



## PRODUCT DOCUMENTATION

### *BTI 7000 Series Operations Solutions Guide*

**Part Number:** BT7A73FA  
**Document Version:** 01  
**Published:** March 2017  
**Type:** STANDARD

***product release 13.5***



# Contents

---

|  |            |
|--|------------|
| <b>Preface</b>   | <b>vi</b>  |
| <b>1.0 Overview of components and provisioning</b>                             | <b>1-1</b> |
| 1.1 Organization of components .....   | 1-2        |
| 1.2 Provisioning methods .....   | 1-3        |
| 1.2.1 Auto provisioning .....  | 1-3        |
| 1.2.2 Pre-provisioning .....   | 1-4        |
| 1.3 Designating names and IDs to system components .....                       | 1-6        |
| <b>2.0 Site and system provisioning</b>  | <b>2-1</b> |
| 2.1 Provisioning site information .....  | 2-2        |
| 2.1.1 Editing the network element, site, and time zone .....                   | 2-2        |
| 2.1.2 Setting the system identification code .....                             | 2-2        |
| 2.1.3 Retrieving the network element, site, time zone, and uptime .....        | 2-2        |
| 2.1.4 Retrieving the vendor, model, NE type and software version .....         | 2-3        |
| 2.2 Provisioning Network Time Protocol (NTP) .....                             | 2-4        |
| 2.2.1 Specifying an NTP server .....   | 2-7        |
| 2.2.2 Specifying NTP poll time .....   | 2-7        |
| 2.2.3 Retrieving associated NTP servers .....                                  | 2-7        |
| 2.2.4 Retrieving NTP client servers .....                                      | 2-8        |
| 2.2.5 Deleting associated NTP servers .....                                    | 2-8        |
| 2.3 Provisioning the date and time on the system .....                         | 2-9        |
| 2.3.1 Editing the date and time .....  | 2-9        |
| 2.3.2 Editing the date and time during a daylight-saving-time transition ..... | 2-9        |
| 2.3.3 Retrieving the system identifier, date, and time .....                   | 2-10       |
| 2.4 Provisioning IP address parameters .....                                   | 2-11       |
| 2.4.1 Changing the default IP address and mask .....                           | 2-11       |

|  |      |
|--|------|
| 2.4.2 Changing the default gateway .....             | 2-11 |
| 2.4.3 Editing the IP address .....                   | 2-12 |
| 2.4.4 Retrieving the IP address .....                | 2-12 |
| 2.4.5 Managing ARP .....                             | 2-13 |
| 2.5 Craft serial interface parameters .....          | 2-14 |
| 2.5.1 Editing craft serial port information .....    | 2-14 |
| 2.5.2 Retrieving craft serial port information ..... | 2-14 |
| 2.6 Filler pack and filler faceplate detection ..... | 2-16 |
| 2.6.1 Setting the FPDTECT option .....               | 2-18 |
| 2.7 Center support detection .....                   | 2-19 |

---

### **3.0 Expansion shelf provisioning rules and configuration** **3-1**

|  |     |
|--|-----|
| 3.1 Expansion shelf provisioning rules .....     | 3-2 |
| 3.2 Configuring expansion shelves .....          | 3-3 |
| 3.3 Repurposing expansion shelves .....          | 3-5 |
| 3.4 Expansion shelf command line interface ..... | 3-6 |

---

### **4.0 Equipment provisioning** **4-1**

|   |      |
|---|------|
| 4.1 Entering new equipment .....          | 4-2  |
| 4.2 Editing equipment .....               | 4-3  |
| 4.3 Removing equipment from service ..... | 4-4  |
| 4.4 Restoring equipment to service .....  | 4-5  |
| 4.5 Retrieving equipment attributes ..... | 4-6  |
| 4.6 Retrieving equipment inventory .....  | 4-7  |
| 4.7 Deleting equipment .....              | 4-10 |

---

### **5.0 Performance Monitoring** **5-1**

|   |     |
|---|-----|
| 5.1 Understanding performance monitoring data ..... | 5-2 |
| 5.2 Bin validity qualifiers .....                   | 5-4 |
| 5.3 Retrieving performance monitoring data .....    | 5-5 |
| 5.4 Threshold crossing alerts .....                 | 5-6 |

---

### **6.0 Log management** **6-1**

|  |     |
|--|-----|
| 6.1 Log categories .....                       | 6-2 |
| 6.1.1 Retrieving logs .....                    | 6-3 |
| 6.1.2 Stopping log recording .....             | 6-4 |
| 6.1.3 Starting log recording .....             | 6-6 |
| 6.1.4 Initializing logs .....                  | 6-6 |
| 6.1.5 Retrieving log attributes .....          | 6-6 |
| 6.2 Security log .....                         | 6-7 |
| 6.2.1 Retrieving Security log attributes ..... | 6-7 |
| 6.2.2 Setting Security log attributes .....    | 6-7 |

---

|   |            |
|---|------------|
| <b>7.0 Security management</b>                            | <b>7-1</b> |
| 7.1 Security user profiles and authorization levels ..... | 7-2        |
| 7.2 User IDs and password identifiers .....               | 7-3        |
| 7.3 Creating a user profile .....                         | 7-4        |
| 7.4 Editing a user profile .....                          | 7-5        |
| 7.5 Changing your password .....                          | 7-6        |
| 7.6 Deleting a user profile .....                         | 7-7        |
| 7.7 Inhibiting a user profile .....                       | 7-8        |
| 7.8 Allowing a user profile .....                         | 7-9        |
| 7.9 Retrieving a list of active users .....               | 7-10       |
| 7.10 Retrieving your security credentials .....           | 7-11       |
| 7.11 Authentication .....                                 | 7-12       |
| 7.12 Provisioning authentication .....                    | 7-14       |
| <br>  |            |
| <b>8.0 Working with the database</b>                      | <b>8-1</b> |
| 8.1 About the database .....                              | 8-2        |
| 8.2 Impact of module replacement on the database .....    | 8-3        |
| 8.3 Recommendations when replacing modules .....          | 8-4        |
| 8.4 Database backup, restore, and delete .....            | 8-5        |
| 8.4.1 Backing up the database to an FTP server .....      | 8-5        |
| 8.4.2 Manual backup processes .....                       | 8-6        |
| 8.4.3 Restoring the database .....                        | 8-7        |
| 8.4.4 Automatic restore process .....                     | 8-10       |
| 8.4.5 Deleting the database .....                         | 8-11       |
| 8.5 Preconfigured SCP scenarios .....                     | 8-15       |
| 8.6 Replacing a failed SCP or module .....                | 8-16       |

---

# 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                     |
| 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 7000 Series common equipment (Continued)**

| <b>Equipment</b>   | <b>PEC</b>    |
|--|---------------|
| 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.



| <b>Agency</b>          | <b>Compliance information</b>  |
|------------------------|--|
| <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 TL1 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.    |
| <br><b>Caution</b> | Means reader be careful. Equipment damage or loss of data can result from your actions. |
| <br><b>Warning</b> | Means reader be careful. Harm to yourself or others can result from your actions.       |



| Convention  | Description  |
|---|--|
| <br><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 Overview of components and provisioning

---

- 1.1, “Organization of components”
- 1.2, “Provisioning methods”
- 1.3, “Designating names and IDs to system components”

## 1.1 Organization of components

---

The hardware and software in a BTI 7000 Series system are organized in a hierarchy, wherein a supporting-supported relationship exists between supporting equipment higher in the hierarchy and supported equipment lower in the hierarchy. This is reflected in the order that equipment can be added to and removed from the system, and removed from and restored to service.

For example, supporting equipment (higher in the hierarchy) must be provisioned before supported equipment (lower in the hierarchy) can be provisioned. Conversely, supported equipment must be removed from service or deleted before supporting equipment can be removed from service or deleted.

The following table lists the components in a system hierarchy.

| Component  | Description   |
|------------|---|
| Site       | A site is the physical location at which a system is located, and is identified through provisionable site elements, such as site identifier, site name, and time zone.   |
| System     | One or more systems can be deployed within a site. Each system must be uniquely identified with system-level parameters, such as network element (NE) name and system identifier (SID).   |
| Shelves    | A system consists of one main shelf and, optionally, additional expansion shelves.<br>Each shelf has a unique shelf number. For example, the main shelf is designated as 1 and expansion shelves are designated as 11, 21, or 31. |
| Modules    | Shelves contain slots for provisionable common equipment modules, optical modules, and service modules. For a full listing of these modules, see the <i>Common Equipment Installation Guide</i> .                                 |
| Facilities | Provisionable modules contain at least facility; for example, an amplifier on an Optical Amplifier module, or a port on a Transponder module.   |

## 1.2 Provisioning methods

Provisioning can be accomplished using TL1 commands or the proNX 900 Node Controller, or automatically through auto-provisioning.

For more information about using TL1 commands, see the *TL1 Reference Guide*. For more information about using the proNX 900 Node Controller, see the *proNX 900 Node Controller Online Help*.

This section covers the following topics:

- [1.2.1, “Auto provisioning”](#)
- [1.2.2, “Pre-provisioning”](#)

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.

### 1.2.1 Auto provisioning

Auto provisioning allows an unprovisioned hardware component, such as a module or port, to be automatically provisioned upon insertion of a module.

Auto provisioning is triggered by the insertion of a module or transceiver and is controlled by the AUTOP parameter, which is accessed through the ED-SYS command. The following table lists the settings that can be applied to the AUTOP parameter.

| AUTOP setting | Description  |
|---------------|--|
| AINS          | Both equipment and supporting facilities are provisioned with their state set to OOS-AU,AINS. The AINS system default timer is used.                 |
| IS            | The hardware component is auto provisioned, set to the in-service (IS) state, and all provisionable parameters are set to default their values.      |
| OOS           | The hardware component is auto provisioned, set to the out-of-service (OOS) state, and all provisionable parameters are set to default their values. |
| OFF           | The auto provisioning feature is turned off; no auto provisioning occurs.  |

## Restrictions

When a module is inserted into an unprovisioned slot, auto provisioning is initiated only if the module is not in one of the following conditions:

- Unknown
- Communications Failure
- Upgrade In Progress
- Upgrade Failed

When a module is present in an unprovisioned slot and then restarted by the INIT-SYS command, auto provisioning is not initiated. Also, auto provisioning is not initiated on slots that are already provisioned. As a result, supported facilities to be added to the equipment in that slot must be manually provisioned.

When auto provisioning fails, the equipment or facility is not provisioned and the "Auto-provisioning failure" event message is generated.

For more information about auto provisioning support, refer to the following documents:

- *Optical Amplifier and DCM Solutions Guide*
- *Multiplexing Solutions Guide*
- *Transponder Solutions Guide*
- *Muxponder Solutions Guide*

## 1.2.2 Pre-provisioning

Pre-provisioning refers to the system's ability to receive and process provisioning commands for equipment that is not present in the shelf. The provisioning sequence is similar to that for normal provisioning commands, with the exception that no action can be taken to activate the provisioning change.

The following components support pre-provisioning:

- Expansion shelves
- Optical Amplifier modules
- Dispersion Compensation modules



- Multiplexing modules
- Muxponder modules
- Transponder modules
- packetVX modules

The following table lists the equipment states that occur depending on the condition of the slot that has been provisioned.

**Table 1-1 Pre-provisioning equipment states**

| <b>Equipment State</b> | <b>Slot Condition</b>                       |
|------------------------|---|
| OOS-AU,AINS&MEA        | Module is not in provisioned slot.          |
| OOS-AU,AINS&UEQ        | Slot is empty.                              |
| IS-NR                  | Pre-provisioned module is inserted in slot. |

## 1.3 Designating names and IDs to system components

---

The following table lists the names and identifiers that must be provisioned and the system limits that pertain to each.

