).

- If the OSC ports are in use in the current release, check to make sure that they are properly provisioned before upgrading to the new release.
- If you are replacing the SCP, ensure that both software banks on the replacement SCP are loaded with the same software image of the release to which you are upgrading, and that the release numbers for the Active and Inactive software banks match.
  - To determine the software release loaded currently on the existing SCP, refer to [4.1, "Determining system software release numbers"](#)
  - For information about replacing SCP, refer to [Appendix B, "SCP replacement procedures"](#).
- Deprovision and remove all of the following modules from your system, as they are declared "End of Life" manufacture discontinued:
  - 10G Wavelength Regenerator - BP1A47AB -xx
  - 10G Tunable Wavelength Regenerator - BP1A47BB
  - 32 Channel DWDM Active Mux/Demux - BP1A35BA
- If you use proNX 900 Node Controller (proNX 900) to manage BTI 7000 Series NEs in the network, ensure the following:
  - The existing release of proNX 900 is available to perform a database backup of the current configuration database.
  - proNX 900 Release 13.5 is available for installation.
  - The computer on which proNX 900 is to be installed meets the minimum requirements for the software; refer to [2.3, "Set up proNX 900"](#).

- Various upgrade paths are supported. For more information, refer to [1.1, “Supported upgrade paths”](#).
- If you are upgrading a BTI 7200, ensure that the CCM module is not undergoing an upgrade. If it is, wait until it is complete before upgrading the BTI 7200. If you upgrade the system software while the CCM module is undergoing its own upgrade, the CCM module may end up in a failure state. If this occurs, restart the CCM module.

## 2.3 Set up proNX 900

---

This section covers the following topics:

- [2.3.1, “Installing proNX 900 Release 13.5 on Microsoft Windows”](#)
- [2.3.2, “Installing proNX 900 Release 13.5 on Solaris”](#)
- [2.3.3, “Installing proNX 900 Release 13.5 on Linux”](#)
- [2.3.4, “Installing proNX 900 Release 13.5 on MAC OS X”](#)
- [2.3.5, “Uninstalling proNX 900 on Microsoft Windows”](#)
- [2.3.6, “Uninstalling proNX 900 on Solaris”](#)
- [2.3.7, “Uninstalling proNX 900 on Linux”](#)
- [2.3.8, “Uninstalling proNX 900 on MAC OS X”](#)
- [2.3.9, “Troubleshooting installation problems”](#)
- [2.3.10, “Logging on to the BTI 7000 Series using proNX 900 over IP network”](#)
- [2.3.11, “Logging on to the BTI 7000 Series using proNX 900 over OSI network”](#)

### 2.3.1 Installing proNX 900 Release 13.5 on Microsoft Windows

Use this procedure to install Release 13.5 of proNX 900 on a computer running Microsoft Windows.

#### What you need

- proNX 900 CD-ROM

#### Prerequisites

Ensure that the computer meets the following minimum requirements:

- Operating system: Windows 2003 Server, Windows XP, or Windows 7
- Recommended minimum screen resolution: 1024 x 768 pixels
- Minimum color depth: 256 colors
- 1 GHz AMD/Intel
- 300 MB minimum of available disk space
- 2 GB minimum of RAM
- If Sun/Oracle Java is not already installed, and you do not want to install proNX 900 with Java, make sure Sun/Oracle Java 1.6 update 10 or later is installed before installing proNX 900.

#### Installing proNX 900 on Windows

Follow these steps to install proNX 900:

**Step 1** Place the CD-ROM in your CD-ROM drive.

**Step 2** Open **My Computer** or use Windows Explorer to navigate to your CD-ROM drive.

**Step 3** Open the installer file located in the `windows` folder.

You can choose to download proNX 900 that includes a Java VM (**bti\_proNX900\_<release\_build number>\_VM\_install**), or without a Java VM (**bti\_proNX900\_<release\_build number>\_NoVM\_install**).

**Step 4** Follow the instructions that appear on the **proNX 900** installer screen.

**proNX 900** installer guides you through the following steps:

- **Introduction**
- **Check Existing Versions**

**Note** Do not uninstall the existing version of proNX 900 until all NEs are upgraded.

- **Choose Install Folder**

**Note** Do not install a new release of proNX 900 into the folder of the existing version. The new proNX 900 release is installed into a new directory by default. If you make an error while specifying the folder, click **Restore Default Folder** to restore the path specifying the default folder.

- **Choose Shortcut Folder**
- **Pre-Installation Summary**
- **Installing**
- **Install Complete**

You have successfully completed this procedure.

## 2.3.2 Installing proNX 900 Release 13.5 on Solaris

Use this procedure to install Release 13.5 of proNX 900 on a UNIX workstation running Solaris.

### What you need

- proNX 900 CD-ROM

### Prerequisites

Ensure that the UNIX workstation meets the following minimum requirements:

- Operating System: Solaris 10
- Recommended minimum screen resolution: 1024 x 768 pixels
- Minimum color depth: 256 colors
- UltraSPARC III CPU

- 300 MB minimum of available disk space
- 2 GB minimum of RAM
- Sun/Oracle Java 1.6

**Note** For convenience, a Sun/Oracle Java 1.6 VM is provided as part of the installation.

## Installing proNX 900 on Solaris

**Step 1** Place the CD-ROM in the CD-ROM drive, and then navigate to the directory where the CD-ROM drive is mounted.

**Step 2** Open the installer script (**bt\_i\_proNX900\_<release\_build number>\_VM\_install.bin**) located in the `solaris` folder. If you are copying the file to the local machine, ensure the permissions are set appropriately for you to run the script.

**Step 3** Follow the instructions that appear on the **proNX 900** installer screen. The **proNX 900** installer guides you through the following steps:

- **Introduction**
- **Check Existing Versions**

**Note** Do not uninstall the existing version of proNX 900 until you are finished upgrading all of your NEs.

- **Choose Install Folder**

**Note** Do not install proNX 900 into the folder of the existing version. proNX 900 is installed into a new directory by default. If you make an error while specifying the folder, click **Restore Default Folder** to restore the path specifying the default folder.

- **Choose Link Folder**  
This is currently not used.
- **Pre-Installation Summary**
- **Installing**
- **Install Complete**

**Step 4** If you are using the provided Java VM installation, do the following:

a) Set the `$PATH` variable to the Java installation.

In the bash shell, you can do this as follows:

```
# export PATH=$PATH:<proNX installation directory>/jre/bin
```

b) Change the permissions on the Java binaries to allow execution.

```
# cd <proNX installation directory>/jre/bin
# chmod ugo+x *
```

c) Verify the Java version.

```
# java -version
java version "1.6.0_26"
Java(TM) SE Runtime Environment (build_1.6.0_26-b03)
Java HotSpot(TM) Client VM (build 20.1-b02, mixed mode)
```

You have successfully completed this procedure.

**Note** To launch the proNX 900, run the proNX900 script:

```
# cd <proNX 900 installation directory>
# ./proNX900
```

### 2.3.3 Installing proNX 900 Release 13.5 on Linux

Use this procedure to install Release 13.5 of proNX 900 on a Linux operating system.

#### What you need

- proNX 900 CD-ROM

#### Prerequisites

Ensure that the Linux workstation meets the following minimum requirements:

- Operating System: Linux (CentOS, Fedora, RedHat, Ubuntu)
- Recommended minimum screen resolution: 1024 x 768 pixels
- Minimum color depth: 256 colors
- Minimum 1 GHz CPU
- 300 MB minimum of available disk space
- 2 GB minimum of RAM
- Sun/Oracle Java 1.6

**Note** For convenience, a Sun/Oracle Java 1.6 VM is provided as part of the installation.

#### Installing proNX 900 on Linux

- Step 1** Place the CD-ROM in the CD-ROM drive, and then navigate to the directory where the CD-ROM drive is mounted.
- Step 2** Open the installer file (**bt\_i\_proNX900\_<release\_build number>\_VM\_install.bin**) located in the `Linux` folder. If you are copying the file to the local machine, ensure the permissions are set appropriately for you to run the script.
- Step 3** Follow the instructions that appear on the **proNX 900** installer screen. The **proNX 900** installer guides you through the following steps:
- **Introduction**



- **Check Existing Versions**

**Note** Do not uninstall the existing version of proNX 900 until all NEs are upgraded.

- **Choose Install Folder**

**Note** Do not install a new version of proNX 900 into the folder of the existing version. The new version of proNX 900 is installed into a new directory by default. If you make an error while specifying the folder, click **Restore Default Folder** to restore the path specifying the default folder.

- **Choose Link Folder**

This is currently not used.

- **Pre-Installation Summary**

- **Installing**

- **Install Complete**

**Step 4** If you are using the provided Java VM installation, do the following:

a) Set the \$PATH variable to the Java installation.

In the bash shell, you can do this as follows:

```
# export PATH=$PATH:<proNX installation directory>/jre/bin
```

b) Change the permissions on the Java binaries to allow execution.

```
# cd <proNX installation directory>/jre/bin
```

```
# chmod ugo+x *
```

c) Verify the Java version.

```
# java -version
```

```
java version "1.6.0_26"
```

```
Java(TM) SE Runtime Environment (build_1.6.0_26-b03)
```

```
Java HotSpot(TM) Client VM (build 20.1-b02, mixed mode)
```

You have successfully completed this procedure.

**Note** To launch the proNX 900, run the proNX900 script:

```
# cd <proNX 900 installation directory>
```

```
# ./proNX900
```

## 2.3.4 Installing proNX 900 Release 13.5 on MAC OS X

Use this procedure to install Release 13.5 of proNX 900 on a computer running MAC OS X.

### What you need

- proNX 900 CD-ROM

## Prerequisites

Ensure that the computer meets the following minimum requirements:

- Operating System: OS X 10.7 or later
- Recommended minimum screen resolution: 1024 x 768 pixels
- Minimum color depth: 256 colors
- 300 MB minimum of available disk space
- 2 GB minimum of RAM
- 1 GHz processor or higher
- Java 1.6 (Java for OS X 2012-006 recommended)

## Installing proNX 900 on MAC OS X

**Step 1** Place the CD-ROM in the CD-ROM drive.

**Step 2** Open the **proNX 900 <release number> <build number>.pkg** file located in the **os x** folder.

**Step 3** Follow the instructions that appear on the **proNX 900** installer screen. The **proNX 900** installer guides you through the following steps:

- **Introduction**
- **Destination Select**
- **Installation Type**

**Note** Check that the install location is "Macintosh HD".

- **Installation**
- **Summary**

You have successfully completed this procedure.

**Note** To launch proNX 900, navigate to the installation folder (typically / Applications/BTI) and double-click on the **proNX <release number> <build number>** executable.

## 2.3.5 Uninstalling proNX 900 on Microsoft Windows

Use this procedure to uninstall proNX 900 on a computer running Microsoft Windows.

**Important** Do not uninstall your proNX 900 unless instructed to do so in the upgrade procedures. You must use your existing version of proNX 900 to initiate the NE upgrade, and finish it with the new version of the proNX 900. Also, do not uninstall the existing proNX 900 until all the NEs are upgraded.

### Prerequisites

- Log out of and exit proNX 900.

### Uninstalling proNX 900 on Windows

Follow these steps to uninstall proNX 900:

**Step 1** From the **Start** button, click **All Programs**, then click the **Uninstall** icon under proNX 900.

The **Uninstall proNX 900** window displays.

**Step 2** Click the **Uninstall** button

proNX 900 uninstaller starts, and displays the message `All items were successfully uninstalled` when the process is completed.

**Step 3** Click **Done**.

You have successfully completed this procedure.

### 2.3.6 Uninstalling proNX 900 on Solaris

Use this procedure to uninstall proNX 900 on a UNIX workstation running Solaris.

**Important** Do not uninstall your proNX 900 unless instructed to do so in the upgrade procedures. You must use your existing version of proNX 900 to initiate the NE upgrade, and then finish it with the new version of the proNX 900. Also, do not uninstall your proNX 900 until you have upgraded all of your NEs.

### Prerequisites

- Log out of and exit proNX 900.

### Uninstalling proNX 900 on Solaris

Follow these steps to uninstall proNX 900:

**Step 1** Open a terminal window and navigate to the directory where proNX 900 is installed.

**Step 2** Change directory to the folder Uninstaller Data:

```
cd UninstallerData
```

**Step 3** Type the following to start the uninstaller application:

```
./Uninstall
```

The proNX 900 uninstaller application displays the message `Uninstall Complete` when the uninstall process is completed.

You have successfully completed this procedure.

## 2.3.7 Uninstalling proNX 900 on Linux

Use this procedure to uninstall proNX 900 on a Linux operating system.

**Important** Do not uninstall your proNX 900 unless instructed to do so in the upgrade procedures. You must use your existing version of proNX 900 to initiate the NE upgrade, and finish with the new version of the proNX 900. Also, do not uninstall your proNX 900 until all NEs are upgraded.

### Prerequisites

- Log out of and exit proNX 900.

### Uninstalling proNX 900 on Solaris

Follow these steps to uninstall proNX 900:

**Step 1** Open a terminal window and navigate to the directory where proNX 900 is installed.

**Step 2** Change directory to the folder Uninstaller Data:

```
cd UninstallerData
```

**Step 3** Type the following to start the uninstaller application:

```
./Uninstall
```

The proNX 900 uninstaller application displays the message `Uninstall Complete` when the uninstall process is completed.

You have successfully completed this procedure.

## 2.3.8 Uninstalling proNX 900 on MAC OS X

Use this procedure to uninstall proNX 900 on a computer running MAC OS X.

**Important** Do not uninstall your proNX 900 unless instructed to do so in the upgrade procedures. You must use your existing version of proNX 900 to initiate the NE upgrade, and then finish it with the new version of the proNX 900. Also, do not uninstall your proNX 900 until you have upgraded all of your NEs.

### Prerequisites

- Log out of and exit proNX 900.

### Uninstalling proNX 900 on MAC OS X

Follow these steps to uninstall proNX 900:

**Step 1** Navigate to `/Applications/BTI`.

**Step 2** Move the folder `proNX900_<release_build number>` to trash.

You have successfully completed this procedure.

### 2.3.9 Troubleshooting installation problems

An installation log file is available in the installation directory for Windows, UNIX and Linux installations. The log file is titled:

`proNX_900_InstallLog.log`

The log file provides information on the software components that installed successfully or failed to install.

#### Firewall precaution

If you have the Windows Firewall enabled, a firewall exception must be configured to allow the proNX 900 FTP server to function. The firewall exception should be configured with the `javaw` executable found in the proNX 900 Installation directory ("`<installation directory>\jre\bin\javaw.exe`").

If you are not using Java VM, then a different Installation directory will be used, depending on how the system is configured.

### 2.3.10 Logging on to the BTI 7000 Series using proNX 900 over IP network

Follow these steps to log on to the system using proNX 900.

<b>Note</b>	proNX 900 connects to the system through either a craft or management LAN port. For more information, see <a href="#">4.5, “Establishing a proNX 900 session using Ethernet”</a> .
-------------	--

**Step 1** Start proNX 900.

**Step 2** In the **Login** dialog, enter the IP address that you want to connect to in the **Network Element** field.

The default IP address of the Management LAN on proNX 900 is 10.0.0.1. The default IP address of the Craft LAN port is 192.168.17.1.

**Step 3** In the **User ID** field, enter a valid user ID. The default user ID is `admin`.

**Step 4** In the **Password** field, enter a valid password. The default password is `admin`.

**Step 5** Click **OK**.

proNX 900 starts and establishes a session with the system.

You have successfully completed this procedure.

### 2.3.11 Logging on to the BTI 7000 Series using proNX 900 over OSI network

Follow these steps to log on to the system using proNX 900 over an OSI network.

**Note** proNX 900 connects to the system through either a craft or management LAN port. For more information, see [4.5, “Establishing a proNX 900 session using Ethernet”](#).