**Table 1-2 Names, identifiers, and custom field limits**

| <b>Names and Identifiers</b> | <b>Limits</b>                                   |
|------------------------------|---|
| Site Name                    | Up to 20 alphanumeric characters                |
| Site ID                      | Integer between 0 and 65535                     |
| NE Name                      | Up to 20 alphanumeric characters and a dash (-) |
| NE ID                        | Integer between 0 and 65535                     |
| Shelf ID                     | Up to 20 alphanumeric characters                |
| SCP ID                       | Up to 20 alphanumeric characters                |
| Module ID                    | Up to 20 alphanumeric characters                |
| ID1                          | Up to 32 alphanumeric characters                |
| ID2                          | Up to 32 alphanumeric characters                |
| Custom1                      | Up to 255 alphanumeric characters               |
| Custom2                      | Up to 255 alphanumeric characters               |
| Custom3                      | Up to 255 alphanumeric characters               |

## 2.0 Site and system provisioning

---

- 2.1, “Provisioning site information”
- 2.2, “Provisioning Network Time Protocol (NTP)”
- 2.3, “Provisioning the date and time on the system”
- 2.4, “Provisioning IP address parameters”
- 2.5, “Craft serial interface parameters”
- 2.6, “Filler pack and filler faceplate detection”
- 2.7, “Center support detection”

## 2.1 Provisioning site information

---

### 2.1.1 Editing the network element, site, and time zone



To edit system-wide provisioning information, use the following TL1 command:

```
ED-SYS:[TID]::[CTAG]:::[NEID=<neid>],[NENAME=<nename>],[GATEWAY=<gateway>],  
[SECGATEWAY=<secgateway>],[SITEID=<siteid>],[SITENAME=<sitename>],[TZ=<tz>],  
[AUTODST=<autodst>],[AUTOP=<autop>],[AINSTMR=<ainstmr>],[STP=<stp>],  
[CONTACT=<contact>;
```

#### Example command

```
ED-SYS:BTI7000::100::TZ=CANADAEASTERN,AUTODST=Y;
```

|             |  |
|-------------|--|
| <b>Note</b> | North American daylight-saving-time rules are automatically supported when AUTODST=Y is applied. |
|-------------|--|

### 2.1.2 Setting the system identification code



To set the system identification code (SID) for a network element, use the following TL1 command:

```
SET-SID:[TID]::[CTAG]:::<sid>;
```

#### Example command

```
SET-SID:BTI7000::100::BTI700023;
```

### 2.1.3 Retrieving the network element, site, time zone, and uptime



To retrieve the network element, site, time zone and uptime information, use the following TL1 command:

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

#### Example command and response

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

```
BTI7000 10-03-02 18:48:12
M 100 COMPLD
  "::TYPE=BTI7000,NEID=0,NENAME=BTI7000,GATEWAY=10.1.1.1,
SITEID=0,SITENAME=SITE1,TZ=USAEASTERN,AUTODST=Y,UPTIME=5122-08-34,
AUTOP=ISAINSTMR=00-00,STP=OFF,CONTACT=Technical
support at 555-5555"
;
```

## 2.1.4 Retrieving the vendor, model, NE type and software version

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

To retrieve the vendor, model, network element type and software version, use the following TL1 command:

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

### Example command and response

```
RTRV-NETYPE:BTI7000::100::;
```

```
BTI7000 06-01-27 10:26:49
M 100 COMPLD
  "BTI,BTI 7060,WDM,8.1.0"
;
```

## 2.2 Provisioning Network Time Protocol (NTP)

When NTP is provisioned, the system time is retrieved periodically from configured time servers and used to set/update the system time and update the local system clock. If the NTP servers are not reachable, the system time falls back to using the local system clock.

Up to five NTP servers can be configured in the NTP servers association list. The NTP client attempts to connect to every configured NTP server to select the best time source.

The provisioning of NTP is supported through the TL1 interface and through SNMP.

### Provisioning NTP using TL1 commands

The following TL1 commands are used to provision NTP. For detailed information about each command, see the *TL1 Reference Guide*.

| Command       | Description   |
|---------------|---|
| ENT-NTPASSOC  | Use this command to add the IP address of an NTP server to the associations list. The maximum number of NTP servers that can be specified is five. When an NTP association is created, it automatically triggers a time retrieval by the NTP client and the polling cycle is restarted. |
| SET-NTP       | Use this command to set the polling interval time updates.  |
| RTRV-NTPASSOC | Use this command to show all of the associated NTP servers.   |
| RTRV-NTP      | Use this command to display NTP status information, such as whether the local system clock is synchronized to a reference clock source, the stratum of the reference clock, and the IP address of the server from which the reference clock is being obtained.                          |
| DLT-NTPASSOC  | Use this command to delete an associated NTP server IP address. Deleting all of the NTP associations disables the NTP client and causes the system time to be maintained using the local system clock. All NTP conditions that were raised are cleared when the NTP client is disabled. |

### Provisioning NTP using SNMP

The following extract from the BTI-7000-MIB in the file "bti7000\_v1.my" lists the MIB objects related to NTP.

```
ntpClient OBJECT IDENTIFIER ::= { networkElement 13 }

ntpClientPollingRate OBJECT-TYPE
    SYNTAX      HoursAndMinutes
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION  "The polling rate for the NTP client to periodically fetch
the
                system time from the list of NTP servers configured."
    ::= { ntpClient 1 }

ntpClientAuthKey OBJECT-TYPE
    SYNTAX      INTEGER (0..65535)
```

```

    MAX-ACCESS    read-write
    STATUS        current
    DESCRIPTION   "The NTP authentication key ID, if authentication is
required."
    ::= { ntpClient 2 }

ntpClientSyncState OBJECT-TYPE
    SYNTAX        DisplayString (SIZE (0..32))
    MAX-ACCESS    read-only
    STATUS        current
    DESCRIPTION   "Status indicating if the node is in sync with one of the
time
                    servers. Either Y or N."
    ::= { ntpClient 3 }

ntpClientStratum OBJECT-TYPE
    SYNTAX        INTEGER (0..65535)
    MAX-ACCESS    read-only
    STATUS        current
    DESCRIPTION   "Specifies the stratum of the timer server the node is in in
sync
                    with."
    ::= { ntpClient 4 }

ntpClientRefIPAddr OBJECT-TYPE
    SYNTAX        IPAddress
    MAX-ACCESS    read-only
    STATUS        current
    DESCRIPTION   "The IP address of the time server the node is in sync
with."
    ::= { ntpClient 5 }

ntpClientAssocTable OBJECT-TYPE
    SYNTAX        SEQUENCE OF NTPClientAssocEntry
    MAX-ACCESS    not-accessible
    STATUS        current
    DESCRIPTION   "A list of NTP servers to poll for the system time. The NTP
                    client then decides which is best clock source."
    ::= { ntpClient 6 }

ntpClientAssocEntry OBJECT-TYPE
    SYNTAX        NTPClientAssocEntry
    MAX-ACCESS    not-accessible
    STATUS        current
    DESCRIPTION   "The list entry for an NTP server."
    INDEX         { ntpClientAssocIdx }
    ::= { ntpClientAssocTable 1 }

NTPClientAssocEntry ::= SEQUENCE { ntpClientAssocIdx      IPAddress,
                                    ntpClientAssocRowStatus RowStatus }

```

```
ntpClientAssocIdx OBJECT-TYPE
    SYNTAX      IPAddress
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION  "The IP address of the NTP server."
    ::= { ntpClientAssocEntry 1 }

ntpClientAssocRowStatus OBJECT-TYPE
    SYNTAX      RowStatus
    MAX-ACCESS   read-create
    STATUS       current
    DESCRIPTION  "Used to control the addition and deletion of entries in the
                  NTP client association table."
    ::= { ntpClientAssocEntry 100 }
```

### **NTP alarm**

The system raises the SRVR-UNRESPONSIVE alarm when it cannot obtain a timing reference from the NTP server that is identified in the alarm.

The SRVR-UNRESPONSIVE alarm does not mean that the system is not synchronized to a reference clock. If there are multiple NTP servers specified in the associations list, the system may be synchronized to another server in the list.

For detailed information about the SRVR-UNRESPONSIVE and how to clear it, see the *Alarm and Troubleshooting Guide*.

This section covers the following topics:

- [2.2.1, “Specifying an NTP server”](#)
- [2.2.2, “Specifying NTP poll time”](#)
- [2.2.3, “Retrieving associated NTP servers”](#)
- [2.2.4, “Retrieving NTP client servers”](#)
- [2.2.5, “Deleting associated NTP servers”](#)



## 2.2.1 Specifying an NTP server

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

To add the IP address of an NTP server to the associations list, use the following TL1 command:

```
ENT-NTPASSOC:[TID]::[CTAG]::ASSOCIPADDR=<associpaddr>;
```

### Example command

```
ENT-NTPASSOC:BTI7000::100::ASSOCIPADDR=156.284.124.629;
```

## 2.2.2 Specifying NTP poll time

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

To set the polling interval time updates, use the following TL1 command:

```
SET-NTP:[TID]::[CTAG]::[POLLPERIOD=<pollperiod>],[AUTHKEY=<authkey>;]
```

### Example command

```
SET-NTP:BTI7000::100::POLLPERIOD=12-01;
```

## 2.2.3 Retrieving associated NTP servers

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

To retrieve all the associated NTP servers, use the following TL1 command:

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

### Example command and response

```
RTRV-NTPASSOC:BTI7000::100;
```

```
BTI7000 10-09-21 10:28:29
M 100 COMPLD
  "ASSOCIPADDR=192.25.6.14"
;
```

## 2.2.4 Retrieving NTP client servers

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

To retrieve NTP client status and information on the node, use the following TL1 command:

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

### Example command and response

```
RTRV-NTP:BTI7000::100;
```

```
BTI7000 07-09-21 10:28:29
```

```
M 100 COMPLD
```

```
"POLLPERIOD=12-12,AUTHKEY=0,SYNCSTATE=Y,STRATUM=3,REFIPADDR=10.4.0.50"
```

```
;
```

## 2.2.5 Deleting associated NTP servers

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

To delete the IP address of an NTP server from the associations list, use the following TL1 command:

```
DLT-NTPASSOC:[TID]::[CTAG]::ASSOCIPADDR=<associpaddr>;
```

### Example command

```
DLT-NTPASSOC:BTI7000::100::ASSOCIPADDR=192.25.6.14;
```

## 2.3 Provisioning the date and time on the system

### 2.3.1 Editing the date and time

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

To edit the time and date of the system, using the following TL1 command:

```
ED-DAT:[TID]::[CTAG]::[<yymmdd>],[<hhmmss>;
```

**Note** The valid two-digit date range is from 70-01-01 to 36-02-06 that represents 1970-01-01 (GMT) to 2036-02-06 (GMT).

#### Example command

```
ED-DAT:BTI7000::100:10-11-30,13-34-00;
```

### 2.3.2 Editing the date and time during a daylight-saving-time transition

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

Inaccurate date and time settings can occur if you set the date and time on the system during a daylight-saving-time (DST) transition. When a time zone changes to or from DST, the local time can roll back by one hour (for example, 2:00 A.M. becomes 1:00 A.M.). The local time during this hour is ambiguous (for example, 1:15 A.M occurs twice on the day that the time zone switches from DST).

To edit the date and time during a daylight-saving-time transition, use the following TL1 commands:

```
ED-DAT:[TID]::[CTAG]::[<yymmdd>],[<hhmmss>;
```

```
ED-SYS:[TID]::[CTAG]::[NEID=<neid>],[NENAME=<nename>],[GATEWAY=<gateway>],
[SECGATEWAY=<secgateway>],[SITEID=<siteid>],[SITENAME=<sitename>],[TZ=<tz>],
[AUTODST=<autodst>],[AUTOP=<autop>],[AINSTMR=<ainstmr>],[STP=<stp>],
[CONTACT=<contact>;
```

#### Step 1 Disable the AUTODST parameter

```
ED-SYS:BTI7000::100::AUTODST=N;
```

#### Step 2 Set the local time

```
ED-DAT:BTI7000::100::YY-MM-DD,HH-MM-SS;
```

where

YY-MM-DD is the date in a year-month-day format

HH-MM-SS is the time in an hour-minute-second format

for example,

```
ED-DAT:BTI7000::100::10-04-07,00-31-57;
```

### Step 3 Re-enable the AUTODST parameter

```
ED-SYS:BTI7000::100::AUTODST=Y;
```

## 2.3.3 Retrieving the system identifier, date, and time

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

To retrieve basic TL1 header information, use the following TL1 command:

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

### Example command and response

```
RTRV-HDR:BTI7000::100::;
```

```
BTI7000 10-11-05 15:00:02
M 100 COMPLD
;
```

## 2.4 Provisioning IP address parameters

### 2.4.1 Changing the default IP address and mask

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

To change the default IP address information for a network element, use the following TL1 command:

**Note** When the ED-IP command changes the IP address information, all open sessions for that interface are terminated.

```
ED-IP:[TID]:<aid>:[CTAG]::[IPADDR=<ipaddr>],[IPMASK=<ipmask>],
[MEDIARATE=<mediarate>],[C1=<custom>],[GATEWAY=<gateway>]:[<pst>],[<sst>;
```

#### Example command

```
ED-IP:NE-117:IP-1-5-2:100:::IPADDR=50.1.1.1,IPMASK=255.255.255.0,
MEDIARATE=AUTO, GATEWAY=10.1.1.1;
```

### 2.4.2 Changing the default gateway

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

To change the default gateway for the network element, use the following TL1 command:

```
ED-SYS:[TID]::[CTAG]::[NEID=<neid>],[NENAME=<nename>],[GATEWAY=<gateway>],
[SECGATEWAY=<secgateway>],[SITEID=<siteid>],[SITENAME=<sitename>],[TZ=<tz>],
[AUTODST=<autodst>],[AUTOP=<autop>],[AINSTMR=<ainstmr>],[STP=<stp>],
[CONTACT=<contact>;
```

**Note** The gateway address must be within the same subnet as the provisioned network.

#### Example command

```
ED-SYS:BTI7000::100:::NEID=34,NENAME=Trenton02, GATEWAY=156.12.4.
12,SITEID=572,SITENAME=Trenton,TZ=USAEASTERN, AUTODST=Y;
```

## 2.4.3 Editing the IP address

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

To edit the IP address information for the network element, use the following TL1 command:

**Note** Using this command can result in temporary loss of contact with the network element.

```
ED-IP:[TID]:<aid>:[CTAG]:::[IPADDR=<ipaddr>],[IPMASK=<ipmask>],
[MEDIARATE=<mediarate>],[C1=<custom>],[GATEWAY=<gateway>]:[<pst>],[<sst>;
```

### Example command

```
ED-IP:NE-117:IP-1-5-2:100:::IPADDR=50.1.1.1,IPMASK=255.255.255.0,
MEDIARATE=AUTO, GATEWAY=10.1.1.1;
```

## 2.4.4 Retrieving the IP address

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

To retrieve the IP address information for the network element, use the following TL1 command:

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

### Example command and response

```
RTRV-IP:NE-117::100::;
```

```
NE-117 04-02-02 12:39:57
M 100 COMPLD
"IP-1-5-1:IPADDR=127.0.0.1,IPMASK=255.0.0.0,UNMBRD=N:
OOS-AU,AINS&UEQ&SGEO,,PORTSTATE=DISABLED"

"IP-CRAFT:IPADDR=192.168.17.1,IPMASK=255.255.255.0,:,"

"IP-1-5-2:IPADDR=40.1.1.1,IPMASK=255.255.255.0,IPBCST=40.1.1.255,
TYPE=ETHERNET,UNMBRD=N,SPEED=100,DUPLEX=FULL,MEDIARATE=100FD,MTU=1500,MACADDR
=0010ec4046f7,:IS-NR,,PORTSTATE=FORWARDING"
;
```

**Note** IP-NMS is the management LAN, IP-CRAFT is the craft LAN, and IP-1-5-(1,2) is the OSC port on the SCP.

## 2.4.5 Managing ARP

To communicate, using TCP/IP, with any device on the network, the transmitting computer (SCP) must know the Ethernet MAC address for the device it is trying to reach. If the device is not on the Local Area Network (LAN), the data goes through the default gateway (router) and the router's MAC address is used. ARP (Address Resolution Protocol) is a request/reply protocol. It is used to associate Layer 3 (network) IPv4 addresses with Layer 2 (data link) MAC addresses, within a single network not across internetwork nodes.

An ARP table is used to manage the list of IP-to-MAC address mappings. As traffic arrives from external sources, the SCP builds an ARP table. If the SCP needs to originate traffic to an IP for which a MAC is not known, it starts an ARP cycle. An ARP cycle sends a broadcast message requesting the MAC address for a specific IP address. A unicast reply with the MAC address is returned, and the address is added to the ARP table. Once the ARP cycle is complete, the SCP continues to send the original traffic. You can use this table to troubleshoot and resolve network connectivity issues related to invalid or aged entries in the table.

The BTI implementation of ARP allows you to display up to 512 entries and flush all entries from the ARP table. Note that you cannot delete individual entries. Following are the TL1 and CLI commands used to manage ARP. For detailed information about these commands, refer to the BTI 7000 Series TLI and CLI command reference guides.

**Table 2-1 ARP commands**

| Command Interface | Command  | Description                         |
|-------------------|----------|-------------------------------------|
| TL1               | RTRV-ARP | Displays the ARP table.             |
| CLI               | show arp |                                     |
| TL1               | DLT-ARP  | Deletes all entries from the table. |
| CLI               | no arp   |                                     |

You can also manage ARP using the proNX 900 graphical interface. Navigate to the SCP, right-click on the module and choose **View ARP Table**. Following is an example of the GUI display:

**Figure 2-1 ARP table display**

| IP Address   | MAC Address       | Type      |
|--------------|-------------------|-----------|
| 10.1.1.1     | 00:10:DB:35:41:56 | DYNAMIC   |
| 10.1.108.2   | 00:14:D0:30:31:32 | PUBLISHED |
| 192.168.17.1 | 00:14:D0:30:31:33 | PUBLISHED |

Buttons: Refresh, Clear Entries, Close, Help

## 2.5 Craft serial interface parameters

When the system is initially commissioned for service, the serial port settings default to the following values:

- Speed = 9600
- Data bits = 8
- Parity = None
- Stop bits = 1
- Flow control = None

### 2.5.1 Editing craft serial port information

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

To edit the serial port information for the network element, use the following TL1 command:

**Note** Using this command can result in temporary loss of contact with the network element, if connected through the serial port.

```
ED-SER:[TID]:<aid>:[CTAG]:::[RATE=<rate>][,DATABITS=<databits>]
[,PARITY=<parity>][,STOPBITS=<stopbits>];
```

**Important** This command cannot be used to edit the default values of the craft serial port on an expansion shelf. The RS-232 default values of the ESI craft serial port are not editable.

#### Example command

```
ED-SER:BTI7000:SER-1:100:::RATE=9600,DATABITS=8,PARITY=NONE, STOPBITS=1;
```

### 2.5.2 Retrieving craft serial port information

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

To retrieve the serial port information for a network element, use the following TL1 command:

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

#### Example command and response

```
RTRV-SER:BTI7000::100::;
```

```
BTI7000 02-11-05 15:00:00
```



M 100 COMPLD

"SER-1:RATE=9600,DATABITS=8,PARITY=NONE,STOPBITS=1";

## 2.6 Filler pack and filler faceplate detection

A filler face plate differs from a filler pack in that there is no way for the system to detect the presence or absence of a filler face plate.

Filler packs are supported on the BTI 7030 and BTI 7060.

Filler packs are not supported on the BTI 7200 because the system cannot detect these packs. The Circuit Pack Missing condition is raised only if a slot is provisioned and there is no circuit pack present. If a slot is not provisioned and is empty, then no Circuit Pack Missing condition is raised against the slot.

For the BTI 7030 and BTI 7060, the system can be configured to enable or disable the filler pack detection using the system option FPDETECT. This option is used to control when the Circuit Pack Missing condition is raised for filler packs on BTI 7030 and BTI 7060 shelves. This option does not apply to the BTI 7200.

The default setting for this option depends on the origin of the database:

- If the database was created pre-8.1, then FPDETECT=ON.
- If the database was created in 8.1, then FPDETECT=OFF.

If FPDETECT is ON: the Circuit Pack Missing condition is raised if there is nothing inserted. If the slot is provisioned, then only one Circuit Pack Missing condition is raised associated with the provisioned pack even if it occupies more than one slot. If there is no provisioning, the condition is raised for every un-provisioned slot.

If FPDETECT is OFF: the Circuit Pack Missing condition is raised only if the slot is provisioned and there is no pack inserted. Only one Circuit Pack Missing condition is raised for the pre-provisioned slot even if the provisioned pack occupies more than one slot.

The following table lists the system behavior under the following conditions:

- BTI 7030 and BTI 7060 systems running R7.3.x
- BTI 7030 and BTI 7060 systems upgrading from R7.3.x to R8.2
- BTI 7030 and BTI 7060 systems running R8.1 with the Filler Pack Detection option turned on
- BTI 7200 systems running R8.2 and higher.
- Filler is **Present** in the slot

| PEC      | Filler type                              | BTI 7020 | BTI 7030                   | BTI 7060                   | BTI 7200 |
|----------|--|----------|----------------------------|----------------------------|----------|
| BP1A55AA | Filler pack                              | No Alarm | No Alarm                   | No Alarm                   | No Alarm |
| BT7A55AA | Filler panel - universal single slot     | No Alarm | Circuit Pack Missing Alarm | Circuit Pack Missing Alarm | No Alarm |
| BT7A55BA | Filler panel - BTI 7060/BTI 7200 CU slot |          |                            |                            | No Alarm |
| BT7A55CA | Filler panel - BTI 7200 MSI slot         |          |                            |                            | No Alarm |

| PEC      | Filler type                      | BTI 7020 | BTI 7030 | BTI 7060 | BTI 7200 |
|----------|----------------------------------|----------|----------|----------|----------|
| BT7A55DA | Filler panel - BTI 7200 CCM slot |          |          |          | No Alarm |
| BT7A55EA | Filler panel Kit - BTI 7060      |          |          | No Alarm |          |

The following table lists the system behavior under the following conditions:

- BTI 7030 and BTI 7060 systems running R7.3.x
- BTI 7030 and BTI 7060 systems upgrading from R7.3.x to R8.2
- BTI 7030 and BTI 7060 systems running R8.1 with the Filler Pack Detection option turned on
- BTI 7200 systems running R8.2 and higher.
- Filler is **Absent** from the slot

| PEC      | Filler type                              | BTI 7020 | BTI 7030                   | BTI 7060                   | BTI 7200 |
|----------|--|----------|----------------------------|----------------------------|----------|
| BP1A55AA | Filler pack                              | No Alarm | Circuit Pack Missing Alarm | Circuit Pack Missing Alarm | No Alarm |
| BT7A55AA | Filler panel - universal single slot     | No Alarm | Circuit Pack Missing Alarm | Circuit Pack Missing Alarm | No Alarm |
| BT7A55BA | Filler panel - BTI 7060/BTI 7200 CU slot |          |                            |                            | No Alarm |
| BT7A55CA | Filler panel - BTI 7200 MSI slot         |          |                            |                            | No Alarm |
| BT7A55DA | Filler panel - BTI 7200 CCM slot         |          |                            |                            | No Alarm |
| BT7A55EA | Filler panel Kit - BTI 7060              |          |                            | No Alarm                   |          |

The following table lists the system behavior under the following conditions:

- BTI 7030 and BTI 7060 systems running R8.2 and higher
- BTI 7030 and BTI 7060 systems upgrading from R7.3.x to R8.2 and higher with the Filler Pack Detection option turned off
- BTI 7200 systems running R8.2 and higher
- Filler is **Absent or Present** in the slot

| PEC      | Filler type                              | BTI 7020 | BTI 7030 | BTI 7060 | BTI 7200 |
|----------|--|----------|----------|----------|----------|
| BP1A55AA | Filler pack                              | No Alarm | No Alarm | No Alarm | No Alarm |
| BT7A55AA | Filler panel - universal single slot     | No Alarm | No Alarm | No Alarm | No Alarm |
| BT7A55BA | Filler panel - BTI 7060/BTI 7200 CU slot |          |          |          | No Alarm |

| PEC      | Filler type                      | BTI 7020 | BTI 7030 | BTI 7060 | BTI 7200 |
|----------|----------------------------------|----------|----------|----------|----------|
| BT7A55CA | Filler panel - BTI 7200 MSI slot |          |          |          | No Alarm |
| BT7A55DA | Filler panel - BTI 7200 CCM slot |          |          |          | No Alarm |
| BT7A55EA | Filler panel Kit - BTI 7060      |          |          | No Alarm |          |

## 2.6.1 Setting the FPDETECT option

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

To change the FPDETECT option, use the following TL1 commands:

### Example command to turn FPDETECT on:

```
ED-SYS:[TID]::100::FPDETECT=ON
```

```
[TID] 10-04-20 17:00:39
```

```
[TID] 10-04-20 17:00:39
```

```
A 3 REPT DBCHG
```

```
"TIME=17-00-39,DATE=10-04-20,SOURCE=100,LINKID=2-16,USERID=admin,DBCHGSEQ=1:ED-SYS::FPDETECT=ON"
```

### Example command to turn FPDETECT off:

```
ED-SYS:[TID]::100::FPDETECT=OFF
```

```
[TID] 10-04-20 17:00:40
```

```
A 3 REPT DBCHG
```

```
"TIME=17-00-40,DATE=10-04-20,SOURCE=100,LINKID=2-16,USERID=admin,DBCHGSEQ=1:ED-SYS::FPDETECT=OFF"
```

## 2.7 Center support detection

In this release center supports with ground pins are not detected by the system. As a result, the width of a slot cannot be determined by the system and in the case of a Circuit Pack Missing alarm the alarm is raised for two slots instead one slot even though the center support has been removed.

The following table lists the system behavior:

| Center support type               | Release         | BTI 7020                   | BTI 7030                   | BTI 7060                   | BTI 7200 |
|-----------------------------------|-----------------|----------------------------|----------------------------|----------------------------|----------|
| Center support with ground pin    | R8.1 or later   | No alarm                   | No alarm                   | No alarm                   | No alarm |
|                                   | R7.x or earlier | Circuit Pack Missing alarm | Circuit Pack Missing alarm | Circuit Pack Missing alarm |          |
| Center support without ground pin | R8.1 or later   | No alarm                   | No alarm                   | No alarm                   | No alarm |
|                                   | R7.x or earlier | Not compatible             | Not compatible             | Not compatible             |          |



## 3.0 Expansion shelf provisioning rules and configuration

---

- 3.1, “Expansion shelf provisioning rules”
- 3.2, “Configuring expansion shelves”
- 3.3, “Repurposing expansion shelves”
- 3.4, “Expansion shelf command line interface”

## 3.1 Expansion shelf provisioning rules

---

### Connection to an unprovisioned port on the System Control Processor (SCP)

When an expansion shelf is connected to an unprovisioned port on the SCP, the following applies:

- The expansion shelf is auto created with the discovered shelf configuration.
- Since the expansion shelf is auto created, it does not depend on the AUTOP flag being set.
- If the AUTOP parameter is set to IS, every slot in the expansion shelf in which a module is installed is auto provisioned, as are supported facilities on the modules.
- If the AUTOP parameter is set to OFF, no slot in the expansion shelf is provisioned.