**Step 1** Start proNX 900.

**Step 2** In the **Login** dialog, enter the IP address of the GNE in the **Network Element** field.

**Step 3** In the **User ID** field, enter a valid user ID. The default user ID is `admin`.

**Step 4** In the **Password** field, enter a valid password. The default password is `admin`.

**Step 5** Click **OK**.

proNX 900 starts and establishes a session with the system.

You have successfully completed this procedure.

## 2.4 Perform a database backup

The BTI 7000 Series SCP maintains all provisionable data in non-volatile storage so that configuration settings are retained during a system shutdown and restart. This configuration database is version controlled to facilitate the detection of an incompatible software load or database.

Before you upgrade the system software, you can back up the database locally, to a remote (S)FTP server, or to the SCP.

**Important** BTI recommends that the database be backed up to the SCP, and either locally or to a remote (S)FTP server. Backing up to the SCP enables you to cancel the upgrade if necessary, and then revert to the configuration database stored on the SCP.

If you choose to back up to an (S)FTP server, you can either specify a particular (S)FTP server or use the (S)FTP utility embedded in proNX 900 Node Controller.

This section covers the following topics:

- [2.4.1, “Database backup using proNX 900 Node Controller ”](#)
- [2.4.2, “Database backup using TL1 ”](#)

### 2.4.1 Database backup using proNX 900 Node Controller

Use this procedure to back up the database to the SCP or to an (S)FTP server using the proNX 900.

#### Prerequisites

- If backing up to an (S)FTP server, the server must be set up for remote backups.
- The backup location has enough space for the data.

**Note** Data for either a main shelf only or for a main shelf and an expansion shelf requires several megabytes of free space.

#### Backing up the database

Follow these steps to back up the database using proNX 900:

**Step 1** Select **Administration** from the **View** menu.

**Important** If alarms are present on the system, select the **Ignore Alarms** check box. The database backup will not proceed if alarms are present on the system and the **Ignore Alarms** check box has not been selected.

**Step 2** In the Navigation pane, click **Database Backup** to display the database backup settings.

**Step 3** From the drop-down menu in the **Backup Settings** panel, do one of the following:

- a) Choose **Embedded FTP server** to back up the database to your local computer. The embedded FTP server is enabled by default. If you decide to use an external FTP server, you must disable the embedded FTP utility running on the proNX 900.

**Note** If you use the embedded FTP server, the default directory will be the same as the proNX 900 installation directory.

- b) Choose **Remote (S)FTP Server** to back up the database to a remote FTP or SFTP server, specify the connection settings to the server, and then enter the path to the file, including the file name, in the **File** field.

**Note** Some UNIX systems may require you to enter the entire directory path and the database file name in the **File** field.

In the **FTP User ID** and **FTP Password** fields, enter a valid user ID and password.

- c) Choose **SCP** to backup the database to the SCP, and then enter a name for the backup file in the **File** field.

**Note** If you select **SCP**, any backup file already stored on the SCP will be overwritten.

**Step 4** In the **File** field, enter a name for the database file and click **Save As**.

**Step 5** Click **Backup**.

Messages indicating the progress of the database backup appear in the **Status** window.

If the backup is successful, the message `Backup Process Completed Successfully` appears. If the backup fails, an error message appears.

## 2.4.2 Database backup using TL1

Use this procedure to back up the database to the SCP or to an FTP server using TL1.

### Prerequisites

- If backing up to an FTP server, the server must be set up for remote backups.
- The backup location has enough space for the data.

**Note** Data for either a main shelf only or for a main shelf and an expansion shelf requires several megabytes of free space.

### Backing up the database

Follow these steps to back up the database using TL1:

**Step 1** Enter the following at the TL1 command line interface:

```
INVK-DB-BKUP:[TID]:::<CTAG>::TYPE=<TYPE>,[IPADDR=<IPADDR>],
[PATH=<PATH>],[USERID=<USERID>],[PWD=<PWD>],[CHKALM=<CHKALM>];
```

where



<TYPE> is FTP or SCP

<IPADDR> is the address of the FTP server where the backup file will be stored

<PATH> is the path to the database backup file, including the file name

**Note** The value <PATH> can contain a maximum of 54 alphanumeric characters when TYPE=FTP or when TYPE=SFTP and 48 alphanumeric characters when TYPE=SCP.

**Note** Some UNIX systems may require you to enter the entire directory path and the database file name.

<USERID> is the user ID for the FTP server

<PWD> is the password assigned to the user ID

<CHKALM> is Y or N

**Important** If CHKALM=Y and alarms are present on the system, the database backup will not proceed.

If the backup is successful, the system returns the following message:

```
BTI 7000 Series 08-12-31 16:22:02
M 100 COMPLD
;
BTI7000>
BTI 7000 Series 08-12-31 16:22:05
A 103 REPT EVT EQPT
"SCP-1-5:DBBKUPPASS,,05-12-31,16-22-04,,,,,:\"Database Backup
Completed Successfully.\" , , , : , "
;
```

If the backup fails, an error message appears.

## 2.5 Load, invoke, and commit the system software upgrade

This release of the system software can be loaded, invoked, and committed using proNX 900 or TL1.

This section covers the following topics:

- [2.5.1, “Loading, invoking, and committing the system software upgrade using proNX 900 ”](#)
- [2.5.2, “Loading, invoking, and committing the system software upgrade using TL1”](#)

### 2.5.1 Loading, invoking, and committing the system software upgrade using proNX 900

Use this procedure to load, invoke, and commit the system software upgrade to Release 13.5 using proNX 900.

#### What you need

- BTI 7000 Series Release 13.5 CD

<b>Note</b>	The BTI 7000 Series CD contains an encrypted manifest file, a binary image file, and a readme file. The manifest file contains a listing of all the software components contained in the binary image. The manifest file and the binary image file are required for upgrading the system software.
-------------	--

#### Prerequisites

- See [2.1, “Upgrade task flow”](#) and [2.2, “Before you upgrade to Release 13.5”](#).

<b>Important</b>	Review the "Troubleshooting" chapter of the particular solution guide for each module type that is installed on your system, for information about additional procedures that might be required during or after the system software upgrade.
------------------	--

- You can perform the upgrade using the Release 13.5 version of proNX 900.
- If you are using an external FTP or SFTP server to access the BTI 7000 Series CD, the (S)FTP root directory must be configured to serve files from the CD, or the CD files must be copied to the (S)FTP root directory.
- The (S)FTP server and the system must have IP connectivity.
- There are no CONTCOM alarms on the system.

#### Recommendations

- The state of the system is In Service.
- Remove or install modules during the upgrade process only if you are instructed to do so.
- Read section [2.2, “Before you upgrade to Release 13.5”](#) thoroughly before performing this procedure.

Follow these steps to load, invoke, and commit the system software upgrade using proNX 900:

**Important** Be sure to use the release and build number information for the software versions you are managing. The folder names and software release and build numbers used in this procedure are for only example purposes to show the required information. The information used in the examples may not match the release numbers you are managing.

**Step 1** Install Release 13.5 of proNX 900.

**Step 2** Insert the BTI 7000 Series CD into the CD-ROM drive.

**Note** If you are using an FTP server other than the embedded FTP server (for example, a remote PC), install the CD in the external FTP server.

**Step 3** From the menu bar, select **View** and click **Administration**, to open the administration options for the system.

**Step 4** In the left frame, click **Software Upgrade** to display the load and upgrade settings.

**Step 5** From the **Load Settings** drop-down menu, choose one of the following options:

- **Embedded FTP Server** (the default): Click **Browse**; the **Open** dialog appears. From the **Look In** drop-down menu select the folder for the current release that contains the binary image file. The folder name is FW7120\_IMAGES\_USED\_BY\_NS712.
- **Remote FTP Server**: Specify the connection settings to the FTP server. In the **Directory** field, enter the path to the folder that contains the binary image file. The path is the same as the folder name for the current release. See the example of the folder name, above, for Embedded FTP Server.
- **Remote SFTP Server**: Specify the connection settings to the SFTP server. In the **Directory** field, enter the path to the folder that contains the binary image file. The path is the same as the folder name for the current release. See the example of the folder name, above, for Embedded FTP Server.

**Note** Some UNIX systems may require you to enter the entire directory path and file name in the **Directory** field.

**Step 6** Click **Check** to verify that the correct software upgrade file is available.

**Step 7** Click **Load**.

The system software takes several minutes to load.

**Step 8** In the **Upgrade Settings** section, verify that Release 13.5 is specified in the **Inactive Release Number** field, and the current software version is specified in the **Active Release Number** field.

**Step 9** If alarms (other than CONTCOM) are present on the system, select the **Ignore Alarms** check box in the **Upgrade Settings** panel.

**Important** The system software upgrade will not proceed if alarms are present on the system and the **Ignore Alarms** check box has not been selected.

**Step 10** Click **Invoke**.

- The SYSUPGRDPROG (System Software Upgrade in Progress) alarm is raised, and its severity is Minor.
- The modules in the system are loaded with Release 13.5 of the system software.
- The alarm severity changes from Minor to Major and the system then restarts, starting with the SCP and followed by the modules. While the modules are rebooting they cannot communicate with the SCP, and therefore status information about them (such as firmware information) cannot be displayed or updated until they are fully in service.
- The proNX 900 session ends.

**Important** The amount of time that the invoke operation takes to complete depends on the configuration of the NE. For example, for a full four-shelf system, the invoke operation may take up to one hour to complete.

**Note** During re-initialization, the red Fail LED on each module in the NE may light temporarily while the green Active LED is lit.

**Step 11** After the red Fail LED on the SCP turns off, start Release 13.5 and log on to the system.

**Note** It can take several minutes to connect to the system.

**Step 12** If the circuit pack upgrade failure (PACKUPGRD) alarm is raised, follow these steps:

- 1 Allow the system upgrade to finish, as stated in Step 13, next.
- 2 Refer to [5.7, “Module upgrade failure”](#) for more information.

A circuit pack upgrade failure is not service affecting. The module continues to run its original software and continues to process optical signals properly.

**Step 13** In the **Alarms** pane, check the severity of the SYSUPGRDPROG alarm.

- If the severity of the SYSUPGRDPROG alarm is Major, the system upgrade is still in progress. Wait until the severity of the SYSUPGRDPROG alarm changes to Minor, which indicates that the system upgrade is complete, and then proceed to the next step.

**Note** You can refresh proNX 900 while the system upgrade is in progress.

- If the severity of the SYSUPGRDPROG alarm is Minor, the system upgrade is complete. Proceed to the next step.

**Note** At this point, you may cancel the software system upgrade if necessary and revert to the previous version of the system software. For information, see [3.1, “Cancelling a system software upgrade before committing the load using proNX 900”](#).

If the invoke operation fails, see [5.3, “Invoke failure”](#) for information.

**Step 14** From the menu bar, select **View** and click **Administration**, to open the administration options for the system.

**Step 15** In the left frame, click **Software Upgrade**.

**Step 16** In the **Upgrade Settings** panel, verify that Release 13.5 is specified in the **Active Release Number** field.

**Step 17** Click **Commit**.

The SYSUPGRDPROG alarm clears, Release 13.5 is specified in the **Active Release Number** field, and the earlier release (the version from which you upgraded) is specified in the **Inactive Release Number** field.

If the commit operation fails, see [5.4, “Commit failure”](#) for information.

**Step 18** Determine if any modules need to have their firmware upgraded.

Right-click on the system name and select **View Inventory** to see the Inventory View table. The Inventory View table shows the firmware versions that are running on the system.

The FW column shows the firmware versions that are currently running on each module. An explicit version number in this field indicates that the firmware is mismatched with the software version on the module. You may continue to operate in this state, but it is recommended that you upgrade the firmware to match the software. To upgrade the firmware, the module must undergo a cold reset. As a cold reset is service-affecting, it is recommended that you perform the cold reset during a maintenance window. An FW version of **NATIVE** indicates that the firmware version on the module matches the software version and that no action needs to be taken.

**Note** The firmware on the MSI module is automatically upgraded to the latest version, and is always displayed with a version number, not **NATIVE**. You do not need to manually upgrade the MSI module firmware.

You have successfully completed this procedure.

## 2.5.2 Loading, invoking, and committing the system software upgrade using TL1

Use this procedure to load, invoke, and commit the system software upgrade to Release 13.5 using TL1.

## What you need

- BTI 7000 Series CD

**Note** The BTI 7000 Series CD contains an encrypted manifest file, a binary image file, and a readme file. The manifest file contains a listing of all the software components contained in the binary image. The manifest file and the binary image file are required for upgrading the system software.

## Prerequisites

- See [2.1, “Upgrade task flow”](#) and [2.2, “Before you upgrade to Release 13.5”](#).

**Important** Review the "Troubleshooting" chapter of the *Solutions Guide* for each module type installed on the system for information about additional procedures that might be required during or after the system software upgrade.

- You must be logged on to the system.
- If you are using an external FTP or SFTP server to access the BTI 7000 Series CD, the (S)FTP root directory must be configured to serve files from the CD, or the CD files must be copied to the (S)FTP root directory.
- The (S)FTP server and the system must have IP connectivity.
- There are no CONTCOM alarms on the system.

## Recommendations

- The state of the system is In Service.
- Remove or install modules during the upgrade process only if you are instructed to do so.
- Read section [2.2, “Before you upgrade to Release 13.5”](#) thoroughly before performing this procedure.

Follow these steps to load, invoke, and commit the system software upgrade to Release 13.5 using TL1:

**Important** Be sure to use the release and build number information for the software versions you are managing. The folder names and software release numbers, in the examples, are for only example purposes to show the required information. The information used in the examples may not match the release and build numbers you are managing.

**Step 1** Insert the BTI 7000 Series CD into the CD-ROM drive of the FTP server, and connect to the server.

**Step 2** Enter the following at the TL1 command line interface to verify that the correct software file is available:

```
CHK-SYS-UPGRD: [ TID ] : : <CTAG> : : : IPADDR=<IPADDR> , [ PATH=<PATH> ] ,  
[ USERID=<USERID> ] , [ PWD=<PWD> ] ;
```

where

<IPADDR> is the IP address of the server where Release 13.5 of the system software is stored

<PATH> is the directory path to the upgrade software

**Note** If Release 13.5 of the system software is stored in the root directory of the FTP server, the PATH parameter is not required.

<USERID> is the user ID for the FTP server

<PWD> is the password assigned to the user ID

For example,

```
BTI7000> CHK-SYS-UPGRD:abcd::100:::IPADDR=172.25.25.
45,PATH=12_1_0_MAIN_001,USERID=user,PWD=***
```

```
sanity 13-03-06 12:03:48
```

```
M 100 COMPLD
;
BTI7000>
```

```
sanity 13-03-06 12:03:48
A 29 REPT EVT EQPT
"SCP-1-5:SYSCHKPASS,,03-06,12-03-48,,,,,\\"Check upgrade completed
successfully.\",,,:","
```

**Note** If the check operation fails, see [5.1, “Check failures”](#) for information.

**Step 3** Enter the following TL1 command to load Release 13.5 of the system software:

```
LOAD-SYS-UPGRD:[TID]::CTAG:::IPADDR=<IPADDR>,[USERID=<USERID>],
[PWD=<PWD>];
```

where

<IPADDR> is the IP address where software Release 13.5 is stored.

For example,

```
BTI7000>LOAD-SYS-UPGRD:abcd::100:::IPADDR=172.25.25.
45,PATH=12_1_0_MAIN_001,USERID=user,PWD=***
```

```
sanity 13-03-06 12:05:00
```

```
M 100 COMPLD
;
BTI7000>
```

```
sanity 13-03-06 12:08:21
```

```
A 30 REPT EVT EQPT
```

```
"SCP-1-5:SYSLOADPASS,,03-06,12-08-21,,,,,:\"Load upgrade completed  
successfully.\",,,\"[12_1_0_MAIN_001] [172.25.25.45]\"\",:,"  
;
```

The system software takes several minutes to load.