### Basic provisioning

- Expansion shelves cannot be de-provisioned when connected to the SCP on the main shelf.
- Expansion shelves can be de-provisioned when not connected to the SCP on the main shelf. Use the DLT-EQPT command.
- Expansion shelf parameters can be edited with or without being connected to the SCP on the main shelf. Use the ED-EQPT command.
- Expansion shelves can be removed from service with or without being connected to the SCP on the main shelf. Use the RMV-EQPT command.
- Expansion shelves can be restored to service with or without being connected to the SCP on the main shelf. Use the RST-EQPT command.

For information about these basic provisioning commands, see [Chapter 4, “Equipment provisioning”](#) and the *TL1 Reference Guide*.

### Fault LEDs

- Fault LEDs on the expansion shelf SFPs in the SCP do not activate if an expansion shelf is not provisioned.

### REPLUNITMEA alarm

- When a REPLUNITMEA alarm is present on an expansion shelf that is connected to an SCP, the expansion shelf can be forced to accept provisioning data by clearing the alarm. For information about clearing this alarm refer to the *BTI 7000 Series Alarm and Troubleshooting Guide*.



## 3.2 Configuring expansion shelves

When provisioning an expansion shelf, use the SHCONF field of the ENT-EQPT or ED-EQPT command to specify the shelf configuration. If no SHCONF value is entered, the system automatically defaults to the 6-SLOT configuration.

Expansion shelves support the configurations described in the following table.

**Table 3-1 BTI 7060 Expansion shelf configuration values**

| Variable | Meaning   |
|----------|---|
| 3-SLOT   | <p>3-slot shelf with all of the center supports removed</p> <p>or</p> <p>3-slot shelf with all of the center supports removed and the EMI plate between slots 1/2 and 3/4 removed to create a double-height slot. In this case, although there are two physical slots (one of which is a double height slot) the system still considers this to be a 3-slot shelf. The system considers that slot 1 is provisioned with the module, and that slot 3 is present but empty.</p> <p>or</p> <p>3-slot shelf with all of the center supports removed and the EMI plate between slots 3/4 and 5/6 removed to create a double-height slot. In this case, although there are two physical slots (one of which is a double height slot) the system still considers this to be a 3-slot shelf. The system considers that slot 3 is provisioned with the module, and that slot 5 is present but empty.</p> |
| 4-SLOT   | <p>4-slot shelf with the center supports for slots 1 and 2, and slots 3 and 4 removed</p> <p>or</p> <p>4-slot shelf with the center support for slots 1 and 2 and slots 3 and 4 removed and the EMI plate between slots 1/2 and 3/4 removed to create a double-height slot. In this case, although there are three physical slots (one of which is a double height slot) the system still considers this to be a 4-slot shelf. The system considers that slot 1 is provisioned with the module, and that slot 3 is present but empty.</p>   |
| 4B-SLOT  | 4-slot shelf with the center supports for slots 1 and 2, and slots 5 and 6 removed  |
| 4C-SLOT  | <p>4-slot shelf with the center supports for slots 3 and 4, and slots 5 and 6 removed</p> <p>or</p> <p>4-slot shelf with the center support for slots 3 and 4 and slots 5 and 6 removed and the EMI plate between slots 3/4 and 5/6 removed to create a double-height slot. In this case, although there are three physical slots (one of which is a double height slot) the system still considers this to be a 4C-slot shelf. The system considers that slot 3 is provisioned with the module, and that slot 5 is present but empty.</p>  |
| 5-SLOT   | 5-slot shelf with the center support for slots 1 and 2 removed  |
| 5B-SLOT  | 5-slot shelf with the center support for slots 3 and 4 removed  |
| 5C-SLOT  | 5-slot shelf with the center support for slots 5 and 6 removed  |

**Table 3-1 BTI 7060 Expansion shelf configuration values (Continued)**

| Variable | Meaning      |
|----------|--------------|
| 6-SLOT   | 6-slot shelf |

For information on how to physically configure an expansion shelf, see the *Common Equipment Installation Guide*.

### 3.3 Repurposing expansion shelves

---

To repurpose an expansion shelf to a main shelf, or vice-versa, the shelves must be removed from service and powered down.

The following equipment is required when changing an expansion shelf to a main shelf:

- Main Shelf Interface (MSI)
- System Control Processor (SCP)

The following equipment is required when changing a main shelf to an expansion shelf:

- Expansion Shelf Interface (ESI)

For information on how to move expansion shelves to a different port or to a different main shelf, refer to the *BTI 7000 Series Common Equipment and Installation Guide*.

## **3.4 Expansion shelf command line interface**

---

Using the command line interface (CLI) and TL1, users can retrieve inventory information about SFPs in the Expansion Shelf Interface (ESI). The CLI is accessed through the ESI craft serial port.

## 4.0 Equipment provisioning

---

- 4.1, “Entering new equipment”
- 4.2, “Editing equipment”
- 4.3, “Removing equipment from service”
- 4.4, “Restoring equipment to service”
- 4.5, “Retrieving equipment attributes”
- 4.6, “Retrieving equipment inventory”
- 4.7, “Deleting equipment”

## 4.1 Entering new equipment

---

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

To enter new equipment, use the following TL1 command:

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

### Example command

```
ENT-EQPT:BTI7000:OPA-1-2:100::BP1A01DA;
```

## 4.2 Editing equipment



To edit equipment provision parameters, use the following TL1 command:

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

### Example command

```
ED-EQPT:BTI7000:OLAM-1-6:100:::C1=Line amplifier for downtown link;
```

## 4.3 Removing equipment from service

---

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

To remove equipment from service, use the following TL1 command:

```
RMV-EQPT:[TID]:<aid>:[CTAG]::;
```

### Example command

```
RMV-EQPT:BTI7000:OLAM-1-1:100;
```



## 4.4 Restoring equipment to service

---

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

To restore equipment to service, use the following TL1 command:

```
RST-EQPT:[TID]:<aid>:[CTAG]::;
```

### Example command

```
RST-EQPT:BTI7000:OLAM-1-1:100;
```

## 4.5 Retrieving equipment attributes

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

To retrieve equipment attributes, use the following TL1 command:

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

### Example

```
RTRV-EQPT:BTI7000::100::;
```

### Response from a BTI 7060 shelf

```
BTI7000 04-08-05 10:24:36
M 100 COMPLD
"MS-1:BT7A53BA:SHCONF=6-SLOT:IS-NR,"
"SCP-1-5:BT7A50AA::IS-NR,"
;
```

### Response from a BTI 7200 shelf

```
BTI7000 10-07-08 15:45:26
M 100 COMPLD
"MS-1:BT7A51AA::IS-NR,"
"ES-11:BT7A51AA::IS-NR,"
"TPR-11-1:BT7A49AA::IS-NR,"
"TPR-11-2:BT7A49AA::IS-NR,"
"TPR-11-3:BT7A49AA::IS-NR,"
"TPR-11-4:BT7A49AA::IS-NR,"
"TPR-11-5:BT7A49AA::IS-NR,"
"TPR-11-6:BT7A49AA::IS-NR,"
"TPR-11-7:BT7A49AA::IS-NR,"
"TPR-11-8:BT7A49AA::IS-NR,"
"TPR-11-9:BT7A49AA::IS-NR,"
"TPR-11-10:BT7A49AA::IS-NR,"
;
```

### Response from a BTI 7030 shelf

```
NE117 04-11-18 17:04:26
M 100 COMPLD
"SH-1:BP1A56AA:SHCONF=3-SLOT:IS-NR,"
"SCP-1-3:BP1A20AA::IS-NR,"
"SMF30-1-1:BP1A10CD-LC::IS-NR,"
"SPA-1-2:BP1A05PA::IS-NR,"
;
```

## 4.6 Retrieving equipment inventory

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

To retrieve an equipment inventory, use the following TL1 command:

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

### Example command

```
RTRV-INV:BTI7000::100::;
```

### Response from a BTI 7060 shelf

```
BTI7000 04-11-18 16:59:36
M 100 COMPLD
"MS-1,EQPT:NAME=MS2060,PEC=BP1A50AA,CLEI=None,FNAME=Main Shelf
BTI7000 2060,SHCONF=6-SLOT,"
"SH-1,EQPT:NAME=2060,PEC=BP1A5021,CLEI=WMMKTWOKRA,FNAME=BTI7000
2060 Shelf,HWREV="\0\","
"SLOT-1-1,EQPT:NAME=FLLR,PEC=BP1A55AA,CLEI=WMPQALX7AA,FNAME=Filler,
SER="\N/A\","HWREV="\0\","MFGDAT="\N/A\","MFGLOCN=N/A,TSTDAT=N/A,
TSTLOCN=N/A,"
"SLOT-1-2,EQPT:NAME=FLLR,PEC=BP1A55AA,CLEI=WMPQALX7AA,FNAME=Filler,
SER="\N/A\","HWREV="\0\","MFGDAT="\N/A\","MFGLOCN=N/A,TSTDAT=N/A,
TSTLOCN=N/A,"
"SLOT-1-3,EQPT:NAME=FLLR,PEC=BP1A55AA,CLEI=WMPQALX7AA,FNAME=Filler,
SER="\N/A\","HWREV="\0\","MFGDAT="\N/A\","MFGLOCN=N/A,TSTDAT=N/A,
TSTLOCN=N/A,"
"SLOT-1-4,EQPT:NAME=FLLR,PEC=BP1A55AA,CLEI=WMPQALX7AA,FNAME=Filler,
SER="\N/A\","HWREV="\0\","MFGDAT="\N/A\","MFGLOCN=N/A,TSTDAT=N/A,
TSTLOCN=N/A,"
"SLOT-1-5,EQPT:NAME=SCP,PEC=BP1A20AA,CLEI=WMEC170KAA,FNAME=System
Control Processor,SER="\03190142\","HWREV="\4\","MFGDAT="\2004-08-17\","
MFGLOCN=BTI7000,TSTDAT=2004-08-17,TSTLOCN=BTI7000,"
"SLOT-1-6,EQPT:NAME=FLLR,PEC=BP1A55AA,CLEI=WMPQALX7AA,FNAME=Filler,
SER="\N/A\","HWREV="\0\","MFGDAT="\N/A\","MFGLOCN=N/A,TSTDAT=N/A,
TSTLOCN=N/A,"
"SI-1,EQPT:NAME=MSI,PEC=BP1A53AA,CLEI=WMEC280KAA,FNAME=Main Shelf
Interface,SER="\SN00001627\","HWREV="\5\","MFGDAT="\2004-08-04\","
MFGLOCN=BTI7000,TSTDAT=2004-08-04,TSTLOCN=BTI7000,"
"CU-1,EQPT:NAME=CU,PEC=BP1A52AA,CLEI=CL1A52AA,FNAME=Cooling Unit,
SER="\454326578\","HWREV="\1\","MFGDAT=
\2002-07-18\","MFGLOCN=BTI7000,TSTDAT=2002-07-18,TSTLOCN=BTI7000,"
;
RTRV-INV:BTI7000::100::;
```

## Response from a BTI 7200 shelf

```
BTI7000 10-07-08 15:33:26
M 100 COMPLD
"MS-1,EQPT:NAME=BTI7000,PEC=BT7A51AA,CLEI=UNKNOWN,FNAME=Main Shelf 7200,HWREV=
\"0\",USI=N/A"
"SLOT-1-1,EQPT:NAME=SCP,PEC=BT7A20CA,FNAME=7060 System Control Processor,SER=
\"SE09391083\",HWREV=\"5\",FW=\"NATIVE\",MFGDAT=\"2009-09-27\",MFGLOCN=19,TSTDAT
=2009-09-27,TSTLOCN=19,USI=N/A"
"ESFP-1-1-2,EQPT:PEC=BP1A58DD-03,SER=\"712330077\",HWREV=\"D\",MFGDAT=\"2007-
05-03\",WAVELENGTH=0,MINBR=100,MAXBR=2525,NOMBR=2500,ENCODING=UNKNOWN,CONNTYPE=C
OPPER_PIGTAIL,VENDORNAME=\"Molex Inc.\",VENDORPN=\"73929-0027\",VENDOROUI=\"0009
3A\",TXFAULTIMP=N,TXDISABLEIMP=N,LOSIMP=N,DDIAGIMP=N,MEDIA=ELECTRICAL,USI=N/A"
"ESFP-1-1-3,EQPT:PEC=BP1A58DD-03,SER=\"712330082\",HWREV=\"D\",MFGDAT=\"2007-
05-03\",WAVELENGTH=0,MINBR=100,MAXBR=2525,NOMBR=2500,ENCODING=UNKNOWN,CONNTYPE=C
OPPER_PIGTAIL,VENDORNAME=\"Molex Inc.\",VENDORPN=\"73929-0027\",VENDOROUI=\"0009
3A\",TXFAULTIMP=N,TXDISABLEIMP=N,LOSIMP=N,DDIAGIMP=N,MEDIA=ELECTRICAL,USI=N/A"
"SI-1,EQPT:NAME=MSI,PEC=BT7A53EA,FNAME=7200 MAIN SHELF INTERFACE,SER=\"SE1024
0111\",HWREV=\"3\",MFGDAT=\"2010-06-18\",MFGLOCN=16,TSTDAT=2010-06-18,TSTLOCN=16
,USI=N/A"
"CU-1-1,EQPT:NAME=CU,PEC=BT7A52EA,FNAME=7060 COOLING UNIT,SER=\"SX09420027\",
HWREV=\"5\",MFGDAT=\"2009-10-19\",MFGLOCN=19,TSTDAT=2009-10-19,TSTLOCN=19,USI=N/
A"
"CU-1-3,EQPT:NAME=CU,PEC=BT7A52EA,FNAME=7060 COOLING UNIT,SER=\"SX09420025\",
HWREV=\"5\",MFGDAT=\"2009-10-19\",MFGLOCN=19,TSTDAT=2009-10-19,TSTLOCN=19,USI=N/
A"
"CCM-1-1,EQPT:NAME=CCM,PEC=BT7A54EA,FNAME=7200 COMMON COMMUNICATION MODULE,SE
R=\"SN10060015\",HWREV=\"1\",MFGDAT=\"03-12-2010\",MFGLOCN=BTI Northside,TSTDAT=
03-12-2010,TSTLOCN=BTI Northside,USI=N/A"
"ES-11,EQPT:NAME=ES7200,PEC=BT7A51AA,CLEI=UNKNOWN,FNAME=Expansion Shelf 7200,
HWREV=\"0\",USI=N/A"
"SLOT-11-1,EQPT:NAME=DTPR,PEC=BT7A49AA,FNAME=Dual 10G Multiprotocol Transpond
er,SER=\"SE10170225\",HWREV=\"15\",FW=\"NATIVE\",MFGDAT=\"2010-04-27\",MFGLOCN=1
9,TSTDAT=2010-04-27,TSTLOCN=19,USI=N/A"
"XFP-11-1-1,EQPT:PEC=BP3AM4DL-14,SER=\"OYG003\",HWREV=\"01\",MFGDAT=\"2007-11
-28L01\",WAVELENGTH=1547.70,REACH=80,MINBR=9900,MAXBR=11100,ENCODING=UNKNOWN,CON
NTYPE=LC,VENDORNAME=\"FUJITSU\",VENDORPN=\"FIM31060/211W37\",VENDOROUI=\"00000E\
\",TXFAULTIMP=Y,TXDISABLEIMP=Y,LOSIMP=Y,DDIAGIMP=Y,MEDIA=OPTICAL,USI=N/A"
"XFP-11-1-2,EQPT:PEC=BP3AM4MS,SER=\"BCN0845088\",HWREV=\"03\",MFGDAT=\"2008-1
1-06\",WAVELENGTH=1310,MINBR=9900,MAXBR=11300,ENCODING=UNKNOWN,CONNTYPE=LC,VENDO
RNAME=\"BOOKHAM\",VENDORPN=\"IGF-42311J\",VENDOROUI=\"0009A6\",TXFAULTIMP=Y,TXDI
SABLEIMP=Y,LOSIMP=Y,DDIAGIMP=Y,MEDIA=OPTICAL,USI=N/A"
"XFP-11-1-3,EQPT:PEC=BP3AM4DL-14,SER=\"OYG004\",HWREV=\"01\",MFGDAT=\"2007-11
-28L01\",WAVELENGTH=1547.70,REACH=80,MINBR=9900,MAXBR=11100,ENCODING=UNKNOWN,CON
NTYPE=LC,VENDORNAME=\"FUJITSU\",VENDORPN=\"FIM31060/211W37\",VENDOROUI=\"00000E\
\",TXFAULTIMP=Y,TXDISABLEIMP=Y,LOSIMP=Y,DDIAGIMP=Y,MEDIA=OPTICAL,USI=N/A"
"XFP-11-1-4,EQPT:PEC=BP3AM4SS,SER=\"CA13BT018\",HWREV=\"A1\",MFGDAT=\"2010-03
-30\",WAVELENGTH=850,MINBR=9900,MAXBR=10800,ENCODING=UNKNOWN,CONNTYPE=LC,VENDORN
AME=\"JDSU\",VENDORPN=\"PLRXXL-SC-S43-BT\",VENDOROUI=\"00019C\",TXFAULTIMP=Y,TXD
ISABLEIMP=Y,LOSIMP=Y,DDIAGIMP=Y,MEDIA=OPTICAL,USI=N/A"
```

## Response from a BTI 7030 shelf

```
NE117 04-11-18 17:04:17
M 100 COMPLD
  "SH-1,EQPT:NAME=MS1030,PEC=BP1A56AA,CLEI=WMMPA10FRA,FNAME=Main Shelf
BTI7000 1030,HWREV=1,SHCONF=3-SLOT,"
  "SLOT-1-1,EQPT:NAME=SMF30,PEC=BP1A10CD-LC,CLEI=CLEI,FNAME=Dispersion
Compensation Module 30km,SER="\11223344",HWREV="\1",
MFGDAT="\2005-11-12", MFGLOCN=BTI7000,TSTDAT=2005-11-12,TSTLOCN=BTI7000,"
  "SLOT-1-2,EQPT:NAME=SPA,PEC=BP1A05PA-SC,CLEI=NotSet,FNAME=Single
Channel Pre-Amplifier-SC,SER="\SN00080183",HWREV="\5",
MFGDAT="\2004-10-14",MFGLOCN=BTI7000,TSTDAT=2004-10-14,TSTLOCN=BTI7000
Thurston,"
  "SLOT-1-3,EQPT:NAME=SCP,PEC=BP1A21AA,CLEI=WMUCAMSLAA,FNAME=System
Control Processor,SER="\03190142",HWREV="\1",MFGDAT="\2004-10-19",
MFGLOCN=BTI7000,TSTDAT=2004-10-19,TSTLOCN=BTI7000,"
  "CU-1,EQPT:NAME=CU,PEC=BP1A57AA,CLEI=WMPQASP7AA,FNAME=Cooling Unit,
SER="\454326578",HWREV="\1",MFGDAT="\2004-10-28",MFGLOCN=BTI7000,
TSTDAT=2004-10-28,TSTLOCN=BTI7000,"
;
```

## 4.7 Deleting equipment

---

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

To delete equipment, use the following TL1 command:

```
DLT-EQPT:[TID]:<aid>:[CTAG]::[<type>]:[CMDMDE=<cmdmde>];
```

**Note** The equipment must be removed from service before it can be deleted.

### Example command

```
DLT-EQPT:BTI7000:OLAM-1-2:100::BP1A04BA;
```

## 5.0 Performance Monitoring

---

- 5.1, “Understanding performance monitoring data”
- 5.2, “Bin validity qualifiers”
- 5.3, “Retrieving performance monitoring data”
- 5.4, “Threshold crossing alerts”

## 5.1 Understanding performance monitoring data

---

The system supports the collecting and reporting of current and historical statistical information that can be used to assess system performance and network health.

### Performance metric (PM) types

The following PM types are used:

- Gauge: Takes a snapshot measurement of the PM parameter.
- Counters: Measure the number of events that occur during a given time interval.
- Accumulated counts: Measure the number of events that have occurred for the equipment since its last restart.
- Temperature: Monitors the module temperature.
- Voltage: Monitors the module supply voltage.

When users request current PMs, the PMs are retrieved directly from the provisioned equipment at that particular moment.

### Historical PMs

Historical PMs (also known as bins) are available for gauge, counter, temperature, and voltage PM types that are associated with the equipment in a shelf. They are stored at 15-minute and 24-hour intervals. The most recent 96 consecutive 15-minute bins and one 24-hour bin are available for retrieval.

Historical PMs are not available after a system startup or an SCP reboot until the first interval turnover occurs. This happens just prior to the quarter hour, half hour, three-quarter hour, and hour (for example, 10:15, 10:30, 10:45, and 11:00). The previous day's 24-hour bin is recorded at 00:00:00 of the day for gauge PMs. For counter PMs, the value recorded is the total count of the interval.

Additionally, an untimed bin is supported for all PMs. The untimed bin (1-UNT) accumulates indefinitely and is reset when the register capacity is exceeded (that is, 2,147,483,647) and rolls over, when the module is reset, or when it is reset to 0 by the INIT-REG-XCVR command.

### Out-of-service PMs

The collection of PM data is suspended for equipment that is out of service (OOS), but resumes once the equipment is restored to service. When retrieving PM data, any periods for which no data was recorded are indicated as not available (NA).

### Fault conditions

During some fault conditions, it may not be possible to retrieve PM data from a given module and/or the value may not be valid (for example, if the equipment is out of service during the reporting interval). At these times, the specific bins are marked as NA.



All PMs are read only and do not change once recorded in a bin, although current counter-type PM values can be initialized to zero.

**Note** PM data is stored in volatile memory and is not backed up to the database. As a result, the data is not maintained on restart of the system or software upgrade.

## 5.2 Bin validity qualifiers

---

All current and historical bins have a validity qualifier that indicates the completeness of PM data collection for the interval. The validity of current bins can change as the bin interval progresses. The validity of historical bins is the validity that the bin receives when its interval completes.

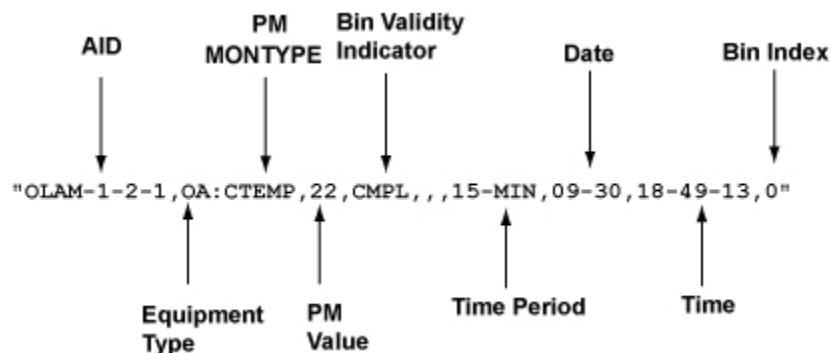
The following table provides information about the supported bin validity qualifiers.

| Qualifier | Description   |
|-----------|---|
| CMPL      | Applies to gauge and counter PMs, and indicates that the collection interval completed normally.  |
| NA        | Applies to gauge and counter PMs, and indicates that no collection occurred during an interval when the collection software had failed to collect PMs or when the equipment had been out of service.  |
| PRTL      | Applies only to counter PMs, and indicates that one of the following conditions occurred during the collection interval: <ul style="list-style-type: none"><li>• The PM collection was interrupted; for example, a transceiver was taken out of service, or a module was inserted after a collection interval started.</li><li>• The register was manually set to zero via the INIT-REG-XCVR command, with parameter MONVAL= 0.</li><li>• The system time was adjusted.</li></ul> |

## 5.3 Retrieving performance monitoring data

Data for current and historical PMs can be retrieved from the system. The following figures explain the meaning of the various fields in the retrieved data.

**Figure 5-1 PM format**



To retrieve current PM data, you specify the time period (tmper), for example, 15-minute, 1-day, or untimed, and an index value. Setting the index value to ALL when tmper is set to 15-minutes retrieves all the data collected for bins 1 to 96. Setting the index value to ALL when tmper is set to 1-day retrieves one bin containing the previous day's PM data.

To retrieve historical PM data, you specify both the date (mondatt) and time (monttm), or the index value. Setting the index to a value between 0 and 96 returns only the data collected for the corresponding bin; setting the index value to ALL returns the data collected for bins 1 to 96.

The following table lists the system-support commands for retrieving PMs. For more information, see the *TLI Reference Guide*.

| Command            | Retrieves PMs for  |
|--------------------|--|
| RTRV-PM-BRI        | BRI port on an 8-Port Multiprotocol Muxponder  |
| RTRV-PM-EQPT       | Retrieves the current or historical temperature data on modules that are equipped with a temperature sensor and retrieves CPU and disk usage from supported modules. |
| RTRV-PM-FC         | FC port on an 8-Port or 10-Port Multiprotocol Muxponder  |
| RTRV-PM-GE         | GE port on a Muxponder module  |
| RTRV-PM-OA         | Optical amplifier  |
| RTRV-PM-OCn        | SONET port on Muxponder module   |
| RTRV-PM-STMn       | SDH port on a Muxponder module   |
| RTRV-PM-STSn/STSnC | SONET path facility object on a Muxponder module   |
| RTRV-PM-VCn/VCnC   | SDH path facility object on a Muxponder module   |
| RTRV-PM-XCVR       | Transceiver port on a Transponder module   |

## 5.4 Threshold crossing alerts

The system monitors the 15-minute and 1-day bins of counter PMs for threshold crossings. When a threshold is crossed during a 15-minute or 1-day time period, a threshold crossing alert (TCA) is generated on all active sessions in the form of a REPT^EVT^ system message for the affected facility.