**Note** If the load operations fails, see [5.2, “Load failures”](#) for information.

**Step 4** Enter the following TL1 command to verify that the current version is stored in the active software bank and that software Release 13.5 is stored in the inactive software bank:

```
RTRV-SYS-RELNUM:[TID]::<CTAG>;
```

For example,

```
RTRV-SYS-RELNUM:BTI7000::100;  
BTI7000 2013-12-28 14:22:30  
M 100 COMPLD  
"ACTIVE=Release 12.1.0 C001,INACTIVE=Release 13.5.0 C001,"  
;
```

**Step 5** Enter the following TL1 command to invoke the system software upgrade:

```
INVK-SYS-UPGRD:[TID]::<CTAG>::RELNUM=<relnum>,[CHKALM=<chkalm>;
```

where

<RELNUM> must match the release and build number, shown in the inactive software bank. (Refer to the RTRV-SYS-RELNUM message in Step 4, above.)

<CHKALM> is Y or N

For example,

```
INVK-SYS-UPGRD:BTI7000::100::RELNUM=Release 13.5.0 C001, CHKALM=N;
```

- The SYSUPGRDPROG (System Software Upgrade in Progress) alarm is raised, and its severity is Minor.
- The modules in the system are loaded with the upgraded system software. The alarm severity changes from Minor to Major and the system then restarts, starting with the SCP and followed by the modules, and then the TL1 session ends.

**Important** The amount of time that the invoke operation takes to complete depends on the configuration of the node. For example, for a full four-shelf system, the invoke operation may take up to one hour to complete.



**Note** During re-initialization, the red Fail LED on each module may light temporarily while the green Active LED is lit.

**Step 6** When the red Fail LED on the SCP turns off, log on to the system.

**Note** It can take several minutes to connect to the system.

**Step 7** Enter the following at the TL1 command line interface to check the severity of the SYSUPGRDPROG alarm:

```
RTRV-ALM-ALL:[TID]::CTAG: , , , , ;
```

For example,

```
RTRV-ALM-ALL:BTI7000::100: , , , , ;
```

- If the severity of the SYSUPGRDPROG alarm is MJ (Major), the system upgrade is still in progress. Use the RTRV-ALM-ALL command to check the severity of SYSUPGRDPROG alarm until the severity changes to MN (Minor), which indicates that the system upgrade is complete, and then proceed to the next step.
- If the severity of the SYSUPGRDPROG alarm is MN (Minor), the system upgrade is complete. Proceed to the next step.

**Note** At this point, you may cancel the software system upgrade if necessary and revert to Release 11.1, 11.2, 11.3, 12.1, 12.2, 13.1, or 13.2 of the system software. For information, see [3.2, “Cancelling a system software upgrade before committing the load using TL1”](#).

**Note** If the invoke operation fails, see [5.3, “Invoke failure”](#) for information.

**Step 8** Enter the following syntax at the TL1 command line interface to verify that Release 13.5 of the system software is stored in the active software bank:

```
RTRV-NETTYPE:[TID]::CTAG;
```

For example,

```
RTRV-NETTYPE:BTI7000::100;
BTI7000 2013-12-28 15:20:31
M 100 COMPLD
BTI7000,BTI 7060,WDM,Release 13.5
;
```

**Step 9** Enter the following at the TL1 command line interface to commit the upgrade:

```
CMMT-SYS-UPGRD:[TID]::CTAG:;;
```

For example,

```
CMMT-SYS-UPGRD:BTI7000::100:;;
```

The SYSUPGRDPROG alarm clears. Optionally, you can use the RTRV-SYS-RELNUM command to verify that Release 13.5 of the system software is stored in the

active software bank and that Release 11.1, 11.2, 11.3, 12.1, 12.2, 13.1, or 13.2 is stored in the inactive software bank.

For example,

```
RTRV-SYS-RELNUM:BTI7000::100;
BTI7000 2013-12-28 16:22:30
M 100 COMPLD
"ACTIVE=Release 13.5.0,INACTIVE=Release 12.1.0,"
;
```

**Note** If the commit operation fails, see 5.4, “Commit failure” for information.

**Step 10** Enter the following at the TL1 command line interface to determine if any modules need to have their firmware upgraded.

```
RTRV-INV:[TID]:[<aid>]:[CTAG]::;
```

A response similar to the following is displayed. Examine the response for any instances similar to **FW="x.x.x"** (for example **FW="7.1.1"**). An instance of this type indicates the firmware version that the module is running, and that the firmware is mismatched with the software version on the module. You may continue to operate in this state, but it is recommended that you upgrade the firmware to match the software. To upgrade the firmware, the module must undergo a cold reset. As a cold reset is service-affecting, it is recommended that you perform the cold reset during a maintenance window. An instance of **FW="NATIVE"**, means that the firmware version on the module matches the software version and that no action needs to be taken.

**Note** The firmware on the MSI module is automatically upgraded to the latest version, and is always displayed with a version number, not **NATIVE**. You do not need to manually upgrade the MSI module firmware.

```
BTI7000 00-12-24 14:30:54
M 100 COMPLD
"MS-1,EQPT:NAME=MS-1,PEC=BT7A50AA,CLEI=WMMKTWOKRA,FNAME=Main Shelf 7060,HWREV=
\"0\",SHCONF=5-SLOT,USI=N/A"
"SLOT-1-1,EQPT:NAME=MXP10G,PEC=BT7A48BA,FNAME=10G MULTIPROTOCOL MUXPONDER - SDH,SER=
\"SN00007376\",HWREV=\"1\",FW=\"7.1.1\",MFGDAT=
\"2009-09-25\",MFGLOCN=BTI,TSTDAT=2009-09-25,TSTLOCN=BTI,USI=N/A"
"XFP-1-1-L1,EQPT:PEC=BP3AM4MS,CLEI=WMOTCMYHAA,SER=\"T08J26874\",HWREV=\"00\",MFGDAT=
\"2008-09-29\",WAVELENGTH=1310,REACH=10,MINBR=10000,MAXBR=11100,ENCODING=NRZ,CONNTYPE=LC
,VENDORNAME=\"Opnext Inc.\",VENDORPN=\"TRF5012FS-LA000\",VENDOROUI=
\"000B40\",TXFAULTIMP=Y,TXDISABLEIMP=Y,LOSIMP=Y,DDIAGIMP=Y,MEDIA=OPTICAL,USI=LBFJTU16089
T08J26874"
"SFP-1-1-C2,EQPT:PEC=BP3AD1SS,CLEI=WMOMA0FAAA,SER=\"F6154704019E\",HWREV=
\"0000\",MFGDAT=
\"2006-05-14-01\",WAVELENGTH=850,MINBR=1050,MAXBR=2205,NOMBR=2100,ENCODING=8B10B,CONNTYP
E=LC,VENDORNAME=\"JDS UNIPHASE\",VENDORPN=\"JSH-21S3AB3\",VENDOROUI=\"00019C
\",TXFAULTIMP=Y,TXDISABLEIMP=Y,LOSIMP=Y,DDIAGIMP=Y,MEDIA=OPTICAL,USI=LBFJTU16065F6154704
019E"
```

```
"SLOT-1-5,EQPT:NAME=SCP,PEC=BT7A20CA,FNAME=7060 System Control Processor,SER=
\"SN00101961\",HWREV=\"2\",MFGDAT=
\"2008-09-29\",MFGLOCN=BTI,TSTDAT=2008-09-29,TSTLOCN=BTI,USI=N/A"
```

You have successfully completed this procedure.

## 2.6 Install and provision equipment

---

After the upgrade to Release 13.5 is committed, any new shelves and modules to be deployed can be added and provisioned. For information, see the following documents:

- *Common Equipment Installation Guide*
- *Operations Solution Guide*
- *Solutions Guide* for the Amplifier, DCM, Multiplexer, Transponder, Muxponder, or packetVX portfolio

When installing and provisioning equipment follow the procedures and warnings and cautions listed in the relevant guides.



- Use an ESD wrist strap when handling modules and SFP and XFP transceivers
- Before connecting optical cables to the transceiver ensure that both the optical cable connectors and optical surfaces are clean
- Ensure all disconnected optical ports on the module and disconnected optical cables are fitted with protective caps
- After provisioning it can take from one to two minutes before the configuration is fully synchronized across all resources, depending on the hardware configuration. If you restart or swap the SCP or restore the database within two minutes of provisioning procedures, the synchronization process may not be complete and the previous settings are relearned by the SCP.
- Equipment provisioning cannot be performed during a database restoration or database delete operation
- Do not restart the SCP during a database restoration
- Following a database delete operation all proNx 900 sessions must be terminated and restarted
- Failure to re-route traffic, when replacing modules, can result in loss of data.



- Ensure that all disconnected optical ports on the module and disconnected optical cables are fitted with protective caps



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.

---

### Provisioning considerations

#### VLAN IDs

In release 7.3.x, VLAN IDs 40xx and 40yy are hardcoded to support Flow Redirect. In Release 8.2 or later these VLAN IDs are no longer reserved for Flow Redirect. If you are upgrading to Release 8.2 or later, you need to re-provision the Flow Redirect feature to use other VLAN IDs. Refer to the *packetVX Solutions Guide* for provisioning procedures.

#### Dual 10G Multiprotocol Transponder and 10-Port Multiprotocol Muxponder

The Dual 10G Multiprotocol Transponder (BT7A49AA-I02) is supported in release 11.1 but can be installed in shelves running earlier releases. For more information, see Chapter 11 of the *BTI 7000 Series Transponder Solutions Guide*.

The 10-Port Multiprotocol Muxponder (BT7A48AA-I02, BT7A48AB-I02) is supported in release 13.1 but can be installed in shelves running earlier releases. For more information, see Chapter 10 of the *BTI 7000 Series Muxponder Solutions Guide*.

### **High Temperature Automatic Shutdown**

Beginning with software release 11.1, the system supports High Temperature Automatic Shutdown (HTAS). HTAS shuts down a module when the module exceeds the shutdown temperature threshold. This is a system level setting that is disabled by default. After an upgrade, you must enable HTAS if you want the system to monitor the module temperature.

HTAS is supported on the following:

- Dual 10G Multiprotocol Transponder (BT7A49AA-I02)
- 10 Port Multiprotocol Muxponders (BT7A48AA-I02 and BT7A48AB-I02) modules.
- DWDM C-Band Low Gain Amplifier (LGA) (BT7A02AA), DWDM C-Band Mid Gain Amplifier (MGA) (BT7A03AA) and DWDM C-Band Mid Gain Amplifier with Mid Stage Access (MGM) BT7A04AA)

For information about provisioning HTAS and related TL1 commands refer to the *BTI 7000 Series Transponder Solutions Guide*, *BTI 7000 Series Muxponder Solutions Guide*, *BTI 7000 Series Optical Amplifier and DCM Solutions Guide* and the *BTI 7000 Series TL1 Reference Guide*.

## 2.7 Auto-upgrade support on modules

---

All modules (that is, Transponders, Muxponders, Optical Amplifiers, DCMs, Multiplexers, and packetVX) ship with pre-loaded software. When a module is inserted into a shelf, the module software release number is checked to determine if it matches that of the system software. The module software is automatically upgraded if it is an earlier version than the system software.

During an auto upgrade, the following occurs:

- The UPGRDPROG minor alarm is raised.
- The module upgrade starts.
- The module initializes.
- The UPGRDPROG alarm clears.

**Important** Review the "Troubleshooting" chapter of the *Solutions Guide* for a module portfolio for information about additional procedures that might be required after an auto-upgrade is completed.

## 3.0 Cancelling a system software upgrade

---

This section provides information about cancelling a BTI 7000 Series system software upgrade to a later software version and returning to the current software version—the software version from which you are performing the upgrade.

**Note** Cancelling before and after committing the new load is performed only when you are returning to the same software version from which you are performing the upgrade. For information on downgrading the system software to any other earlier release, refer to [Appendix C, “Downgrading to an earlier system software version”](#).

- [3.1, “Cancelling a system software upgrade before committing the load using proNX 900”](#)
- [3.2, “Cancelling a system software upgrade before committing the load using TL1”](#)
- [3.3, “Cancelling a system software upgrade after committing the load using proNX 900”](#)
- [3.4, “Cancelling a system software upgrade after committing the load using TL1”](#)

## 3.1 Cancelling a system software upgrade before committing the load using proNX 900

---

Use this procedure to cancel a system software upgrade process using proNX 900.

### Prerequisites

- You must be logged into the system using proNX 900.
- The invoke operation of the system software upgrade process has been performed.
- The commit operation of the system software upgrade process has not been performed.
- All modules, including the SCP, have been upgraded and reinitialized.
- The SYSUPGRDPROG (System Software Upgrade in Progress) alarm is raised and its severity is Minor, and that there are no module software upgrades in progress (Use the command RTRV-EQPT to check that the modules are no longer in software download state (SWDL)).

**Important** The examples include software release and build numbers for only example purposes to show the required information, and may not match the software release you are managing. Be sure to use the appropriate information for the software release you are managing.

### Cancelling a system software upgrade process

Follow these steps to cancel a system software upgrade process using proNX 900:

- Step 1** In the **Alarms** pane, verify that a SYSUPGRDPROG (System Software Upgrade in Progress) alarm is raised and its severity is Minor.
- Step 2** Select **Administration** from the **View** menu.
- Step 3** In the **System** pane, click **Software Upgrade**.
- Step 4** In the **Upgrade Settings** panel, verify that Release 13.5 is specified in the **Active Release Number** field and Release 11.1, 11.2, 11.3, 12.1, 12.2, 13.1, or 13.2 is specified in the **Inactive Release Number** field.
- Step 5** Click **Cancel**.

The following confirmation message is displayed:

"Warning: Cancelling an upgrade may cause service interruption. Refer to the Upgrade Guide for details regarding cancelling an upgrade."

Are you sure you want to cancel the upgrade?"

Click **Yes** to cancel the upgrade.



The SYSUPGRDPROG alarm changes to Major, the system restarts, starting with the SCP and followed by the modules, and then the proNX 900 session ends.

**Note** During reinitialization, the red Fail LED on each module may light temporarily, while the green Active LED is lit.

**Step 6** After the red Fail LED on the SCP turns off, start proNX 900, and log on to the system.

**Note** It can take several minutes to connect to the system.

**Step 7** In the Alarms pane, verify that the SYSUPGRDPROG alarm has cleared.

**Step 8** Select **Administration** from the **View** menu.

**Step 9** In the **System** pane, click **Software Upgrade**.

**Step 10** In the **Upgrade Settings** panel, verify that Release 11.1, 11.2, 11.3, 12.1, 12.2, 13.1, or 13.2 is specified in the **Active Release Number** field and Release 13.5 is specified in the **Inactive Release Number** field.

**Note** If the cancel operation fails, see [5.5, “Cancel failure”](#) for information.

You have successfully completed this procedure.

## 3.2 Cancelling a system software upgrade before committing the load using TL1

---

Use this procedure to cancel a Release 11.1, 11.2, 11.3, 12.1, 12.2, 13.1, or 13.2 to Release 13.5 system software upgrade process using TL1.

### Prerequisites

- You must be logged into the system.
- The invoke operation of the system software upgrade process has been performed.
- The commit operation of the system software upgrade process has not been performed.
- All modules, including the SCP, have been upgraded and re-initialized.
- The SYSUPGRDPROG (System Software Upgrade in Progress) alarm is raised and its severity is Minor, and that there are no module software upgrades in progress (Use the command RTRV-EQPT to check that the modules are no longer in software download state (SWDL)).

**Important** The examples include software release and build numbers for only example purposes to show the required information, and may not match the software release you are managing. Be sure to use the appropriate information for the software release you are managing.