When the next 15-minute or 1-day time period starts, the current bins are reset to zero and counting continues. If the threshold is crossed again in the new time period, another TCA is generated.

When a new threshold value is set and then crossed because the new value is lower than the earlier value, a TCA is immediately generated provided that a TCA has not been sent already for that time period.

Setting the threshold to zero disables the TCA. By re-initializing the counter to zero, the TCA is re-alarmed for that time period.

The following table lists system-supported commands and messages for setting, retrieving, and reporting TCAs. For more information, see the *TL1 Reference Guide*.

| Set command       | Retrieve command   | Report message      | Facility  |
|-------------------|--------------------|---------------------|---|
| SET-TH-FC         | RTRV-TH-FC         | REPT^EVT^FC         | FC port on an 8-Port or 10-Port Multiprotocol Muxponder |
| SET-TH-GE         | RTRV-TH-GE         | REPT^EVT^GE         | GE port on a Muxponder module                           |
| SET-TH-OCn        | RTRV-TH-OCn        | REPT^EVT^OCn        | SONET port on Muxponder module                          |
| SET-TH-STMn       | RTRV-TH-STMn       | REPT^EVT^STMn       | SDH port on a Muxponder module                          |
| SET-TH-STSn/STSnC | RTRV-TH-STSn/STSnC | REPT^EVT^STSn/STSnC | SONET path facility object on a Muxponder module        |
| SET-TH-VCn/VCnC   | RTRV-TH-VCn/VCnC   | REPT^EVT^VCn/VCnC   | SDH path facility object on a Muxponder module          |
| SET-TH-XCVR       | RTRV-TH-XCVR       | REPT^EVT^XCVR       | Transceiver port on a Transponder module                |

## 6.0 Log management

---

- 6.1, “Log categories”
- 6.2, “Security log”

## 6.1 Log categories

The system maintains a log for all actions, which is organized into individual categories. By default, the system is configured to maintain the log categories described in the following table.

| Log category               | Description   |
|----------------------------|---|
| Alarms                     | Contains all alarm raise and clear events (REPT ALM)  |
| Commands (other than RTRV) | Contains all TL1 commands issued except for RTRV commands   |
| Commands (RTRV)            | Contains all RTRV commands issued   |
| Database changes           | Contains all provisioning change events (REPT DBCHG)  |
| Events                     | Contains all events not included in the database changes category, including removals from service (REPT RMV), restores to service (REPT RST), and system upgrades, module plugs, and module unplugs (REPT EVT) |
| Security                   | Contains all security-related events, such as, login attempts, login failures and logouts(SECURITY)   |
| All                        | Contains all log categories   |

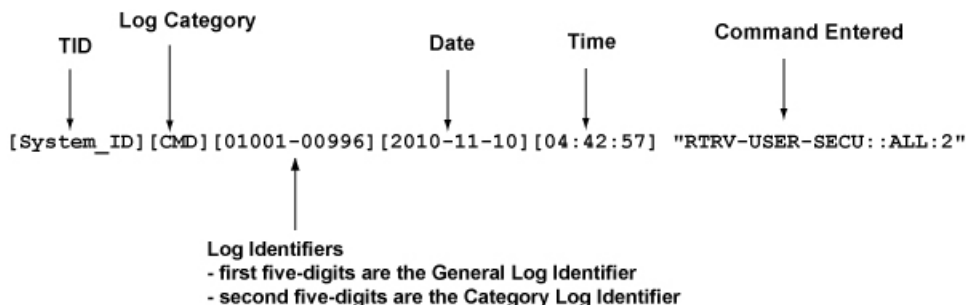
Logging is on by default, and all log information is stored persistently during SCP restarts.

On a fully provisioned system with significant activity, the log file will maintain information covering a 24-hour period of activity. If the system sees little activity, the log file will maintain information covering more than 24-hours of activity, but only up to 1000 entries per category.

Log information is retrievable by both date and time, or by general log identifier. The general log identifier is a sequence number that increments once each time a log of any category is recorded. A second sequence number, which identifies the log category, increments once each time a log of its specific category is recorded.

The following figure explains the meaning of various fields in retrieved log data.

### Figure 6-1 Log format



All log categories, except for the Security category, can be stopped, restarted, and initialized. For information about working with the security log, see [6.2, “Security log”](#).

Log categories can contain a limited number of messages. Each time a message is added to a log stream, the log is checked to see if it has exceeded its maximum size. If the log has exceeded its maximum size, the oldest entry is removed. The maximum size for a log file is 5000 entries.

**Note** Log records are truncated after 200 characters.

This section covers the following topics:

- 6.1.1, “Retrieving logs”
- 6.1.2, “Stopping log recording”
- 6.1.3, “Starting log recording”
- 6.1.4, “Initializing logs”
- 6.1.5, “Retrieving log attributes”

## 6.1.1 Retrieving logs

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

To retrieve log information, use the following TL1 command:

```
RTRV-LOG:[TID]:[<lognm>]:[CTAG]:[<stalogid>],[<stplogid>],[<stadat>],
[<statm>],[<stpdat>],[<stptm>];
```

### Example 1 command and response

```
RTRV-LOG:BTI7000:RTRV:100::,,,,,;
BTI7000 10-10-11 18:02:56
M 100 RTRV
[BTI7000] [RTRV] [01148-00986] [2002-11-10] [04:30:03] "RTRV-HDR:::206"
[BTI7000] [RTRV] [00991-00989] [2002-11-10] [04:41:49] "RTRV-USER-SECU::ALL:
4"
[BTI7000] [RTRV] [00999-00994] [2002-11-10] [04:42:53] "RTRV-USER-SECU::ALL"
[BTI7000] [RTRV] [01001-00996] [2002-11-10] [04:42:57] "RTRV-USER-SECU::ALL:
2"
[BTI7000] [RTRV] [01005-00998] [2002-11-10] [04:43:38] "RTRV-USER-SECU::ALL:
4"
*/
>
BTI7000 10-10-11 18:02:58
M 100 COMPLD
;
```

**Note** In log entries that contain a password, the password replaced by an asterisk (\*).

### Example 2 command and response

In this example, a specific range of logs is retrieved by requesting the stalogid (44205) and the stplogid (44206).

```
RTRV-LOG:BTI7000::100::44205,44206,,,,,;
BTI7000 10-01-05 12:02:12
M 100 RTRV
/*
```

```
[BTI7000] [RTRV] [44205-41712] [2004-01-03] [06:13:56] "User
'admin': RTRV-OA:BTI7000:OLAM-1-3-1:166"
[BTI7000] [RTRV] [44206-41713] [2004-01-03] [06:14:00] "User
'admin': RTRV-PM-OA:BTI7000:OLAM-1-3-1:167"
*/
>
BTI7000 04-01-05 12:02:14
M 100 COMPLD;
```

### Example 3 command and response

In this example, a specific range of alarm logs is retrieved by requesting the statdat and statm parameters (2004-02-03 and 07-20-00) and the stpdat and stptm parameters (2004-02-03 and 07-45-00).

```
RTRV-LOG:BTI7000:ALM:100::,2004-02-03,07-20-00,2004-02-03,07-45-00;
BTI7000 10-02-05 13:04:48
M 100 RTRV
/*
[BTI7000] [REPT-ALM-EQPT] [43973-39343] [2004-02-03] [07:20:53]
"SLOT-1-6,CL,CONTCOM,NSA,2004-02-03,07-20-53,,,,,\"Clear communications
failure.\",,,,,,"
[BTI7000] [REPT-ALM-EQPT] [43974-39344] [2004-02-03] [07:20:55]
"SLOT-1-6,MN,UPGRDPROG,NSA,2004-02-03,07-20-54,,,,,\"Pack Upgrade In
Progress.\",,,,,,"
[BTI7000] [REPT-ALM-EQPT] [43986-39345] [2004-02-03] [07:23:42]
"SLOT-1-6,CL,UPGRDPROG,NSA,2004-02-03,07-20-54,,,,,\"Clear Pack Upgrade
In Progress.\",,,,
,,,"
[BTI7000] [REPT-ALM-EQPT] [43987-39346] [2004-02-03] [07:23:44]
"SLOT-1-6,MN,REPLUNITFAIL,NSA,2004-02-03,07-23-43,,,,,\"Equipment
failure.\",,,,,,"
[BTI7000] [REPT-ALM-EQPT] [44054-39347] [2004-02-03] [07:43:39]
"SLOT-1-6,CL,REPLUNITFAIL,NSA,2004-02-03,07-43-39,,,,,\"Clear equipment
failure.\",,,,,,"
*/
>
BTI7000 04-02-05 13:04:48
M 100 COMPLD;
```

## 6.1.2 Stopping log recording

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

To stop log recording, use the following TL1 command:

```
STP-LOG:[TID]:[<aid>]:[CTAG]::<lognm>;
```

### Example command

```
STP-LOG:BTI7000::100::ALM;
```



**Note** The STP-LOG command only applies to the specified log category. If ALL is specified, log recording for categories except Security is stopped.

### 6.1.3 Starting log recording

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

To start log recording, use the following TL1 command:

```
STA-LOG:[TID]:[<aid>]:[CTAG]::<lognm>;
```

#### Example command

```
STA-LOG:BTI7000::100::ALM;
```

### 6.1.4 Initializing logs

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

To initialize log recording (that is, reset the category log identifier for the specified log category to 1), use the following TL1 command:

```
INIT-LOG:[TID]:[<aid>]:[CTAG]::<lognm>;
```

**Note** The Security log category cannot be initialized.

#### Example command

```
INIT-LOG:BTI7000::100::ALM;
```

### 6.1.5 Retrieving log attributes

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

To retrieve the attributes for a log category, such as on/off status of the log category and the number of permissible logs, use the following TL1 command:

```
RTRV-ATTR-LOG:[TID]:[<lognm>]:[CTAG]:;;
```

#### Example command and response

```
RTRV-ATTR-LOG:BTI7000::100::;
```

```
BTI700010-11-05 15:00:04
M 100 COMPLD
  "ALM, ON, 1000"
  "CMD, ON, 1000"
  "EVT, ON, 1000"
  "DBCHG, ON, 1000";
```

## 6.2 Security log

Security log attributes indicate the on/off status of the log category, the number of permissible logs, and the message a user sees when connecting to the system. These attributes can be retrieved, and when necessary, the connection message can be added or modified.

This section covers the following topics:

- 6.2.1, “Retrieving Security log attributes”
- 6.2.2, “Setting Security log attributes”

### 6.2.1 Retrieving Security log attributes

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

To retrieve Security log attributes, use the following TL1 command:

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

#### Example command and response

```
RTRV-ATTR-SECULOG:BTI7000::100::;
```

```
BTI7000 02-11-05 15:00:03
M 100 COMPLD
"SECU, ON, 1000"
/* "NOTICE: This is a private computer system. Unauthorized access or use
may lead to prosecution."
*/
;
```

### 6.2.2 Setting Security log attributes

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

To set Security log attributes, use the following TL1 command:

```
SET-ATTR-SECULOG:[TID]:[<aid>]:[CTAG]:::[WARN=<warning>];
```

#### Example command

```
SET-ATTR-SECULOG:BTI7000::100:::WARN="NOTICE: This is a private computer
system. Unauthorized access or use may lead to prosecution.";
```



## 7.0 Security management

---

- 7.1, “Security user profiles and authorization levels”
- 7.2, “User IDs and password identifiers”
- 7.3, “Creating a user profile”
- 7.4, “Editing a user profile”
- 7.5, “Changing your password”
- 7.6, “Deleting a user profile”
- 7.7, “Inhibiting a user profile”
- 7.8, “Allowing a user profile”
- 7.9, “Retrieving a list of active users”
- 7.11, “Authentication”
- 7.12, “Provisioning authentication”

## 7.1 Security user profiles and authorization levels

---

The system supports a maximum of 500 user profiles, which can be created using the TL1, CLI, or proNX 900 interface, or any combination of these interfaces.

Each user profile, Superuser, Provisioning, Maintenance, and Surveillance, requires a user identifier and password for authentication purposes. For information, see [7.2, “User IDs and password identifiers”](#).

User profiles are associated with standard operator security authorization levels defined in Telcordia TR-NWT-835, as described in the following table.

**Table 7-1 Authorization levels**

| Authorization Level | Access Rights   | Default Timeout |
|---------------------|---|-----------------|
| Superuser           | Full access to all system operations  | 15 minutes      |
| Provisioning        | Full access to all system operations except security operations             | 30 minutes      |
| Maintenance         | Access to system operations except the provisioning and security operations | 45 minutes      |
| Surveillance        | Read only access  | unlimited       |

### Superuser profile

The system has a default Superuser profile whose userid is “admin” and password is “admin”. This profile permits initial connectivity to the system. BTI recommends creating a new Superuser profile and then deleting or disabling the default profile.

The system prevents the editing, disabling, and deleting of the last Superuser profile to ensure that there is always an account with full system access available. The only parameter of the last Superuser profile that can be modified is the password identifier.

## 7.2 User IDs and password identifiers

---

The user identifier (UID) associated with a user profile must contain one to 10 case-sensitive alphanumeric characters. The password identifier (PID) associated with a user profile must contain six to 10 alphanumeric characters.

All special characters are supported for passwords except the following: - = ; : ‘ “ , ? Also, a profile's UID and its PID must not match. For example, the UID “George6” cannot have a PID of “George6”.

BTI recommends changing the default password of the default Superuser profile (default UID = “admin”; default PID = “admin”), after it is used to log on to the system for the first time.

Although the default password for the system contains five characters, the new PID must contain six to 10 characters.

|             |   |
|-------------|---|
| <b>Note</b> | Changes made to any profile are not applicable to the active session. They take effect once a user disconnects and then reconnects to the system. |
|-------------|---|

## 7.3 Creating a user profile

---

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

To create a user profile, use the following TL1 command:

```
ENT-USER-SECU:[TID]:<uid>:[CTAG]::<pid>,,<uap>:[TIMEOUT=<timeout>];
```

### Example command

```
ENT-USER-SECU:BTI7000:james:100::october,,supuser:TIMEOUT=15;
```



## 7.4 Editing a user profile

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

To edit a user profile, use the following TL1 command:

```
ED-USER-SECU:[TID]:<uid>:[CTAG]::[<nuid>],[<pid>],,[<uap>]:  
[TIMEOUT=<timeout>];
```

### Example command

```
ED-USER-SECU:BTI7000:james:100::,city23,:TIMEOUT=60;
```

## 7.5 Changing your password

---

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

To change the password of your user profile, use the following TL1 command:

```
ED-PID:[TID]:<uid>:[CTAG]::<oldpid>,<newpid>;
```

### Example command

```
ED-PID:BTI7000:james:100::city23,mainstn;
```

**Note** The new password comes into effect after you log out of the current session.

## 7.6 Deleting a user profile

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

To delete a user profile, enter the following at the TL1 command line interface:

```
DLT-USER-SECU:[TID]:<uid>:[CTAG];
```

### Example command

```
DLT-USER-SECU:BTI7000:james:100::;
```

**Note** If the deleted profile is an active session, the session remains in effect until the user logs out.

## 7.7 Inhibiting a user profile

---

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

To inhibit a user profile, use the following TL1 command:

```
INH-USER-SECU:[TID]:<uid>:[CTAG];
```

### Example command

```
INH-USER-SECU:BTI7000:danny:100::;
```

## 7.8 Allowing a user profile

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

To allow a user profile, use the following TL1 command:

```
ALW-USER-SECU:[TID]:<uid>:[CTAG];
```

### Example command

```
ALW-USER-SECU:BTI7000:danny:100::;
```

## 7.9 Retrieving a list of active users

---

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

To retrieve a list of active users, use the following TL1 command:

```
RTRV-ACT-USER:[TID]::[CTAG]::;
```

### Example command and response

```
RTRV-ACT-USER:BTI7000::100;
```

```
BTI7000 03-09-29 10:29:39
M 100 COMPLD
admin:SUPERUSER:192.168.172.163:3083
;
```

---

## 7.10 Retrieving your security credentials

---

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

To retrieve your security credentials, use the following TL1 command:

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

### Example command and response

```
RTRV-USER:BTI7000::;
```

```
BTI7000 05-03-16 14:47:57
```

```
M 110 COMPLD
```

```
admin: SUPERUSER: TIMEOUT=5, STATUS=IS
```

```
;
```

## 7.11 Authentication

The BTI 7000 Series supports local authentication and remote RADIUS authentication.

### Local authentication

Local authentication performs user authentication at each BTI 7000 Series node, separately. The user supplies a username and password that is sent to the system's server. A centralized server is not used for local authentication.

### Remote RADIUS authentication

Remote RADIUS authentication performs user authentication through an external RADIUS server, to facilitate the exchange of user credentials between the client and an external RADIUS server. The external RADIUS server can reside on a BTI 7000 Series, or on a third-party server. RADIUS is disabled by default.

**Note** The BTI 7000 Series RADIUS client does not support session accounting.

The RADIUS authentication exchange occurs only at user login. The status of the RADIUS server is not maintained and not known until the next login attempt. This means that the current login session is not impacted by changes to the availability or configuration of the external server, which may occur during the current login session.

If firewall traversal is required, then the firewall must be configured to allow RADIUS traffic. The default port for RADIUS traffic is 1812.

The BTI 7000 Series supports the following RADIUS packet types and attributes, according to RFC 2865:

| Packet type   | Attribute         | Description  |
|---|-------------------|--|
| <b>ACCESS-REQUEST</b> - Sent by the BTI 7000 Series remote client to the external RADIUS server to request authentication.  | User-Name         | User's login userid.   |
|   | User-Password     | User's login password.   |
|   | Called-Station-Id | Set to "BTI:7000."   |
|   | Service-Type      | Set to "Login."  |
|   | NAS-Identifier    | Set to the node's TID.   |
|   | NAS-Port          | Set to zero.   |
|   | NAS-IP-Address    | Set to the IPv4 address of the interface used to send the request.   |
| <b>ACCESS-ACCEPT</b> - Sent by the external RADIUS server to the BTI 7000 Series. This response message must be received by the remote client to allow the client user login. | Reply-Message     | Must be present. Determines the privilege level of the user. Contains one of "Superuser," "Provisioning," "Maintenance," or "Surveillance."                              |
|   | Idle-timeout      | Must be present. Determines the inactivity timeout of the user. Valid ranges are: <ul style="list-style-type: none"><li>Zero: Disabled</li><li>5 to 60 minutes</li></ul> |



## Remote RADIUS configuration

When configured for remote authentication, the BTI 7000 Series acts as a network access server (NAS). Authentication credentials are encrypted using a “shared secret” that is known to both the client and the server. When a user attempts to login, the client provides encrypted user credentials to the external RADIUS server. The external server determines the access service that the client is authorized to use, and provides information to the to facilitate the specific access service to be used.

Up to three authentication servers can be configured—a primary, an optional secondary, and an optional tertiary server:

- If a secondary server is configured, the authentication request is sent to the secondary if the primary server does not respond.
- If a tertiary server is configured, the authentication request is sent to the tertiary if the primary and secondary servers cannot be reached.
- If the primary server responds but fails to authenticate the user, the request is not sent to the secondary or tertiary servers.

## External RADIUS server configuration

The external RADIUS server must be configured to accept authentication requests from each BTI 7000 Series Network Element with matching Server Authentication Keys (shared secret). The external server can identify BTI 7000 Series originated requests based on the Called-Station-Id attribute.

The authentication dictionary must contain the following entries for a BTI 7000 Series client to successfully authenticate, in accordance with RFC 2865:

| RADIUS Attribute | Content   |
|------------------|---|
| User-Name        | User ID of the user described by the entry.   |
| User-Password    | Password of the user described by the entry.  |
| Reply-Message    | Authorization level. Must contain one of “Superuser,” “Provisioning,” “Maintenance,” or “Surveillance.”   |
| Idle-timeout     | Must be present. Determines the inactivity timeout of the user. Valid ranges are: <ul style="list-style-type: none"> <li>• Zero: Disabled</li> <li>• 5 to 60 seconds</li> </ul> |

**Note** If you are using the proNX Service Manager as the external RADIUS server, refer to the *proNX Service Manager; Installation Guide* for procedures on configuring the PSM as an external RADIUS server.

## 7.12 Provisioning authentication

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

The following table describes the parameters for provisioning local and remote RADIUS authentication. Local authentication administers a single (local) node. Remote RADIUS authentication can administer many nodes.

**Table 7-2 Provision Authentication Servers dialogue**

| Parameter                      | Description  | Values   |
|--------------------------------|--|--|
| <b>Authentication Priority</b> | Determines what type of authentication to use.   | <p>Disabled: Only local authentication is used.</p> <p>Local: Local authentication is tried first. If that fails RADIUS authentication is tried.</p> <p>Remote: RADIUS authentication is tried first. If that fails local authentication is tried.</p> |
| <b>Server IP Address</b>       | Required. The IP address that points to an authentication server.  | Valid IPv4 address.  |
| <b>Port</b>                    | The port value of the external RADIUS server.  | Default setting is 1812. The value must be an integer between 1 and 65535.   |
| <b>Role</b>                    | Sets the role of the external RADIUS server.   | Disabled, Primary, Secondary, Tertiary   |
| <b>Timeout</b>                 | Determines, in seconds, how long the client server waits for a response from the authentication server, before sending another request to the authentication server.   | <p>1 to 10 seconds</p> <p>The default setting is 5 seconds.</p>  |
| <b>Retries</b>                 | The number of attempts to contact an authentication server before attempting to contact the next configured server.  | <p>1 to 5 attempts</p> <p>The default setting is 1 attempt.</p>  |
| <b>Key</b>                     | <p>The Key value must be 6-256 case-sensitive alphanumeric characters. The following special characters are supported:</p> <p>! @ # \$ % ^ &amp; * ( ) _ + - = { }   [ ] ' &lt; &gt; / ~ `</p> <p>The following special characters are not supported for TL1: : ; , ?</p> <p>The following special characters are not supported for CLI: \ ! " ?</p> | <p>Default or user defined</p> <p><b>Note</b></p> <p>The key on the client and server must match.</p>  |

### Guideline

Following are provisioning guidelines to consider:

- Provisioning a secondary and tertiary authentication server is optional.

- You can provision the authentication servers independent from each other, so that a server can be taken off-line without a change to the other servers' configurations.

Follow these steps to provision an authentication server.

**Step 1** Click the **System Configuration** icon, right-click on the system you are provisioning, and click **Provision Authentication Servers**.

The **Provision Authentication Servers** dialog displays.

**Step 2** From the **Authentication Priority** pull-down menu, select the type of authentication to use.

**Provision Authentication Servers**

Authentication Priority: Disabled ▼

Configured Servers

| IP Address |          | Port | Timeout | Retry |
|------------|----------|------|---------|-------|
| 10.1.0.0   | Disabled | 1812 | 7       | 1     |
| 12.0.0.0   | Disabled | 1812 | 5       | 1     |

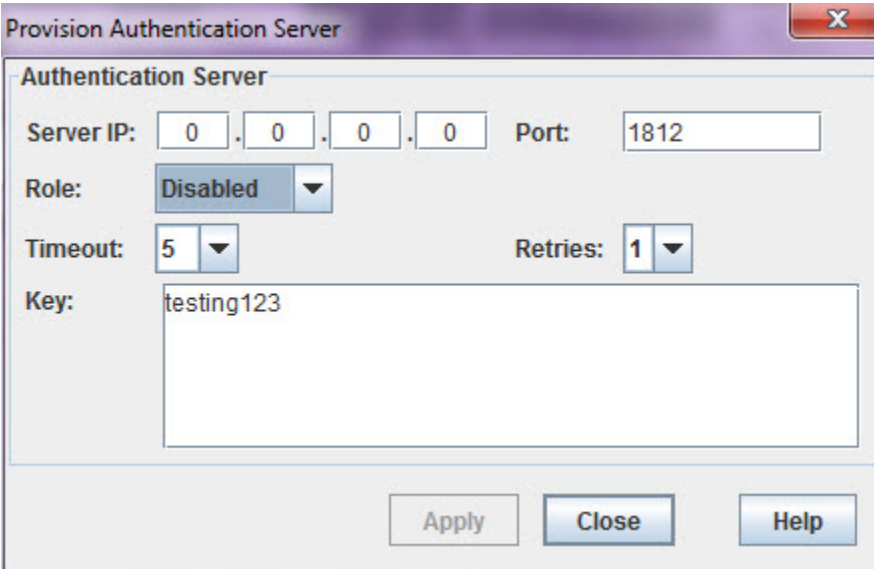
Add Edit Delete

Apply Close Help

The **Configured Servers** table lists the existing authentication servers.

**Step 3** Click **Add**. The **Provision Authentication Server** dialog displays.

**Step 4** Configure the server.



The image shows a Windows-style dialog box titled "Provision Authentication Server". It contains a section titled "Authentication Server" with the following fields: "Server IP" with four input boxes each containing "0", "Port" with a text box containing "1812", "Role" with a dropdown menu showing "Disabled", "Timeout" with a dropdown menu showing "5", and "Retries" with a dropdown menu showing "1". Below these is a "Key" label followed by a large text area containing "testing123". At the bottom right are three buttons: "Apply", "Close", and "Help".