### Cancelling a system software upgrade

Follow these steps to cancel a system software upgrade process using TL1:

- Step 1** Enter the following syntax at the TL1 command line interface to verify that a SYSUPGRDPROG (System Software Upgrade in Progress) alarm is raised and its severity is Minor:

```
RTRV-ALM-ALL:[TID]::CTAG:,,,,,,,,;
```

- Step 2** Enter the following syntax at the TL1 command line interface to cancel the system software upgrade and confirm that the SYSUPGRDPROG alarm clears:

```
CANC-SYS-UPGRD:[TID]::CTAG;
```

For example,

```
CANC-SYS-UPGRD:BTI7000::100;
```

The system returns the following messages:

```
BTI7000 10-09-30 09:46:32
A 94 REPT ALM EQPT
"SCP-1-5:CL,SYSUPGRDPROG,NSA,09-29,16-00-43,,,,,:\"Cleared: System upgrade in
```

```

progress.\",,,:,\"
;

BTI7000 10-09-30 09:46:32
** 95 REPT ALM EQPT
   \"SCP-1-5:MJ,SYSUPGRDPROG,NSA,09-30,09-46-31,,,,,:\"System upgrade in progress.
\",,,:,\"
;

```

The modules on the main shelf start upgrading (reverting to the previous load). This is followed by the re-initialization of the modules and the SCP, causing you to lose communication with the SCP. Once the SCP has finished restarting, log back in.

**Note** During re-initialization, the red Fail LED on each module may light temporarily, while the green Active LED is lit.

**Step 3** After the red Fail LED on the SCP turns off, log on to the system.

**Note** It can take several minutes to connect to the system.

Once you are logged in to the system, the SYSUPGRDPROG alarm is active:

```
\"SCP-1-5,EQPT:MJ,SYSUPGRDPROG,NSA,09-30,09-47-20,NEND,,,\"System upgrade in progress.\""
```

All of the modules on the shelf re-initialize. Once all of the modules are finished re-initializing (which may take several minutes), the SYSUPGRDPROG alarm clears.

```

BTI7000 10-09-30 09:48:24
A 7 REPT ALM EQPT
   \"SCP-1-5:CL,SYSUPGRDPROG,NSA,09-30,09-47-20,,,,,:\"Cleared: System upgrade in
progress.\",,,:,\"

```

**Step 4** Enter the following syntax at the TL1 command line interface to verify that Release 11.1, 11.2, 11.3, 12.1, 12.2, 13.1, or 13.2 is stored in the active software bank and Release 13.5 is stored in the inactive software bank:

```
RTRV-SYS-RELNUM:[TID]::<CTAG>;
```

For example,

```
RTRV-SYS-RELNUM:BTI7000::100;
```

The system returns the following message:

```

BTI7000 10-09-30 09:51:31
M 100 COMPLD
   \"ACTIVE=Release 12.1.0 C001,INACTIVE=Release 13.5.0 C001\"
;

```

**Note** If the cancel operation fails, see [5.5](#), “[Cancel failure](#)” for information.

You have successfully completed this procedure.

### 3.3 Cancelling a system software upgrade after committing the load using proNX 900

After a system software upgrade from Release 11.1, 11.2, 11.3, 12.1, 12.2, 13.1, or 13.2 to Release 13.5 has been committed, use this procedure to revert to the system software load that already exists in the inactive software bank (from which you have upgraded) using proNX 900.



#### Prerequisites

- You must be logged on to the system using Release 13.5 of proNX 900.
- There are no CONTCOM alarms on the system.
- Back up the database.

#### Recommendations

- The state of the system is In Service.
- Remove or install modules during the downgrade process only if you are instructed to do so.

#### Downgrading the system software

Follow these steps to downgrade the system software using proNX 900.

**Important** Any modifications provisioned on the system while Release 13.5 of the system software was running will be lost.

**Note** If there are no active modules on the system, database recovery is not possible.

**Step 1** Select **Administration** from the **View** menu.

**Step 2** In the **System** pane, click **Software Upgrade** to display the upgrade settings.

**Step 3** In the **Upgrade Settings** panel, verify that Release 11.1, 11.2, 11.3, 12.1, 12.2, 13.1, or 13.2 is specified in the **Inactive Release Number** field.

**Step 4** If alarms are present on the system, select the **Ignore Alarms** check box in the **Upgrade Settings** panel.

**Important** The system software downgrade will not proceed if alarms are present on the system and the **Ignore Alarms** check box has not been selected.

**Step 5** Click **Invoke**.

- The SYSUPGRDPROG (System Software Upgrade in Progress) is raised, and its severity is Minor.
- The modules in the system are loaded with Release 11.1, 11.2, 11.3, 12.1, 12.2, 13.1, or 13.2 of the system software. The alarm severity changes to Major, and the system

then restarts, starting with the SCP and followed by the modules, and then the proNX 900 session ends.

**Important** The amount of time that the invoke operation takes to complete depends on the configuration of the node. For example, for a full four-shelf system, the invoke operation may take up to one hour to complete.

**Note** During re-initialization, the red Fail LED on each module may light temporarily while the green Active LED is lit.

**Step 6** When the red Fail LED on the SCP turns off, start proNX 900, and log on to the system.

**Note** It can take several minutes to connect to the system.

**Step 7** In the **Alarms** pane, check the severity of the SYSUPGRDPROG alarm.

- If the severity of the SYSUPGRDPROG alarm is Major, the system downgrade is still in progress. Wait until the severity of the SYSUPGRDPROG alarm changes to Minor, which indicates that the system downgrade is complete, and then proceed to the next step.
- If the severity of the SYSUPGRDPROG alarm is Minor, the system downgrade is complete. Proceed to the next step.

**Note** If the invoke operation fails, see [5.3, “Invoke failure”](#) for information.

**Step 8** Select **Administration** from the **View** menu.

**Step 9** In the **System** pane, click **Software Upgrade**.

**Step 10** In the **Upgrade Settings** panel, verify that Release 11.1, 11.2, 11.3, 12.1, 12.2, 13.1, or 13.2 is specified in the **Active Release Number** field and Release 13.5 is specified in the **Inactive Release Number** field.

You have successfully completed this procedure.

## 3.4 Cancelling a system software upgrade after committing the load using TL1

After a system software upgrade from Release 11.1, 11.2, 11.3, 12.1, 12.2, 13.1, or 13.2 to Release 13.5 has been committed, use this procedure to revert to the system software load that already exists in the inactive software bank (from which you have upgraded). If the load from which you upgraded has been overwritten in the inactive software bank, use the procedure "Downgrading the system software using TL1" to downgrade your system.

### Prerequisites

- You must be logged into the system.
- The commit operation of the system software upgrade process has been performed.
- The SYSUPGRDPROG (System Software Upgrade in Progress) alarm is not raised.

**Important** The examples include software release and build numbers for only example purposes to show the required information, and may not match the software release you are managing. Be sure to use the appropriate information for the software release you are managing.

### Reverting to an existing system software load

This procedure re-instates the database from the previous load.

Follow these steps to revert to the system software load that already exists in the inactive software bank (from which you have upgraded):

**Step 1** Enter the following syntax at the TL1 command line interface to verify that a SYSUPGRDPROG (System Software Upgrade in Progress) alarm is not raised:

```
RTRV-ALM-ALL:[TID]::CTAG:,, , , , ;
```

**Step 2** Enter the following at the TL1 command line to verify that Release 13.5 is stored in the active software bank and that the load from which you upgraded (Release 11.1, 11.2, 11.3, 12.1, 12.2, 13.1, or 13.2) is stored in the inactive software bank:

```
RTRV-SYS-RELNUM:[TID]::<CTAG>;
```

For example,

```
RTRV-SYS-RELNUM:BTI7000::100;
BTI7000 2008-01-21 14:22:30
M 100 COMPLD
"ACTIVE=Release 13.5.0 ,INACTIVE=Release 12.1.0 ,"
;
```

**Step 3** Enter the following at the TL1 command line interface to invoke the system software upgrade:

```
INVK-SYS-UPGRD:[TID]::<CTAG>::RELNUM=<relnum>,[CHKALM=<chkalm>];
```

where

<RELNUM> is the release number of the system software in the inactive bank to which you want to revert.

<CHKALM> is Y or N

For example,

```
INVK-SYS-UPGRD:BTI7000::100::RELNUM=9.3.0,CHKALM=N;
```

- The SYSUPGRDPROG (System Software Upgrade in Progress) alarm is raised, and its severity is Minor.
- The modules in the system are loaded with the upgraded system software. The alarm severity changes from Minor to Major and the system then restarts, starting with the SCP and followed by the modules, and then the TL1 session ends.

**Important** The amount of time that the invoke operation takes to complete depends on the configuration of the node. For example, for a full four-shelf system, the invoke operation may take up to one hour to complete.

**Note** During re-initialization, the red Fail LED on each module may light temporarily while the green Active LED is lit.

**Note** If the invoke operation fails, see [5.3, “Invoke failure”](#) for information.

**Step 4** After the red Fail LED on the SCP turns off, log on to the system.

**Note** It can take several minutes to connect to the system.

Once you are logged in to the system, the SYSUPGRDPROG alarm is active:

```
"SCP-1-5,EQPT:MJ,SYSUPGRDPROG,NSA,09-30,09-47-20,NEND,,,\"System upgrade in progress.\""
```

All of the modules on the shelf re-initialize. Once all of the modules are finished re-initializing (which may take several minutes), the SYSUPGRDPROG alarm clears.

```
BTI7000 10-09-30 09:48:24
```

```
A 7 REPT ALM EQPT
```

```
"SCP-1-5:CL,SYSUPGRDPROG,NSA,09-30,09-47-20,,,,,\"Cleared: System upgrade in progress.\",,,,"
```

**Step 5** Enter the following syntax at the TL1 command line interface to verify that Release 11.1, 11.2, 11.3, 12.1, 12.2, 13.1, or 13.2 is stored in the active software bank and Release 13.5 is stored in the inactive software bank:

```
RTRV-SYS-RELNUM:[TID]::<CTAG>;
```

For example,

```
RTRV-SYS-RELNUM:BTI7000::100;
```

The system returns the following message:



```
BTI7000 10-09-30 09:51:31
M 100 COMPLD
"ACTIVE=Release 12.1.0 C001,INACTIVE=Release 13.5.0 C001"
;
```

**Note** If the invoke operation fails, see [5.3, “Invoke failure”](#) for information.

You have successfully completed this procedure.



## 4.0 Useful procedures

---

This section provides information about other procedures you can perform when upgrading.

- [4.1, “Determining system software release numbers”](#)
- [4.2, “Determining the firmware version”](#)
- [4.3, “Database restore using proNX 900”](#)
- [4.4, “Database restore using TL1”](#)
- [4.5, “Establishing a proNX 900 session using Ethernet”](#)
- [4.6, “Establishing a TL1 session using RS-232”](#)

## 4.1 Determining system software release numbers

---

Use this procedure to determine the release number of the active and inactive system software.

### Determining the system software release number using proNX 900

- 1 Select **Administration** from the **View** menu.
- 2 In the System pane, select **Software Upgrade**.

System release number information is provided in the **Active Release Number** and **Inactive Release Number** fields.

### Determining the system software release number using TL1

The following table lists the TL1 commands that retrieve system software release numbers.

Command	Release retrieved
RTRV-NETTYPE	Active release
RTRV-SYS-RELNUM	Active release and Inactive release

## 4.2 Determining the firmware version

You can view the firmware version for the system inventory or a hardware module, using proNX 900 and TL1 interfaces.

### Determining the firmware version using proNX 900

In proNX 900 you view the firmware for the system inventory and hardware module in two separate dialogs, as described in the sections that follow.

Use this procedure to view the firmware for the system inventory.

- 1 In the toolbar, click the **System Configuration** icon. The list of systems appears in the Navigation tree.
- 2 Right-click on the system name and click **View Inventory**. The **Inventory View** table appears.

**Figure 4-1 Inventory View Table**

AID	NAME	PEC	CLEI	FNAME	SER	HWREV	FW	MFGDAT	MFGLOCN	TSTDAT	TSTLOCN	WAVELE...
MS-1	MS7200	BT7A51AA	UNKNO...	Main Sh...	SN1012...			2010-07...	BTI Nort...	2010-07...	BTI Nort...	
SLOT-1-1	SCP	BT7A20...		7060 Sy...	SE0939...	5	NATIVE	2009-09...	19	2009-09...	19	
SLOT-1-2	DTPR	BT7A49...		Dual 10...	SE1306...	2	1-1	2013-02...	19	2013-02...	19	
SLOT-1-9	PVX	BT7A81AA		12 POR...	SE0950...	11	NATIVE...	2009-12...	19	2010-07...	16	
SFP-1-9...		BP3AM1...			PMM3N...	01		2012-05...				1310
PVX-1-9-...												
PVX-1-9-...												
SLOT-1-...	PVX	BT7A81...		24 POR...	SE1011...	14	NATIVE...	2010-03...	19	2010-03...	19	
PVX-1-1...												
PVX-1-1...												
PVX-1-1...												
PVX-1-1...												
SLOT-1-...	DTPR	BT7A41...		DUAL 4...	SE0952...	9	NATIVE	2009-12...	19	2009-12...	19	
SFP-1-1...		BP3AM1...			PMM3P9S	01		2012-05...				1310
SI-1	MSI	BT7A53...		7200 MA...	SN1024...	3	1111	2010-06...	19	2010-06...	16	
CCM-1-1	CCM	BT7A54...		7200 C...	SE1044...	15		2010-10...	19	2012-03...	16	
CU-1-1	CU	BT7A52...		7060 C...	SX0942...	5		2009-10...	19	2009-10...	19	
CU-1-2	CU	BT7A52...		7060 C...	SX0942...	5		2009-10...	19	2009-10...	19	
CU-1-3	CU	BT7A52...		7060 C...	SX0942...	5		2009-10...	19	2009-10...	19	
CU-1-4	CU	BT7A52...		7060 C...	SX0942...	5		2009-10...	19	2009-10...	19	

- 3 Click **Refresh** to ensure you are viewing the latest inventory information.
- 4 Go to the **FW** column to learn the firmware version.
- 5 Click **Close** to exit this view.

Use this procedure to view the firmware for a hardware module.

- 1 In the toolbar, click the **System Configuration** icon. The list of systems appears in the Navigation tree.
- 2 Expand the system folder for the system that includes the particular hardware module you want to view.
- 3 Right-click on a module, either from the Navigation tree or the graphical view, and click **Display Module Inventory**. The **Display Inventory Information** dialog appears.

**Figure 4-2 Display Inventory Information Dialog**

**Display Inventory Information for the Module in Slot 1**

**General**

Full Name: 7060 System Control Processor

Name: SCP Shelf: 1 Slot: 1

**Hardware**

PEC Code: BT7A20CA Release Number: 5

CLEI Code: Serial Number: SE09391073

Firmware: NATIVE

USI: N/A

**Manufacturing**

Date: 2009-09-26 Location: 19

**Testing**

Date: 2009-09-26 Location: 19

Close Help

- 4 Go to the **Firmware** field to learn the firmware version for that module. Note the following:
  - If the field value indicates NATIVE, the firmware is compatible to the current system software version.
  - If the field value indicates an actual version number, the firmware is not compatible to the current system software version. The firmware should be upgraded.

**Note** The firmware on the MSI module is automatically upgraded to the latest version, and is always displayed with a version number, not **NATIVE**. You do not need to manually upgrade the MSI module firmware.

- 5 Click **Close** to exit this view.

## Determining the firmware version using TL1

The following command retrieves information for the system inventory and hardware modules:

```
RTRV-INV:[TID]:[<aid>]:[CTAG]:;
```

The following example displays a portion of the output of this command. The **FW** parameter indicates the firmware version. Note the following:

- If the FW value indicates NATIVE, the firmware is compatible to the current system software version.
- If the FW value indicates an actual version number, the firmware is not compatible to the current system software version, and the firmware should be upgraded.