**Step 5** Click **Apply**. Click **Close**.

You are returned to the **Provision Authentication Servers** dialog. The new server appears in the **Configured Servers** table.

You have successfully completed this procedure.

## 8.0 Working with the database

---

- 8.1, “About the database”
- 8.2, “Impact of module replacement on the database”
- 8.3, “Recommendations when replacing modules”
- 8.4, “Database backup, restore, and delete”
- 8.5, “Preconfigured SCP scenarios”
- 8.6, “Replacing a failed SCP or module”

## 8.1 About the database

---

All configuration data is stored in a non-volatile database on the System Control Processor (SCP). This includes the following information:

- System identifier (SID)
- Internet protocol (IP) addresses
- Amplifier settings (such as, gain, power, etc.)
- Transponder, Muxponder, and packetVX module settings
- Log files
- Simple Network Management Protocol (SNMP) settings
- User IDs and passwords

A complete copy of the database is backed up to volatile memory on every active module in the system. The database on the expansion shelf interface (ESI) of each expansion shelf in the system is also backed up.

When a replacement SCP is inserted into an active system, it automatically acquires the database from the active modules. If no active modules are available, the SCP uses its non-volatile database.

### Database backup caveats

- The database is not backed up to filler and passive modules.
- The database is not backed up to intelligent modules in expansion shelves.

## 8.2 Impact of module replacement on the database

The following table lists the impact of module replacement on the configuration database.

| Module   | Removal  | Insertion  |
|--|--|--|
| System Control Processor   | Do not remove the SCP for at least 60 seconds after the last TL1 command is entered.   | The SCP acquires the database from active modules.   |
| Main Shelf Interface (MSI)   | When the MSI is removed, the SCP loses communications to all circuit packs and backups cannot be supported.  | The database is backed up to each newly inserted active module after its software is upgraded. |
| Cooling Unit   | No impact. Cooling unit is not involved in the backup process.   | No impact. Cooling unit is not involved in the backup process.                                 |
| Active modules (e.g., Optical Amplifiers, Transponders, Muxponders, packetVX modules)                                  | Can be removed if there is at least one other active module left in the system.<br><br><b>Note</b><br>Backups of the database are stored in volatile memory and are lost once an active module is removed. | The database is backed up to active module after its software is upgraded.                     |
| Passive modules<br>(such as, dispersion compensation modules, optical add-drop modules and multiplexer/demultiplexers) | No impact. Passive modules are not involved in the backup process.   | No impact. Passive modules are not involved in the backup process.                             |

## 8.3 Recommendations when replacing modules

---

- When replacing the SCP, ensure that one active module remains in the shelf.
- When replacing both the SCP and the MSI, ensure that the MSI is replaced first.
- When replacing the SCP in a shelf populated with only passive modules, do the following:
  - 1 Perform a database backup through the FTP server.
  - 2 Replace the SCP.
  - 3 Re-enter IP addresses (otherwise, the SCP starts with the default IP addresses).
  - 4 Restore the database through the FTP server.



## 8.4 Database backup, restore, and delete

The SCP maintains all provisionable data in non-volatile storage so that configuration settings are retained during system shutdowns and restarts. The configuration database is version controlled to facilitate the detection of an incompatible software load and/or database.

The system supports user-initiated backup of the configuration database. The database is uploaded to a user-specified network location (that is, a local PC or a remote PC) using the file transfer protocol (FTP), or it is stored locally on the SCP.

The system also supports user-initiated restore of the configuration database. The database is restored using a version of the file from an FTP server or locally from the SCP. The integrity of the file is validated to ensure that it matches the current software load.

If required, the database can be deleted and the factory-default (empty) database restored.

This section covers the following topics:

- 8.4.1, “Backing up the database to an FTP server”
- 8.4.2, “Manual backup processes”
- 8.4.3, “Restoring the database”
- 8.4.4, “Automatic restore process”
- 8.4.5, “Deleting the database”

### 8.4.1 Backing up the database to an FTP server

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

#### Prerequisite

The FTP server must be set up for remote backups.

**Caution** BTI recommends you clear any alarms on the system before you backup a database.

#### Step 1 Check the available space on the FTP Server

If you intend to perform an FTP backup, confirm that the FTP server has at least the following amounts of free space:

- Main shelf only: 1 MB of free space
- Main shelf and expansion shelves: 2 MB of free space

#### Step 2 Invoke the backup process

Entering the following TL1 command:

```
INVK-DB-BKUP:[TID]::<CTAG>::TYPE=<type>,[IPADDR=<ipaddr>],
[PATH=<path>],[USERID=<userid>],[PWD=<pwd>],[CHKALM=<chkalm>];
```

where

`type` is either `FTP` or `SCP`.

`ipaddr` is the IP address of where the backup file is going to be stored (if doing an `FTP` backup).

`path` is the path to the directory where the backup file is to be stored. If `TYPE=FTP`, then the path must end with a slash (/).

`userid` is the user identifier.

`pwd` is the password.

`chkalm` is either `Y` or `N` for checking the status of alarms.

For added protection, backup the database both locally on the `SCP` and remotely through `FTP`.

**Note** The maximum path length is 54 alphanumeric characters when `TYPE=FTP` and 48 alphanumeric characters when `TYPE=SCP`. Some UNIX systems may require that the entire directory path and backup file name must be entered for the `path` field.

The system defaults to the following format for the backup file name: `BTI 7000 Series_<NENName>_<MONTH><DAY>_<YEAR>`.

**Note** If the `CHKALM` value is set to `Y`, then for the file name to function correctly one or more alphabetic characters and the underscore must precede the `NENName` field.

The system returns the following message:

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

You have successfully completed this procedure.

## 8.4.2 Manual backup processes

The following table describes the supported manual backup processes.

| Backup process | Description  |
|----------------|--|
| Local SCP      | A local backup stored on the <code>SCP</code> consists of one backup file that is overwritten by new backups files. When a local backup occurs, it triggers immediate backups to the active modules in the system. |

| Backup process | Description  |
|----------------|--|
| Local PC FTP   | A local FTP backup is stored on a connected PC that acts as an FTP server. |
| Remote PC FTP  | A remote FTP backup is stored on an FTP server.                            |

**Note** For manual backups to occur, there should be no alarms present on the system. Although, an alarm override is available, its use is usually not recommended.

### 8.4.3 Restoring the database

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 8.4.5, “Deleting the database”.

**Note** 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.

**Important** Equipment provisioning cannot be performed during a database restore operation.

**Warning** 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

**Note** The value <PATH> can contain a maximum of 54 alphanumeric characters when TYPE=FTP 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

<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.

## 8.4.4 Automatic restore process

The system supports the following automatic restore processes:

- System running current software, replace SCP with a unit loaded with the current software
- System running current software, replace SCP with a unit loaded with an earlier or later software load
- System running current software, cycle power

### System running current software, replace SCP with a unit loaded with the current software

- 1 While the SCP is starting, it queries all active modules for database revisions.
- 2 Selects the database from the pack with the latest revision.
- 3 Performs a database integrity check.
- 4 Uses the database if the integrity check passes. Otherwise, the SCP selects another database and raises the “DB recovery failure” alarm if all checks fail.
- 5 Increments the revision and backs-up the database to all active modules.

### System running current software, replace SCP with a unit loaded with an earlier or later software load

- 1 The “Release number mismatch” alarm is raised.
- 2 The SCP uses the database with factory default settings.
- 3 The SCP can be brought to current software release by loading the correct software through the FTP server and issuing the INVK-SCP-RELNUM command.
- 4 The SCP restarts following the previous restore process:
  - 1 While the SCP is starting, it queries all active modules for database revisions.
  - 2 Selects the database from the pack with the latest revision.
  - 3 Performs a database integrity check.
  - 4 Uses the database if the integrity check passes. Otherwise, the SCP selects another database and raises the “DB recovery failure” alarm if all checks fail.
  - 5 Increments the revision and backs-up the database to all active modules.

### System running current software, cycle power

- 1 While the SCP is starting, it queries all active modules for database revisions.
- 2 The modules do not have databases as this is stored in volatile memory.
- 3 The SCP uses its own database and will backup to all of the active modules.

## 8.4.5 Deleting the database

Use this procedure to delete the configuration database and return to the factory-default database.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

### Prerequisites

- All alarms on the system have been cleared.

**Important** If you are deleting the database as part of a software downgrade, use the procedure "Downgrading the system software using TL1" in the *BTI 7000 Series Upgrade Guide*. Do not use this procedure to downgrade system software.

**Important** Equipment provisioning cannot be performed during a database delete operation.

**Caution** Do not insert or remove any replaceable unit, i.e., modules, transceivers, expansion shelves, and common equipment, during a database delete operation unless instructed to do so.

### Deleting the database

Follow these steps to delete the configuration database.

**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 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 syntax at the TL1 command line interface:

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

where

<CHKALM> is Y or N

For example,

```
BTI7000>
```

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

The system returns the following message:

```
BTI7000 08-11-14 23:49:45
M 100 COMPLD
;
BTI7000>

BTI7000 08-11-14 23:49:46
** 2 REPT ALM EQPT
"SCP-1-5:MJ,DBDLTPROG,NSA,11-14,23-49-45,,,,,:\"Database Delete In Progress.\",,,,;"
;

BTI7000 08-11-14 23:49:50
A 3 REPT EVT EQPT
"SCP-1-5:INVKDBDLTPASS,,11-14,23-49-45,,,,,:\"INVK-DB-DLT pass. Config may be viewed
on SCP.\",,,,;"
;
```

**Step 3** Do one of the following:

a) To cancel the database delete operation and recover the existing configuration database, enter the following at the TL1 command line interface:

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

For example,



BTI7000>

CANC-DB-DLT:BTI7000::100::;

The system returns the following message:

BTI7000 08-11-14 17:35:09

M 100 COMPLD

;

BTI7000>

BTI7000>

BTI7000 08-11-14 17:35:12

A 4 REPT DBCHG

"TIME=17-35-12,DATE=08-11-14,SOURCE=0000,DBCHGSEQ=0:ED-IP:IP-NMS:::IS-NR,"

;

BTI7000 08-11-14 17:35:12

A 5 REPT DBCHG

"TIME=17-35-12,DATE=08-11-14,SOURCE=0000,DBCHGSEQ=1:ED-IP:IP-CRAFT:::IS-NR,"

;

BTI7000 08-11-14 17:35:14

A 6 REPT ALM EQPT

"SCP-1-5:CL,DBDLTPROG,NSA,11-14,17-34-42,,,,,:\"Clear Database Delete In Progress.\",,,:,"

;

- b)** To commit the database delete operation, enter the following at the TL1 command line interface:

CMMT-DB-DLT:[TID]::<CTAG>::;

For example,

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

The system returns the following message:

BTI7000 08-11-14 17:54:03

M 100 COMPLD

;

BTI7000>

BTI7000>

BTI7000 08-11-14 17:54:06

A 3 REPT ALM EQPT

"SCP-1-5:CL,DBDLTPROG,NSA,11-14,17-46-06,,,,,:\"Clear Database Delete In Progress.\",,,:,"

;

**Important** When the commit operation is completed, restart the SCP.

- Step 4** Log back into the system. Reconnect via the local Craft port using the factory-default communications settings.
- Step 5** 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 6** 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.

## 8.5 Preconfigured SCP scenarios

In some cases, it can be useful to pre-configure an SCP with all the provisioning information and then have the provisioning data automatically sent to each active module in the system. This procedure only works in the following scenarios.

The following table describes preconfigured SCP scenarios.

| Scenario  | Description  |
|---|--|
| Provision the SCP in Shelf 1, and then insert the modules in Shelf 1.   | The system automatically provisions the inserted modules using the database on the SCP.  |
| Provision the SCP in Shelf 1, move the SCP to Shelf 2, which is unequipped, and then insert the modules in Shelf 2. | The system automatically provisions the inserted active modules using the database on the SCP.   |
| Provision the SCP in Shelf 1, move the SCP to Shelf 2, which is equipped with modules.                              | <p>If the shelf never had an SCP or the shelf was power cycled, the system automatically provisions the active modules using the database on the SCP.</p> <p>If the shelf had an SCP at one time, the new SCP acquires the database from the active modules.</p> |

## 8.6 Replacing a failed SCP or module

---

Under normal circumstances, a new SCP acquires the database from the active modules in the shelf; however, a Database Recovery Failure alarm can occur. If this alarm occurs, do one of the following:

- If the database was backed up to a remote FTP, restore the database from the FTP server.
- Provision an SCP on another shelf, perform a remote backup to an FTP server, and then restore the database.
- Provision an SCP on another shelf, perform a local backup, replace the SCP, and then restore the database using the local backup file.
- If working in a lab situation, power cycle the shelf and re-enter the provisioning data.

When a failed module is replaced, the replacement module is automatically provisioned using the database on the SCP.





*Part Number:*  
*Document Version:*  
*Published:*  
*Type:*

*BT7A73FA*  
*01*  
*March 2017*  
*STANDARD*

*product release 13.5*