<b>Note</b>	The firmware on the MSI module is automatically upgraded to the latest version, and is always displayed with a version number, not <b>NATIVE</b> . You do not need to manually upgrade the MSI module firmware.
-------------	---

```
RTRV-INV:BTI7000::100::;
BTI7000 00-12-24 14:30:54
M 100 COMPLD
"MS-1,EQPT:NAME=MS-1,PEC=BT7A50AA,CLEI=WMMKTWOKRA,FNAME=Main Shelf
7060,HWREV=\"0\",USI=N/A"
"SLOT-1-1,EQPT:NAME=MXP10G,PEC=BT7A48BA,FNAME=10G MULTIPROTOCOL MUXPONDER
- SDH,SER=\"SN00007376\",HWREV=\"1\",FW=\"NATIVE\",MFGDAT=
\"2009-09-25\",MFGLOCN=BTI
Northside,TSTDAT=2009-09-25,TSTLOCN=BTI Northside,USI=N/A"
"XFP-1-1-L1,EQPT:PEC=BP3AM4MS,CLEI=WMOTCMYHAA,SER=\"T08J26874\",HWREV=
\"00\",MFGDAT=

.....
```

## 4.3 Database restore using proNX 900

---

Use this procedure to restore the system database from a backup using proNX 900.

### What you need

- Backup file of the database

### Prerequisites

- The database backup file corresponds to the network element to which it will be restored.

<b>Note</b>	If restoring a database with communication port settings that are different from the current settings, connectivity can be lost. After the database restore operation is completed, reconnect using the communication port settings specified in the restored database.
-------------	---

<b>Important</b>	Equipment provisioning cannot be performed during a database restore operation.
------------------	---

<b>Warning</b>	Do not restart the SCP during a database restore operation.
----------------	---

### Restoring the database

Follow these steps to restore the database:

**Step 1** Select **Administration** from the **View** menu.

**Step 2** In the System pane, click **Database Restore**.

**Step 3** In the **Load Settings** panel, do one of the following:

- Choose **Embedded FTP Server** to load a database backup file stored on the embedded FSTP server, and then click **Browse** to navigate to and select the file.
- Choose **Remote (S)FTP Server** to load a database backup file stored on a remote (S)FTP server, enter the IP address of the FTP server, enter a user ID and a password in the **FTP User ID** and **FTP Password** fields, respectively, and then enter path to the file, including the file name, in the **File** field.

<b>Note</b>	Some UNIX systems may require you to enter the entire directory path and the database file name in the <b>File</b> field.
-------------	---

<b>Note</b>	Windows users should use a UNIX style directory name on a Windows FTP server. For example, if the files are stored in C:/Program Files/FTP Server/Files, omit the C: and enter the path as /Program Files/FTP Server/Files.
-------------	---

- Choose **SCP** to load the database backup file stored on the SCP.

**Step 4** Click **Load**.

The file name of the database backup file appears in the **Status** window of the **Database Restore Settings** panel.



**Step 5** Click **Invoke**.

**Step 6** Do one of the following:

- a) Click **Accept**, and then proceed to the next step.
- b) Click **Cancel** to cancel the database restore operation.

**Note** Cancelling the database restore operation causes the system to restart and all proNX 900 sessions to end.

**Step 7** Click **Commit** to restore the database

Messages indicating the progress of the database restore operation appear in the **Status** window.

If the database restore operation is successful, the message `Restore Process Completed Successfully` appears. If the operation fails, an error message appears.

You have successfully completed this procedure.

## 4.4 Database restore using TL1

---

Use this procedure to restore the system database from a backup using TL1.

### What you need

- Backup file of the database

### Prerequisites

- All alarms on the system have been cleared.
- The database backup file corresponds to the network element to which it will be restored.
- If a system has a packetVX module, you should delete the existing database before you restore the database from backup; refer to the *BTI 7000 Series Operations Solutions Guide* for instructions on how to do this.

<b>Note</b>	If restoring a database with communication port settings that are different from the current settings, connectivity can be lost. After the database restore operation is completed, reconnect using the communication port settings specified in the restored database.
-------------	---

<b>Important</b>	Equipment provisioning cannot be performed during a database restore operation.
------------------	---

<b>Warning</b>	Do not restart the SCP during a database restore operation.
----------------	---

### Restoring the database

Follow these steps to restore the database:

**Step 1** Enter the following syntax at the TL1 command line interface to load the database file:

```
LOAD-DB-RST:[TID]::<CTAG>:::TYPE=<TYPE>,[IPADDR=<IPADDR>],  
[PATH=<PATH>],[USERID=<USERID>],[PWD=<PWD>],[TIDCHK=<TIDCHK>;
```

where

<TYPE> is FTP or SCP

<IPADDR> is the address of the FTP server where the backup file is stored

<PATH> is the path to the database backup file, including the file name

<b>Note</b>	The value <PATH> can contain a maximum of 54 alphanumeric characters when TYPE=FTP and 48 alphanumeric characters when TYPE=SCP.
-------------	--

<b>Note</b>	Some UNIX systems may require you to enter the entire directory path and the database file name.
-------------	--

<USERID> is the user ID for the FTP server

<PWD> is the password assigned to the user ID

<TIDCHK> is Y or N

If the value <PATH> includes the TID, the TID in the database file name must match the TID of the system. However, if the default file name is changed, set the parameter TIDCHK to N.

The system returns the following message:

```

      NYC101 06-01-28 06:22:01
M   100 COMPLD
;
BTI7000>
      NYC101 06-01-28 06:22:03
A   3 REPT EVT EQPT
      "SCP-1-5:DBLOADPASS,,06-01-28,06-22-02,,,,,:\"Database Load
Completed Successfully.\",,\",[BTI7000_NYC101_January24_2006] [10.1.1.
100]\",:,,"
;

```

**Step 2** Enter the following syntax at the TL1 command line to retrieve the database file:

```
RTRV-DB-RST:[TID]::<CTAG>;
```

For example,

```
RTRV-DB-RST:NYC101::100;
```

The system returns the following message, which indicates the name of the database file that is loaded:

```

      NYC101 06-01-28 06:22:02
M   100 COMPLD
      "[BTI7000_NYC101_January24_2006]";
;

```

**Step 3** Enter the following syntax at the TL1 command line to invoke the database restore process:

```
INVK-DB-RST:[TID]::<CTAG>:::FILENAME=<FILENAME>,
[CHKALM=<CHKALM>];
```

where

<FILENAME> is the name of the database file

<CHKALM> is Y or N

**Note** The system defaults to the following format for the file name: BTI7000\_<NENName>\_<MONTH><DAY>\_<YEAR>. For the file name to function correctly, one or more alphabetic characters and the underscore must precede <NENName>.

For example,

```
INVK-DB-RST:BTI7000::100:::
_NYC101_January24_2006,CHKALM=N;
```

The system returns the following message:

```
NYC101 06-01-28 06:23:05
M 100 COMPLD
;
BTI7000>
NYC101 03-01-28 06:23:06
** 4 REPT ALM EQPT
"SCP-1-5,MJ,DBRSTPROG,NSA,06-01-28,06-23-05,,,,,\\"Database
Restore In Progress.\",,,,,"
;
NYC101 03-01-28 06:23:06
A 5 REPT EVT EQPT
"SCP-1-5:INVKDBRSTPASS,,06-01-28,06-23-05,,,,,\\"Invoke
Database Restore Completed Successfully.\",,,,,"
;
```

**Step 4** Do one of the following:

- a) To accept the database file, enter the following syntax at the TL1 command line interface, and then proceed to the next step:

```
ACPT-DB-RST:[TID]::<CTAG>;
```

For example,

```
ACPT-DB-RST:NYC101::100;
```

The system returns the following message:

```
NYC101 06-01-28 06:23:32
M FD COMPLD
;
BTI7000>
NYC101 06-01-28 06:23:33
A 6 REPT EVT EQPT
"SCP-1-5:APPLDBRSTPASS,,06-01-28,06-23-32,,,,,\\"Apply
Database Restore Completed Successfully.\",,,,,"
;
```

- b) To cancel the database restore operation, enter the following at the TL1 command line interface:

```
CANC-DB-RST:[TID]::<CTAG>;
```

For example,

```
CANC-DB-RST:NYC101::100;
```

The system returns the following message:

```
NYC101 06-01-28 06:23:54
A 21 REPT ALM EQPT
"SCP-1-5,CL,DBRSTPROG,NSA,06-01-28,06-23-54,,,,,\\"Clear
Database Restore In Progress.\",,,,,"
;
```

<b>Note</b>	Cancelling the database restore operation causes the system to restart and all TL1 sessions to end.
-------------	---

**Step 5** Enter the following at the TL1 command line interface to commit the database restore operation:

```
CMMT-DB-RST:[TID]::<CTAG>;
```

For example,

```
CMMT-DB-RST:NYC101::100;
```

The system returns the following message:

```
BTI7000>  
06-01-28 06:23:54  
M 100 COMPLD  
;
```

You have successfully completed this procedure.

## 4.5 Establishing a proNX 900 session using Ethernet

Use 4.5.1, “Method One: Connecting through the management LAN”, or 4.5.2, “Method Two: Connecting through the craft LAN port” to establish an Ethernet connection to the system.

**Note** The same functions are available through the craft LAN and the management LAN interfaces.

The following table lists the IP addresses for the BTI 7000 Series LAN communication ports.

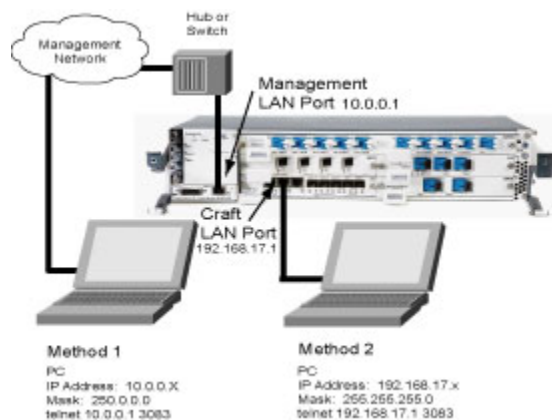
**Table 4-1 IP Addresses**

Communications Port	Default IP Address	Default IP Mask	Default IP Gateway
<b>Default IP Addresses</b>			
Management LAN Port	10.0.0.1	255.0.0.0	0.0.0.0
Craft LAN Port	192.168.17.1	255.255.255.0	0.0.0.0
<b>For a PC Connected To:</b>			
Management LAN Port	10.x.y.z Where x and y are 0 to 255, and $2 \leq z \leq 254$	255.0.0.0	
Craft LAN Port	192.168.17.z Where $2 \leq z \leq 254$	255.255.255.0	

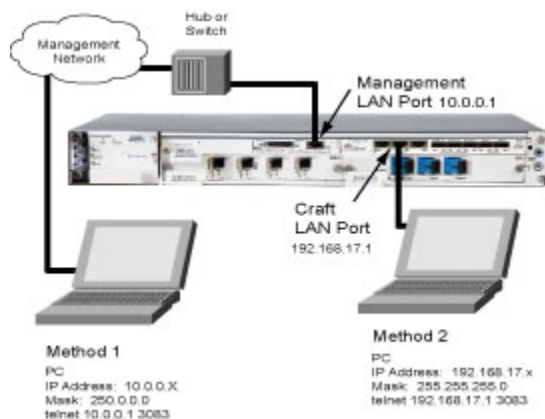
**Note** The Ethernet ports are set to Auto-Negotiate. To ensure optimum communication between the system and your equipment, we recommend that you set your equipment to Auto-Negotiate, as well.

The following illustrations shows the two methods to use when establishing a TL1 session using Ethernet.

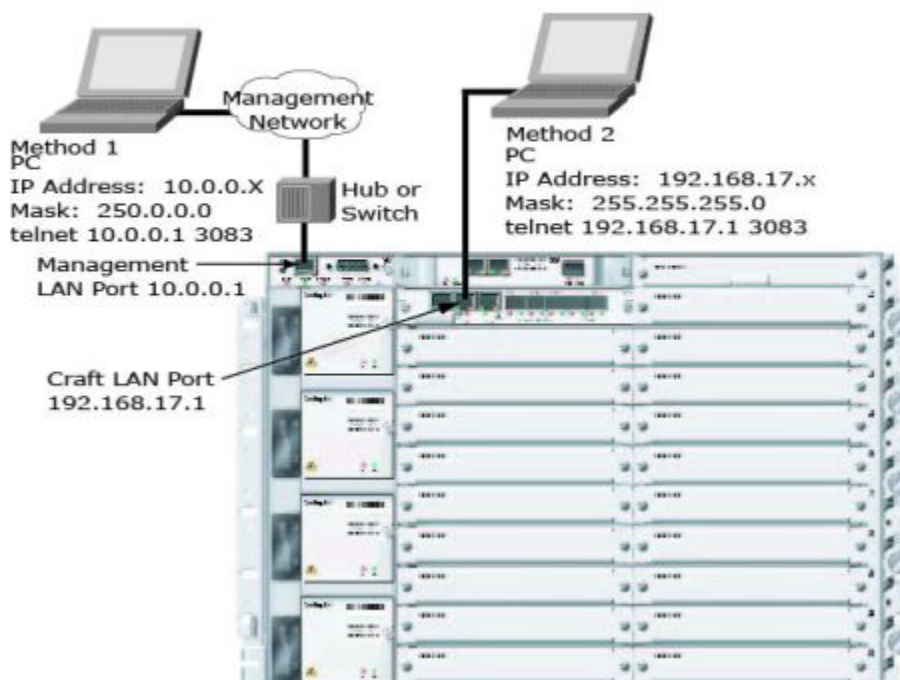
### Establishing a proNX 900 session on the BTI 7060 using Ethernet



### Establishing a proNX 900 session on the BTI 7030 using Ethernet



### Establishing a proNX 900 session on the BTI 7200 using Ethernet



## 4.5.1 Method One: Connecting through the management LAN

Authorization required

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

Use this procedure to connect a PC, or router, to the BTI 7000 Series equipment through a hub or switch that is connected to the management LAN port.

To connect a PC directly to the management LAN port on the BTI 7000 Series, you require a CAT 5 shielded, grounded Ethernet cable of sufficient length with RJ-45 male connectors.

The Ethernet LAN ports automatically determine what device is attached and they automatically configure the input and output signals for the Ethernet cable used.

#### **Step 1 Provision the IP Address**

If not yet configured, provision the BTI 7000 Series with the IP address of your intended management Ethernet LAN.

#### **Step 2 Connect the BTI 7000 Series Ethernet Cables**

- a) Insert one end of a shielded and grounded Ethernet cable in the management LAN port.
- b) Insert the other end of the shielded and grounded Ethernet cable in the RJ-45 female Ethernet LAN connector on your hub or switch.

#### **Step 3 Connect the Computer Ethernet Cables**

- a) Insert one end of a shielded and grounded Ethernet cable in the RJ-45 female Ethernet LAN connector on your PC.
- b) Insert the other end of the shielded and grounded Ethernet cable in the RJ-45 female connector of your management LAN.

#### **Step 4 Start a proNX 900 Session**

#### **Step 5 Log on to the BTI 7000 Series using the proNX 900**

You have successfully completed this procedure.

### **4.5.2 Method Two: Connecting through the craft LAN port**

#### **Authorization required**



Use this procedure to connect a PC to a BTI 7000 Series shelf through the craft LAN port.

The BTI 7030 Ethernet LAN ports automatically determine what device is attached and they automatically configure the input and output signals for the Ethernet cable used.

#### **Step 1 Provision the IP Address**

If not yet configured, provision the BTI 7000 Series shelf with the IP address of your intended craft Ethernet LAN.

#### **Step 2 Connect the Ethernet Cable**



- a) Insert one end of the shielded and grounded Ethernet cable in the craft LAN port.
- b) Insert the other end of the shielded and grounded Ethernet cable in the RJ-45 female Ethernet LAN connector on your PC or laptop.

**Step 3 Start a proNX 900 Session**

**Step 4 Log on to the BTI 7000 Series using the proNX 900**

You have successfully completed this procedure.

## 4.6 Establishing a TL1 session using RS-232

---

### Authorization required

Authorization Required

Superuser

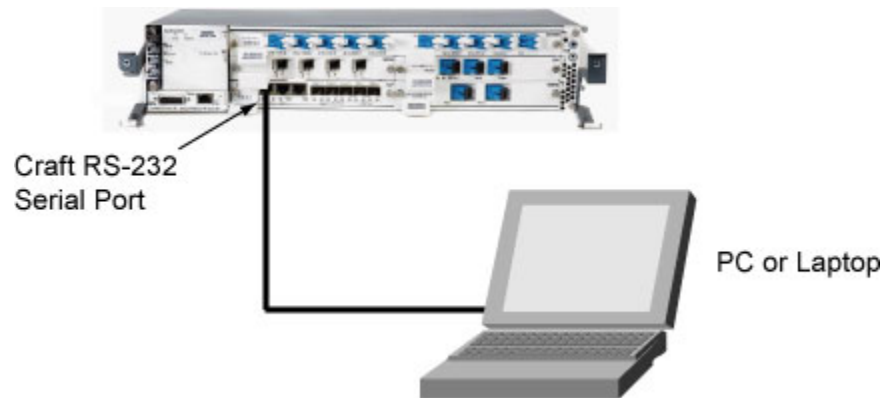
Provisioning

Maintenance

Surveillance

Use this procedure to connect a PC to a BTI 7000 Series shelf through the RS-232 craft serial port on the shelf.

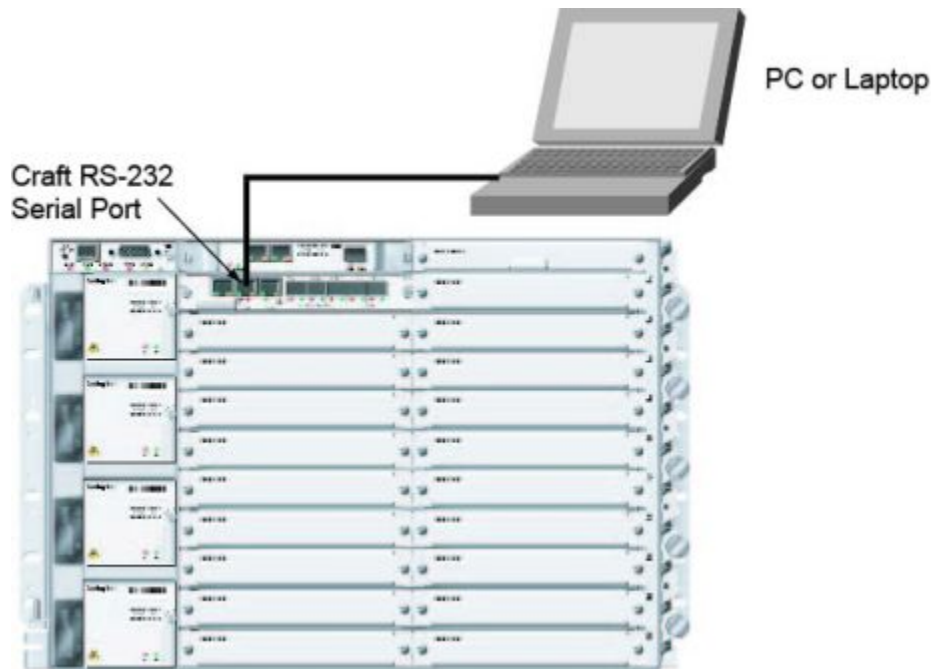
### Establishing a TL1 session using the RS-232 Craft serial port on a BTI 7060



### Establishing a TL1 session using the RS-232 Craft serial port on a BTI 7030



---

**Establishing a TL1 session using the RS-232 Craft serial port on a BTI 7200****Step 1 Connect the RS-232 Cable**

- 1 Insert one end of the RS-232 cable in the craft serial port on the BTI 7000 Series shelf.
- 2 Insert the other end of the RS-232 cable in the RS-232 male connector on your PC or laptop.

**Step 2 Set the RS-232 Parameters**

Set the default RS-232 parameters for the PC to match the BTI 7000 Series shelf:

Rate: 9600 bps

Data Bits: 8 bits

Parity: None

Stop Bits: 1 bit

Flow Control: None

**Step 3 Establish a TL1 Session**

From a terminal emulator, establish a TL1 session to the BTI 7000 Series shelf by pressing the Return key.

**Response**

The system responds with the system prompt.

**Step 4 Log on to the BTI 7000 Series**

To log on to the BTI 7000 Series, enter the following at the TL1 command line interface:

```
ACT-USER:[TID]:<uid>:<CTAG>::<pid>;
```

where

**TID** is the target identifier (BTI7000 is the default target identifier)

**uid** is the user identifier (admin is the default system administrator uid)

**CTAG** is the correlation tag (100 is the default correlation tag)

**pid** is the password identifier (admin is the default system administrator pid)

<b>Note</b>	User identifier "admin" and password identifier "admin" are the default system administrator credentials.
-------------	---

#### Example

```
ACT-USER:BTI7000:admin:100::*****;
```

#### Response

The BTI 7000 Series sends back a COMPLD message to indicate a successful log on.

You have successfully completed this procedure.

## 4.6.1 RS-232 serial communications

The BTI 7000 Series has a craft serial port that uses the RS-232 protocol.

### Cables required

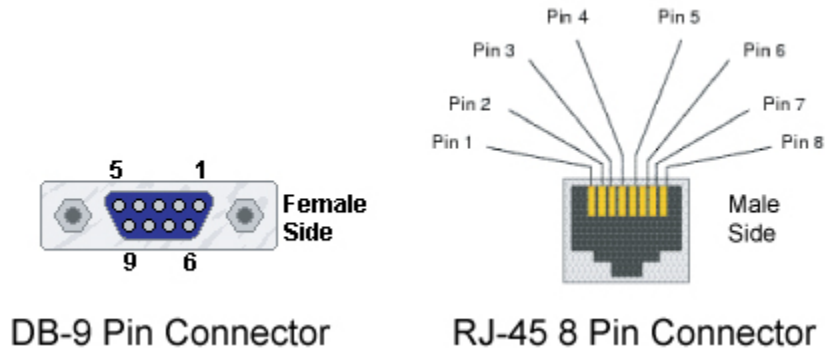
When connecting a PC or laptop to the craft serial port, use a straight-through RS-232 cable with a DB-9 pin male connector.

If you anticipate using the RS-232 serial port, determine the length of cable required to connect the system to your PC, and prepare the cable with the appropriate male connector.

### RS-232 pin assignment

The following figure shows the RS-232 DB-9 pin DCE connector as well as the RS-232 RJ-45 8 pin connector and the associated pin numbering schemes.

## DB-9 Pin Connector and 8 Pin RJ-45 Connector Numbering Schemes



The following table lists the RS-232 pin assignment for the DB-9 pin connector and RJ-45 connector pin numbering schemes.

**Table 4-2 Pin Assignments for RS-232 DB-9 Pin Connectors and RS-232 RJ-45 Connectors**

DB-9 Pin Connector	DCE Purpose	RJ-45 Connector	DCE Purpose
1	Data Terminal Ready	1	Request to Send
2	Transmitted Data	2	Data Terminal Ready
3	Received Data	3	Transmitted Data
4	DTE Ready	4	Signal Ground
5	Signal Ground	5	Signal Ground
6	DCE Ready	6	Received Data
7	Clear to Send	7	Data Carrier Detect / Data Set Ready
8	Request to Send	8	Clear to Send
9	Ring Detector		



## 5.0 Troubleshooting

---

This section provides information about troubleshooting the issues that might arise when upgrading from Release 11.1, 11.2, 11.3, 12.1, 12.2, 13.1, or 13.2 to Release 13.5.

- [5.1, “Check failures”](#)
- [5.2, “Load failures”](#)
- [5.3, “Invoke failure”](#)
- [5.4, “Commit failure”](#)
- [5.5, “Cancel failure”](#)
- [5.6, “Provisioning failure”](#)
- [5.7, “Module upgrade failure”](#)
- [5.8, “Database recovery failure”](#)

## 5.1 Check failures

---

The software image on the FTP server can be checked for compatibility using the CHK-SYS-UPGRD command. If the compatibility check fails, an autonomous event message is raised. The message indicates why the check has failed. Listed below are some examples.

### CHK-SYS-UPGRD failure when file is not found on FTP server

```
BTI7000 2008-04-29 08:46:47
A 17538 REPT EVT EQPT
  "SCP-1-5:SYSCHKFAIL,,2008-04-29,08-46-46,,,,,:Check Upgrade Failure.
Requested operation failed. No FTP file found.,,,:,"
;
```

### CHK-SYS-UPGRD failure when FTP server is not found

```
BTI7000 2008-04-29 08:49:16
A 17539 REPT EVT EQPT
  "SCP-1-5:SYSCHKFAIL,,2008-04-29,08-49-15,,,,,:Check Upgrade Failure.
Requested operation failed. FTP Server not available.,,,:,"
;
```

### CHK-SYS-UPGRD failure when inventory does not match load

```
BTI7000 2008-04-30 08:47:26
A 17762 REPT EVT EQPT
  "SCP-1-5:SYSCHKFAIL,,2008-04-30,08-47-25,,,,,:Check Upgrade Failure.
Inventory does not match Load provided.,,,:,"
;
```

### CHK-SYS-UPGRD failure when an invalid manifest file is found

```
BTI7000 2008-04-30 08:55:34
A 17763 REPT EVT EQPT
  "SCP-1-5:SYSCHKFAIL,,2008-04-30,08-55-33,,,,,:Check Upgrade Failure.
Invalid Manifest file found.,,,:,"
```

### CHK-SYS-UPGRD failure when an invalid username or password is found

```
BTI7000 06-12-19 10:55:45
A 529 REPT EVT EQPT
  "SCP-1-5:SYSCHKFAIL,,12-19,10-55-44,,,,:\"Check Upgrade Failure. Invalid
username or password.\",,,:,"
;
```



**CHK-SYS-UPGRD failure when the wrong FTP server is accessed**

```
BTI7000 06-12-19 10:42:01
A 516 REPT EVT EQPT
"SCP-1-5:SYSCHKFAIL,,12-19,10-42-00,,,,,\\"Check Upgrade Failure. Requested
operation failed. Internal system fault.\",,,:,"
;
```

**CHK-SYS-UPGRD failure when the wrong path is specified**

```
BTI7000 06-12-19 10:58:20
A 536 REPT EVT EQPT
"SCP-1-5:SYSLOADFAIL,,12-19,10-58-19,,,,,\\"Software Load Failed. File does
not exists.\",,,:,"
;
```

**CHK-SYS-UPGRD failure when another load or CHK-SYS-UPGRD was already started**

```
BTI7000 06-12-19 10:50:09
A 524 REPT EVT EQPT
"SCP-1-5:SYSCHKFAIL,,12-19,10-50-08,,,,,\\"Check Upgrade Failure. Invalid
Upgrade Sequence.\",,,:,"
;
```

**CHK-SYS-UPGRD failure when gateway is not set and IP address is outside the IP-NMS subnet**

```
BTI7000 06-12-19 13:37:28
A 9 REPT EVT EQPT
"SCP-1-5:SYSCHKFAIL,,12-19,13-37-26,,,,,\\"Check Upgrade Failure. No route
to host.\",,,:,"
;
```

**CHK-SYS-UPGRD failure when you do not have read permission on the FTP server**

```
BTI7000 06-12-19 13:52:37
A 12 REPT EVT EQPT
"SCP-1-5:SYSCHKFAIL,,12-19,13-52-36,,,,,\\"Check Upgrade Failure.
Permission denied.\",,,:,"
;
```

## 5.2 Load failures

---

When the LOAD-SYS-UPGRD command is issued, the software image on the FTP server transfers to the BTI 7000 Series . If the transfer is unsuccessful, the system generates an autonomous event message or an event response message that indicates why the load has failed. Listed below are some examples.

### LOAD-SYS-UPGRD failure when a handshake failure to the FTP server occurs

```
BTI7000 2003-04-29 08:58:26
A 17364 REPT EVT EQPT
  "SCP-1-5:SYSLOADFAIL,,2003-04-29,08-58-25,,,,,\\"Software Load Failed.
\\"Requested operation failed. FTP Not Defined.,,,,,";
```

### LOAD-SYS-UPGRD failure when file is not found on FTP server

```
BTI7000 2003-04-29 08:58:26
A 17544 REPT EVT EQPT
  "SCP-1-5:SYSLOADFAIL,,2003-04-29,08-58-25,,,,,\\"Software Load Failed.
\\"Requested operation failed. No FTP file found.,,,,,";
```

### LOAD-SYS-UPGRD failure when FTP server is not found

```
BTI7000 2003-04-29 08:59:04
A 17545 REPT EVT EQPT
  "SCP-1-5:SYSLOADFAIL,,2003-04-29,08-59-03,,,,,\\"Software Load Failed.
\\"Requested operation failed. FTP Server not available.,,,,,"
;
```

LOAD-SYS-UPGRD failure when an invalid FTP server IP address is specified

```
BTI7000 06-12-19 11:09:16
M 100 DENY
  IDNV
  /* Data not valid. Invalid Address. Error #2819. */
;
```

LOAD-SYS-UPGRD failure when valid but wrong IP address is specified and there is no answer from the remote node

```
BTI7000 06-12-19 11:04:02
A 537 REPT EVT EQPT
  "SCP-1-5:SYSLOADFAIL,,12-19,11-04-01,,,,,\\"Software Load Failed.
Connection to FTP server timed out.\",,,,,";
```

### LOAD-SYS-UPGRD failure when there is no FTP server running on the designated IP address

```
BTI7000 06-12-19 11:07:14
A 540 REPT EVT EQPT
  "SCP-1-5:SYSCHKFAIL,,12-19,11-07-13,,,,,\\"Check Upgrade Failure. FTP
server not available, connection refused.\",,,,,";
```

## LOAD-SYS-UPGRD failure when trying to load while a load is in progress

```
BTI7000 2003-04-29 09:00:35
A 17546 REPT EVT EQPT
"SCP-1-5:SYSLOADFAIL,,2003-04-29,09-00-34,,,,,\\"Software Load Failed.
\\"Requested operation failed. Upgrade Load Process Already Started.,,,:,";
```

## LOAD-SYS-UPGRD failure when a bad load is found

```
BTI7000 2003-04-30 09:00:20
A 17766 REPT EVT EQPT
"SCP-1-5:SYSLOADFAIL,,2003-04-30,09-00-19,,,,,\\"Software Load Failed.
\\"Bad Load found.,,,:,";
```

Corrective action - The load has failed its checksum test. This indicates that there was a problem copying the load from the FTP server to the system. Repeat the LOAD-SYS-UPGRD step. If you are using a management network and the problem persists connect to the system directly with a laptop or PC and user proNX 900 to load the file from the laptop or PC directly onto the system.

## LOAD-SYS-UPGRD failure when the invoke process is in progress

```
BTI7000 2003-04-30 09:09:06
A 17771 REPT EVT EQPT
"SCP-1-5:SYSLOADFAIL,,2003-04-30,09-09-05,,,,,\\"Software Load Failed.
\\"Requested operation failed. Upgrade Load Process Already
Started.,,,:,";
```

## LOAD-SYS-UPGRD failure when the inactive software bank has failed.

```
BTI7000 05-04-13 19:22:24
A 4 REPT EVT EQPT
"SCP-1-5:SYSLOADFAIL,,04-13,19-22-23,,,,,\\"Software Load Failed. Unmapped
error code.\",,,:,";
```

<b>Note</b>	See the <i>Alarm and Troubleshooting Guide</i> for information about replacing the SCP.
-------------	---

## LOAD-SYS-UPGRD failure when a circuit pack is unknown or the circuit pack has corrupted inventory data

```
BTI7000 06-12-19 11:29:45
A 547 REPT EVT EQPT
"SCP-1-5:SYSLOADFAIL,,12-19,11-29-44,,,,,\\"Software Load Failed. Inventory
does not match Load provided.\",,,:,";
```

## 5.3 Invoke failure

---

When the INVK-SYS-UPGRD command is issued and the invoke process is unsuccessful, the system generates an event response message that indicates why the invoke has failed. Listed below are some examples.

### TL1 Invoke failure messages

When the INVK-SYS-UPGRD command is issued, the software image on the inactive memory bank becomes active. If the invoke process is unsuccessful, the system generates an event response message that indicates why the invoke has failed. Listed below are some examples.

#### INVK-SYS-UPGRD failure when alarms are present on the system

```
BTI7000 2008-04-29 09:03:18
M 100 DENY
SNVS
/* Not in Valid State. System must be alarm-free. */
;
```

#### INVK-SYS-UPGRD failure when the release number is already active

```
BTI7000 2008-04-29 09:03:46
M 100 DENY
SROF
/* Upgrade to Requested Release not possible. */
;
```

#### INVK-SYS-UPGRD failure when the system upgrade has already been invoked

```
BTI7000 2008-04-30 09:08:19
M 100 DENY
SROF
/* Requested operation failed. Command not allowed while upgrade invoke
stage is in progress. */
;
or
```

```
BTI7000 2008-02-31 19:03:44
M 100 DENY
SROF
/* Requested Operation Failed. Upgrade In Progress. */
;
```

### 5.3.1 Recommended actions for invoke failures

**Step 1** Check for file transfer problems:

If the error message `Database Load Failed` is returned, check to see if there has been a problem during the file transfer process. Check that:

- the filename is correct
- the correct IP address is entered
- the FTP server is running
- the gateway on the FTP server is correct
- the FTP server can communicate with the BTI 7000 Series by pinging the BTI 7000 Series from the FTP server
- the path is set correctly. Some UNIX FTP servers require the user to specify the complete directory path of the file. Also, check that UNIX permissions are set to global read-write access.
- there was no network interruption during the system upgrade or database restore

If no apparent reason can be found for the file transfer failure, contact your next level of support.

**Step 2** Check the Alarms to see if any alarms are present. See the applicable alarm clearing procedure for instructions to clear the alarm.**Step 3** If an alarm is present and you want to proceed with the Invoke, check to see if the **Ignore Alarms** option in the Software Upgrade window, is enabled.**Step 4** If you are using TL1, INVK-SYS-UPGRD command may be blocked.

The following conditions cause the INVK-SYS-UPGRD command to be blocked:

- If alarms are present in the system, the INVK-SYS-UPGRD command is blocked. Clear the alarms that are present and then proceed with the INVK-SYS-UPGRD command.
- If the system has already upgraded to the new product release, the INVK-SYS-UPGRD command is blocked. You cannot upgrade the system to the product release that the system is currently running.
- If the INVK-SYS-UPGRD command has already been issued, or if an upgrade is already in progress, the INVK-SYS-UPGRD command is blocked. A subsequent INVK-SYS-UPGRD command cannot be issued before the upgrade is completed.
- If there is an attempt to downgrade the system software, the INVK-SYS-UPGRD command is blocked. Contact your next level of support if you need assistance.

For the scenarios described above, wait for any ongoing commands to complete and then determine where you are in respect to the current system status.

If you cannot determine what state the system is in, contact your next level of support.

## 5.4 Commit failure

---

When the CMMT-SYS-UPGRD command and the commit is unsuccessful, the system generates an event response message that indicates why the load has failed. Listed below is an example.

### **CMMT-SYS-UPGRD failure when the software has not been loaded or invoked**

```
.BTI 7000 Series 2008-04-30 08:52:39
M 100 DENY
  SROF
  /* Requested operation failed. Upgrade Process Not Started. */
;
```

Ensure that you have invoked the system upgrade before issuing the CMMT-SYS-UPGRD command.

---

## 5.5 Cancel failure

---

When the CANC-SYS-UPGRD command is issued and the transfer is unsuccessful, the system generates an event response message that indicates why the cancel has failed. Listed below are some examples.

### CANC-SYS-UPGRD failure when an invoke has not been started

```
BTI7000 2007-12-31 19:02:05
M 100 DENY
SROF
/* Requested operation failed. Upgrade Process Not Started. */
;
```

### CANC-SYS-UPGRD failure when an invoke is in progress

```
BTI7000 2007-12-31 09:27:38
M 100 DENY
SROF
/* Requested operation failed. Command not allowed while upgrade invoke
stage is in progress. */
;
```

### CANC-SYS-UPGRD failure after upgrade has already been cancelled

```
BTI7000 2007-12-31 19:01:34
M 100 DENY
SROF
/* Requested operation failed. Upgrade Process Not Started. */
;
```

#### 5.5.1 Recommended actions for cancel failures

The following conditions can cause the CANC-SYS-UPGRD command to be blocked:

- If the INVK-SYS-UPGRD command has not been issued, the CANC-SYS-UPGRD command is blocked. Issue the INVK-SYS-UPGRD command and wait for the invoke process to complete before issuing the CANC-SYS-UPGRD command.
- If an invoke operation is in progress, the CANC-SYS-UPGRD command is blocked. Wait for the invoke process to complete and then issue the CANC-SYS-UPGRD command.
- If the CANC-SYS-UPGRD command has already been issued, the CANC-SYS-UPGRD command is blocked. There is no need to issue the CANC-SYS-UPGRD command again.

If you are unable to cancel the upgrade or determine what state the system is in, contact your next level of support.

## 5.6 Provisioning failure

---

### ENT-EQPT failure when a system software upgrade is in progress

When the ENT-EQPT command is issued during a system software upgrade, the system attempts to enter new provisioning parameters. With the a system software upgrade in progress, the system generates an event response message that indicates that the command is blocked. Listed below is an example.

```
BTI7000 2003-04-30 09:10:19
M 100 DENY
SROF
/* Command blocked due to current system access level. */
;
```

Wait for the a system software upgrade to complete before issuing a provisioning command.



## 5.7 Module upgrade failure

---

The BTI 7000 Series confirms when all modules have been successfully upgraded to a new software release. If a module fails to upgrade properly, the system raises a Circuit Pack Upgrade Failure alarm (PACKUPGRDFAIL). This alarm indicates which module failed to upgrade.

- |             |  |
|-------------|--|
| <b>Note</b> | <ul style="list-style-type: none"><li>• The module upgrade failure is not a service affecting condition. The module continues to run its original software and continues to process optical signals properly.</li><li>• While the PACKUPGRDFAIL alarm is active, both alarm reporting and performance monitoring data collection are disabled.</li></ul> |
|-------------|--|

If a module upgrade fails, contact BTI Support.

## 5.8 Database recovery failure

---

When an SCP is replaced, the new SCP automatically acquires the provisioning database from an active module in the system. This simplifies the replacement process because a manual database restore operation is not required.

The BTI 7000 Series confirms when the SCP has successfully recovered the database from the system. If the database is not recovered, a Database Recovery Failure alarm (DBRECVRYFAIL) is raised. In this situation, the database must be restored manually from a remote FTP server. For information about clearing this alarm, see the *Alarm and Troubleshooting Guide*.

# Appendix A: Upgrading the network element from a BTI 2060 SCP to a BTI 7060 SCP

---

Use this procedure to upgrade a network element (NE) from a BTI 2060 SCP (BP1A20BA) to a BTI 7060 SCP (BT7A20CA) running Release 7.2.x. To upgrade your system to a release later than 7.2.x, complete this procedure first, and then use the Upgrade Guide for the later release to complete the upgrade.

## What you need

- Access to the desired versions of BTI 7000 Series software
- Slot-head or Phillips screwdriver
- Electrostatic discharge (ESD) wrist strap



### 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).

## Prerequisites

- See [2.1, “Upgrade task flow”](#).

**Important** Review the "Troubleshooting" chapter of the *Solutions Guide* for each module type installed on the system for information about additional procedures that might be required during or after the system software upgrade.

- Perform a database backup. See [2.4, “Perform a database backup”](#). If you cannot perform a database backup because of an SCP failure, then locate the latest backup on the FTP database backup server.

- You must have a laptop or PC with an FTP server running on it.
- There are no CONTCOM alarms on the system.

### **Recommendations**

- The state of the system is In Service.
- Remove or install modules during the upgrade process only if you are instructed to do so.

## A.1 Upgrade the NE from a BTI 2060 SCP (BP1A20BA) running Release 6.2 to a BTI 7060 SCP (BT7A20CA) running Release 7.2.x

Use this procedure to upgrade a NE from a BTI 2060 SCP (BP1A20BA) running Release 6.2 to a BTI 7060 SCP (BT7A20CA) running Release 7.2.x

Follow these steps to replace the SCP, and then to load, invoke, and commit the system software upgrade to 7.2.x using TL1:

**Step 1** Replace the BTI 2060 SCP (BP1A20BA) with a BTI 7060 SCP (BT7A20CA). Ensure that all cables are replaced in the correct locations.

The BTI 7060 SCP recovers the IP address of the 2060 SCP, resulting in a mismatch of the MAC address. Therefore there is a short delay until the IP address is available.

Once the SCP has finished restarting, continue at the next step.

**Step 2** Log on to the system using TL1 using the existing IP address and credentials.  
Once you are logged in the RELNUMMEA (Release Number Mismatch) alarm is raised.

**Step 3** Verify that the software load to which you want to upgrade is stored in both software banks.

```
RTRV-SYS-RELNUM:[TID]::<CTAG>;
```

For example,

```
RTRV-SYS-RELNUM:BTI7000::100;
BTI7000 2008-01-21 14:22:30
M 100 COMPLD
"ACTIVE=7.2.1 C003, INACTIVE=7.2.1 C003,"
;
```

If the software load to which you want to upgrade is not in both banks, contact your BTI support representative. Do not proceed further with this procedure. If the software load to which you want to upgrade is in both banks, continue at the next step.

**Step 4** Enter the following at the TL1 command line interface to invoke the system software upgrade:

```
INVK-SYS-UPGRD:[TID]::<CTAG>::RELNUM=<relnum>,[CHKALM=<chkalm>];
```

where

<RELNUM> is the release number of the system software

<CHKALM> is N because there are standing alarms

For example,

```
INVK-SYS-UPGRD:BTI7000::100::RELNUM=7_2_1_C003,CHKALM=N;
```

- The SYSUPGRDPROG (System Software Upgrade in Progress) alarm is raised, and its severity is Major.
- The SCP is loaded with the upgraded system software.

Connectivity with the NE is lost.

**Step 5** When the red Fail LED on the SCP turns off, log on to the system.

**Note** It can take several minutes to connect to the system.

Once you are logged in, note the following alarms:

- the RELNUMMEA (Release Number Mismatch) alarm is cleared
- the REPLUNITMEA (Circuit pack mismatch for the SCP) alarm is raised
- the SYSUPGRDPROG (System Software Upgrade in Progress) alarm is Major or Minor. If the alarm is Major, it means that not all of the modules have finished upgrading. Once all of the modules have finished upgrading, the alarm changes to Minor. Do not proceed to the next step until the alarm has changed to Minor.

**Step 6** Enter the following at the TL1 command line interface to commit the upgrade:

```
CMMT-SYS-UPGRD:[TID]::CTAG::;
```

For example,

```
CMMT-SYS-UPGRD:BTI7000::100::;
```

The SYSUPGRDPROG alarm clears. Optionally, you can use the RTRV-SYS-RELNUM command to verify that the desired release of the system software is stored in the active software bank.

For example,

```
RTRV-SYS-RELNUM:BTI7000::100;
BTI7000 2008-01-21 16:22:30
M 100 COMPLD
"ACTIVE=7.2.1 C003, INACTIVE=7.2.1 C003,"
;
```

**Note** If the commit operation fails, see [5.4, “Commit failure”](#) for information.

**Step 7** Clear the REPLUNITMEA (Circuit pack mismatch for the SCP) alarm by editing the PEC for the SCP. Enter the following command:

```
ED-EQPT:[TID]:<aid>:[CTAG]:[:<type>][:ID=<id>],[C1=<custom1>],
[C2=<custom2>],[C3=<custom3>],[SHCONF=<shconf>][:<pst>]
[,<sst>]];
```

For example,

```
ED-EQPT:BTI7000:SCP-1-5:100:BT7A20CA::;
```

You have successfully completed this procedure.

## Appendix B: SCP replacement procedures

---

When an SCP is replaced the system detects the new SCP and determines if the software on the new SCP matches the software on the system. If the SCP has the same release as the system, then after the SCP boots up, the system automatically restores the provisioning database to the SCP module from an active module in the shelf, clears all related alarms, and places the SCP module in service. No further action is required by the operator. However, if the SCP software does not match the system software, then there are several options, which are explained in the following procedures:

- [B.1, “Upgrading your system that is running Release 11.1, 11.2, 11.3, 12.1, 12.2, 13.1, or 13.2 by replacing the SCP with one that has Release 13.5 software”](#) - Use this procedure to upgrade your system by replacing the SCP with one that has a newer software release.
- [B.2, “Replacing an SCP with one that has a different software release than the system”](#) - Use this procedure to replace the SCP and then bring the SCP to the same release of software as the system.

## B.1 Upgrading your system that is running Release 11.1, 11.2, 11.3, 12.1, 12.2, 13.1, or 13.2 by replacing the SCP with one that has Release 13.5 software

Use this procedure to upgrade your system that is running Release 11.1, 11.2, 11.3, 12.1, 12.2, 13.1, or 13.2 by replacing the SCP with one that has Release 13.5 software.

**Important** The new SCP with must have Release 13.5 in both software banks.

### Connectivity Requirements

We recommend that you perform this upgrade/downgrade procedure using the TL1 and using the Craft LAN port on the SCP.

### Changing the IP address of your computer

This procedure requires that you modify the IP address of your computer twice:

- When you re-establish your TL1 connection to the BTI 7000 Series.
- When you log into the BTI 7000 Series.

Change the IP address on your computer to be on the same subnet as the default Craft LAN port BTI 7000 Series IP address. Depending on the operating system used by your computer, you may need to reboot your computer before performing the upgrade. This occurs because IP address information for older operating systems do not take effect until the computer is rebooted.

**Step 1** Invoke the system upgrade. Enter the following TL1 command:

```
INVK-SYS-UPGRD:[TID]::CTAG::[RELNUM=<relnum>],
[CHKALM=<chkalm>];
```

where:

*relnum* is the version number of the upgrade software.

*chkalm* is either Y or N (Y is the default).

**Note** The upgrade is not invoked if there are alarms on the system unless the *chkalm* parameter is set to N. Additionally, any expansion shelf that has an Expansion Shelf Mismatch (REPLUNITMEA) alarm does not upgrade and no error message is presented.

### Example

```
INVK-SYS-UPGRD:BTI 7000 Series::100::RELNUM=Release 13.5.x,CHKALM=N;
```

where:

*x* represents a numeral based on the software that has been ordered

### Response

The system checks the image for integrity, transfers the load to the modules, and reboots the modules starting with the SCP. During this process, a System Software in Progress (SYSUPGRDPG) alarm is raised. The alarm's severity changes to major while the



SCP is being upgraded, and then returns to minor when the upgrade completes. Also during this process, the system displays autonomous messages completes. Also during this process, the system displays autonomous messages showing the progress of the upgrade. Depending on the system configuration, the autonomous messages will change from system to system.

- Note**
- During the reboot process, the red fail LED on modules can be on temporarily while the active green LED is on.
  - If the command does not complete successfully, see [Chapter 5, “Troubleshooting”](#).
  - It will take several minutes for the various modules to be loaded with the upgrade software and then re-initialized. Progress is displayed through TL1 messages.

## Step 2 Log into the BTI 7000 Series

Once the system upgrade has completed, all system provisioning data is restored. Connect to the system using the originally provisioned userid, password, and IP addresses.

### Craft LAN Port

If you are using the Craft LAN port, you may need to change the IP address parameters on your computer or laptop to the same subnet as the originally provisioned Craft LAN port on the NE.

- Note** If you have already changed the LAN IP address on your computer, you do not need to change anything

### Craft Serial Port

If you are using the Craft serial port and the TL1 session is not running, you may need to change, on your computer or laptop, the serial parameters set up to match the originally provisioned serial port parameters on the BTI 7000 Series.

You are now ready to log on to the BTI 7000 Series. Enter the following TL1 command:

```
ACT-USER:[TID]:[<userid>]:CTAG::[<password>;
```

### Example

```
ACT-USER:BTI 7000 Series:admin:100::*****;
```

## Step 3 Check the status of the system upgrade process. Enter the following TL1 command:

```
RTRV-ALM-ALL:[TID]::CTAG::,,,,;
```

### Example

```
RTRV-ALM-ALL:BTI 7000 Series::100::,,,,;
```

Check for a SYSUPGRDPROG alarm. If there is no SYSUPGRDPROG alarm, then the upgrade is complete. If the SYSUPGRDPROG alarm is active, then the system is still upgrading. Wait for the alarm to clear.

**Note** The RELNUMMEA (Release Number Mismatch) alarm may be masked by the REPLUNITMEA (Shelf Mismatch) alarm. It is recommended that you view all outstanding conditions by issuing the `RTRV-COND-ALL` TL1 command.

This procedure is complete.

## B.2 Replacing an SCP with one that has a different software release than the system

Use this procedure to replace an SCP that is running a different software version than is currently loaded on the BTI 7000 Series, and bring the new SCP to the same software release as the system. When an SCP in the system is replaced with an SCP running a different version of the system software, a Release Number Mismatch (RELNUMMEA) or Shelf Unknown (REPLUNITUNK) alarm or condition is raised after the SCP boots up. In this situation, the system/SCP takes no further action and waits for user intervention. The SCP waits for the system provisioning data to be downloaded after the upgrade.

### Connectivity Requirements

**Important** To avoid possible IP address conflicts, disconnect the NE from the management network before performing this procedure.

We recommend that you perform this upgrade/downgrade procedure using the TL1 and using the Craft LAN port on the SCP.

### Changing the IP address of your computer

This procedure requires that you modify the IP address of your computer twice:

- When you re-establish your TL1 connection to the BTI 7000 Series.
- When you log into the BTI 7000 Series.

Change the IP address on your computer to be on the same subnet as the default Craft LAN port BTI 7000 Series IP address. Depending on the operating system used by your computer, you may need to reboot your computer before performing the upgrade. This occurs because IP address information for older operating systems do not take effect until the computer is rebooted.

**Note** When performing this procedure, ensure that you have the files on hand for the version of software to which you are upgrading/downgrading the SCP.

**Step 1** Replace the current SCP with a new SCP module.

**Step 2** Re-establish your TL1 connection to the BTI 7000 Series.

When the SCP restarts, you are logged out of your TL1 session.

Before proceeding, your PC or laptop must be provisioned on the same subnet as the default Craft LAN port settings on the BTI 7000 Series.

Default Craft LAN Port Settings.

IP Address: 192.168.17.1

IP Mask: 255.255.255.0

Continue by logging into the BTI 7000 Series using the default Craft LAN settings.

**Step 3** Log in to the BTI 7000 Series.

**Step 4** Set up the FTP server.

The upgrade process uses the File Transfer Protocol (FTP) protocol to transfer the upgrade software image from a FTP server to the BTI 7000 Series.

The FTP server can run on a Windows, Solaris, or Linux operating system.

Prepare the FTP server as follows:

- 1 Insert the software CD with the software release that is active on the system into the CD-ROM drive of the FTP server.
- 2 Start the FTP application or daemon, if not started already.
- 3 Configure the FTP root directory to serve files from the CD-ROM. Alternatively, copy the files from the CD-ROM to the default FTP root directory. Do not remove, delete, or rename any of the files. Ensure that the directory and its files have global read-write access.
- 4 Confirm that the FTP server and the BTI 7000 Series have IP connectivity by pinging the BTI 7000 Series from the FTP server.

**Step 5** Load the software.

Load the software version to which you are upgrading by entering the following TL1 syntax. This step takes approximately two to four minutes to complete:

```
LOAD-SYS-UPGRD:[TID]::CTAG::IPADDR=<ipaddr>;
```

where:

*ipaddr* is the IP address where the upgrade software is located.

**Note** If the software upgrade file is stored in the root directory, you do not need to specify a path for the software upgrade file.

**Example**

```
LOAD-SYS-UPGRD:BTI7000::100::IPADDR=192.168.172.110;
BTI7000 2012-01-21 14:20:41
M 100 COMPLD
;
Netstender>
BTI7000 2012-01-21 14:22:10
A 7 REPT EVT EQPT
"SCP-1-5:SYSLOADPASS,,2012-01-21,14-22-09,,,,,:\"Software Load
Completed Successfully.\",,[/] [192.168.172.110] ,:,"
```

**Note** If the command does not complete successfully, the error message "Failed Check Software" is returned. See [Chapter 5, "Troubleshooting"](#).

**Step 6** Use the RTRV-ALM-ALL command and the RTRV-COND-ALL command to determine if there is a Release Number Mismatch (RELNUMMEA) or a Shelf Unknown (REPLUNITUNK) alarm or condition present.

- a) If the alarm or condition is Release Number Mismatch (RELNUMMEA),** then enter the following command:

```
INVK-SCP-RELNUM:[TID]::CTAG::[RELNUM=<relnum>],[CHKALM=<chkalm>];
```

where  
relnum is the release number of the upgrade software  
chkalm is either Y or N (Y is the default).

**Note** The SCP upgrade is not invoked if there are alarms on the system, unless the chkalm parameter is set to N..

### Example

```
INVK-SCP-RELNUM:OLS::100::RELNUM=10.2.x,CHKALM=n
```

where

x represents a numeral based on the software version.

**Note** The SCP Release Number Change in Progress (SCPCHGPROG) alarm is raised at this point in the upgrade process.

If the invoke fails, the system issues an error message. See the BTI 7000 Series Alarm and Troubleshooting Guide to resolve the error condition.

**b) If the alarm or condition is Shelf Unknown (REPLUNITUNK), then enter the following command:**

```
INVK-SYS-UPGRD:[TID]::<CTAG>::RELNUM=<relnum>,[CHKALM=<chkalm>];
```

where

<RELNUM> is the release number of the system software

<CHKALM> is Y or N

For example,

```
INVK-SYS-UPGRD:BTI7000::100::RELNUM=10.2,CHKALM=N;
```

After the SCP reboots, the system provisioning data is restored to the new SCP.

### Step 7 Log into the BTI 7000 Series

Once the system upgrade is completed, all TL1 sessions with the BTI 7000 Series end. You must reconnect to the system.

Log in to the BTI 7000 Series by entering the following TL1 syntax:

```
ACT-USER:[TID]:[<userid>]:CTAG::[<password>];
```

### Example

```
ACT-USER:BTI 7000 Series:admin:100::*****;
```

Check the alarms to confirm that there are no upgrade-related alarms present.

### Step 8 Reconnect the NE to the management network.

You have successfully completed this procedure.



## Appendix C: Downgrading to an earlier system software version

---

This section describes how to downgrade to an earlier software version from the current software version that is running on your network. Downgrading deletes the database and all configuration is lost. This type of downgrade is not hitless. Manual intervention (e.g. reseating a card) may also be required.

<b>Note</b>	Downgrading is different than cancelling an upgrade. Cancelling an upgrade returns the system to the current software version from which you are performing an upgrade. For information on cancelling an upgrade refer to <a href="#">Chapter 3, “Cancelling a system software upgrade”</a> .
-------------	---

- [C.1, “Downgrading the system software using TL1”](#)

## C.1 Downgrading the system software using TL1

Use this procedure to downgrade the system software from the current software version to any earlier release, using TL1 commands.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

### Prerequisites

- You must be logged on to the system.
- There are no CONTCOM alarms on the system.
- Back up the database.

**Note** This procedure deletes the database and all NE configuration is lost. This type of downgrade is not hitless. Manual intervention (e.g. reseating a card) may also be required.

### Recommendations

- The state of the BTI 7000 Series system is In Service.
- Remove or install modules during the downgrade process only if you are instructed to do so.

**Important** The release numbers in the examples are for only example purposes to show the required information and may not match the release numbers you are managing. Be sure to use the appropriate information for the software versions you are managing.

### Downgrading the system software

Follow these steps to downgrade the system software using TL1.

**Important** This procedure deletes the database, and all provisioning on the NE is lost.

**Note** The BTI 7200 cannot be downgraded to a release earlier than 8.1.

**Step 1** If there are any expansion shelves connected to the main shelf, disconnect them all from the main shelf by unplugging the expansion shelf cables from the ports on the SCP. Label the cables before you unplug them so that you can plug them back into the correct ports later.

**Step 2** Enter the following at the TL1 command line interface to load the version of the system software to which you want to downgrade:

```
LOAD-SYS-UPGRD: [TID]::CTAG:::IPADDR=<IPADDR>;
```

where

<IPADDR> is the IP address where the system software is stored



For example,

```
LOAD-SYS-UPGRD:BTI7000::100:::IPADDR=112.23.45.62;
BTI7000 2008-01-21 14:20:41
M 100 COMPLD
;
BTI7000>
BTI7000 2008-01-21 14:22:10
A 7 REPT EVT EQPT
"SCP-1-5:SYSLOADPASS,,2008-01-21,14-22-09,,,,,:\"Software Load
Completed Successfully.\",,[/] [192.168.172.110] ,:,"
;
```

The system software takes several minutes to load.

**Note** If the check operations fails, see 5.1, “Check failures” for information.

**Step 3** Enter the following at the TL1 command line to verify that an earlier version of the system software is stored in the inactive software bank and Release 13.5 is stored in the active software bank:

```
RTRV-SYS-RELNUM:[TID]::<CTAG>;
```

For example,

```
RTRV-SYS-RELNUM:BTI7000::100;
BTI7000 2014-01-21 14:22:30
M 100 COMPLD
"ACTIVE=Release 13.5.0 ,INACTIVE=Release 12.1.0,"
;
```

**Step 4** Enter the following at the TL1 command line interface to remove the database from the system.

```
INVK-DB-DLT:[TID]::[CTAG]:::[CHKALM=<chkalm>];
```

where

<CHKALM> is Y or N

For example,

```
INVK-DB-DLT:BTI7000::100:::CHKALM=N;
```

**Note** Deleting a database restores the factory-default communications settings; therefore, connectivity is lost. After the database delete operation is complete, reconnect to the NE through the local Craft port using the factory-default communications settings.

**Note** Following a database delete operation, all proNX 900 sessions must be terminated and then restarted.

**Step 5** Enter the following at the TL1 command line interface to commit the database deletion.

```
CMMT-DB-DLT:[TID]::[CTAG];
```

For example,

```
CMMT-DB-DLT:BTI7000::100;
```

All of the modules on the shelf re-initialize, except for the SCP. Once all of the modules are finished re-initializing (which may take several minutes), continue at the next step.

**Step 6** Log back into the system. Reconnect via the local Craft port using the factory-default communications settings.

**Step 7** Enter the following at the TL1 command line interface to invoke the system software downgrade:

```
INVK-SYS-UPGRD:[TID]::CTAG::[RELNUM=<RELNUM>],[CHKALM=<CHKALM>];
```

where

<RELNUM> is the release number of the system software

<CHKALM> is Y or N

For example,

```
INVK-SYS-UPGRD:BTI7000::100::RELNUM=11.3.0,CHKALM=N;
```

- The SYSUPGRDPROG (System Software Upgrade in Progress) alarm is raised, and its severity is Minor.
- The modules in the system are loaded with the upgraded system software. The alarm severity changes to Major, and the system then restarts, starting with the SCP and followed by the modules, and then the TL1 session ends.

<b>Important</b>	The amount of time that the invoke operation takes to complete depends on the configuration of the node. For example, for a full four-shelf system, the invoke operation may take up to one hour to complete.
------------------	---

<b>Note</b>	During reinitialization, the red Fail LED on each module may light temporarily while the green Active LED is lit.
-------------	---

**Step 8** When the red Fail LED on the SCP turns off, log on to the system.

**Step 9** Enter the following at the TL1 command line interface to check the severity of the SYSUPGRDPROG alarm:

```
RTRV-ALM-ALL:[TID]::CTAG::,,,,,;
```

For example,

```
RTRV-ALM-ALL:BTI7000::100::,,,,,;
```

- If the severity of the SYSUPGRDPROG alarm is MJ (Major), the system downgrade is still in progress. Use the RTRV-ALM-ALL command to check the severity of the SYSUPGRDPROG alarm until the severity changes to MN (Minor), which indicates that the system downgrade is complete, and then proceed to the next step.

- If the severity of the SYSUPGRDPROG alarm is MN (Minor), the system downgrade is complete. Proceed to the next step.

**Note** If the invoke operation fails, see 5.3, “[Invoke failure](#)” for information.

**Step 10** Enter the following at the TL1 command line interface to verify that the earlier version of the system software is stored in the active software bank:

```
RTRV-NETYPE:[TID]::CTAG;
```

For example,

```
RTRV-NETYPE:BTI7000::100;
BTI7000 2014-01-21 15:20:31
M 100 COMPLD
BTI7000,BTI 7060,WDM,11.3.0
;
```

**Step 11** Enter the following at the TL1 command line interface to commit the downgrade:

```
CMMT-SYS-UPGRD:[TID]::CTAG::;
```

For example,

```
CMMT-SYS-UPGRD:BTI7000::100::;
```

**Note** If the commit operation fails, see 5.4, “[Commit failure](#)” for information.

The SYSUPGRDPROG alarm clears. Optionally, you can use the RTRV-SYS-RELNUM command to verify that the earlier version of the system software is stored in the active software bank and that Release 13.5 is stored in the inactive software bank.

For example,

```
RTRV-SYS-RELNUM:BTI7000::100;
BTI7000 2014-01-21 16:22:30
M 100 COMPLD
"ACTIVE=Release 12.1.0,INACTIVE=Release 13.5.0"
;
```

**Step 12** Power-cycle all modules on all of the expansion shelves for this main shelf by either unplugging all of the modules, and then plugging them all back in, or by turning the power to each of the expansion shelves off and back on again at the power distribution panel.

**Step 13** Reconnect the expansion shelves to the main shelf. Perform this step for each expansion shelf starting with 11, then 21, and finally 31.

- a) Plug the expansion shelf cable to its port on the SCP.
- b) Wait for the expansion shelf and its modules to re-initialize.

**Note** During re-initialization, the red Fail LED on each module may light temporarily, while the green Active LED is lit.

- c) Use the command RTRV-EQPT to check that the modules are no longer in software download state (SWDL). Once all of the modules on the expansion shelf are in a state other than SWDL, you can reconnect the next expansion shelf. For example:

```
RTRV-EQPT:BTI7000::100::;

BTI7000 04-02-19 10:43:56
M 100 COMPLD
BTI7000 10-09-30 09:21:39
M 100 COMPLD
"MS-1:BP1A5021::IS-NR, "
"SCP-1-5:BT7A20CA::IS-NR, "
"WR-1-6:BP1A42AA::IS-NR, "
"ES-11:BP1A5021::IS-NR, "
"MXP-11-1:BT7A48AA::IS-NR, "
"ES-21:BT7A51AA::IS-NR, "
"TPR-21-17:BT7A49AB::IS-NR, "
;
```

You have successfully completed this procedure.





*Part Number:*  
*Document Version:*  
*Published:*  
*Type:*

*BT7A72BA*  
*01*  
*March 2017*  
*STANDARD*

***product release 13.5***