



PRODUCT DOCUMENTATION

BTI 7000 Series SNMP Overview Guide

Part Number: BT7A74AA
Document Version: 01
Published: March 2017
Type: STANDARD

product release 13.5

Contents

Preface	v
1.0 SNMP overview	1-1
1.1 About SNMP	1-2
1.2 UDP ports for SNMP	1-4
1.3 Supported SNMP operations	1-5
1.4 Usage guidelines	1-6
1.5 MIB requirements	1-7
1.5.1 MIB-II object hierarchy	1-8
1.6 Special characters	1-10
1.7 Updates to the MIBs in this release	1-11
2.0 Provisioning SNMP	2-1
2.1 About community strings	2-2
2.1.1 Provisioning community strings	2-2
2.1.2 Deleting community strings	2-3
2.1.3 Related TL1 commands for provisioning community strings	2-3
2.2 About trap receivers	2-4
2.2.1 Provisioning trap receivers	2-4
2.2.2 Deleting trap receivers	2-5
2.2.3 Related TL1 commands for provisioning trap receivers	2-5
3.0 Protection group pairs	3-1
3.1 Protection groups	3-2
3.2 Protection Group Pair Objects	3-3

4.0 Fault and event management	4-1
4.1 Trap support in SNMP	4-2
4.2 Viewing standing conditions	4-3
4.3 Decoding trap events	4-5
5.0 Performance monitoring	5-1
5.1 PM support in SNMP	5-2
5.1.1 Organization of PM table indices, values, and qualifiers	5-2

Preface

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

Audience

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

Features of the BTI 7000 Series

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

BTI 7000 Series common equipment

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

BTI 7000 Series common equipment

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

BTI 7000 Series common equipment (Continued)

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

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

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

Management software suite

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

Equipment compliance

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




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

Organization of the BTI 7000 Series documentation

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

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

Documentation conventions

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

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

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

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

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

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

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

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

Copyright 1990-2001 Sleepycat Software. All rights reserved.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1.0 SNMP overview

This section describes the Simple Network Management Protocol (SNMP) implementation on the BTI 7000 Series.

This contains the following:

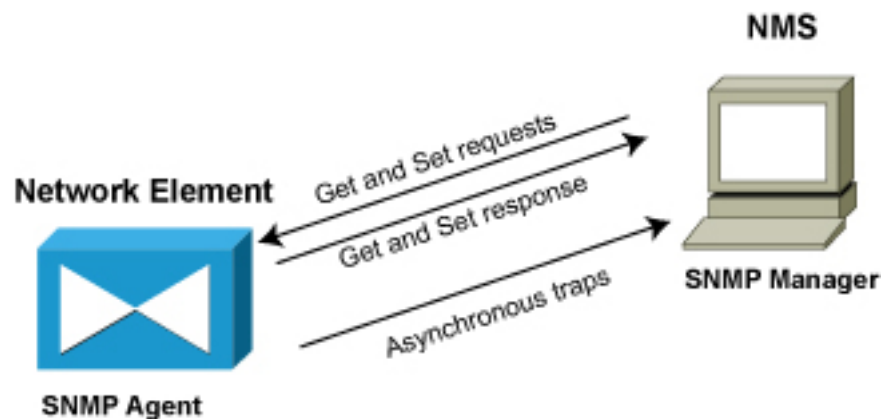
- 1.1, “About SNMP”
- 1.2, “UDP ports for SNMP”
- 1.3, “Supported SNMP operations”
- 1.4, “Usage guidelines”
- 1.5, “MIB requirements”
- 1.6, “Special characters”
- 1.7, “Updates to the MIBs in this release”

1.1 About SNMP

The *Simple Network Management Protocol* (SNMP) is an application-layer protocol designed to facilitate the exchange of management information between network devices and management stations. SNMP enables setting and retrieving configuration and status information on devices as well as trap-directed notification of events on a device.

The following figure shows the interaction between the NMS and the BTI 7000 Series using SNMP.

Figure 1-1 SNMP connectivity



Note Use either the NMS or Craft Ethernet ports on the BTI 7000 Series to communicate with the SNMP agent.

BTI's SNMP implementation supports SNMP Version 1 (SNMPv1) as defined in RFCs 1155, 1157, 1212, 1213, and 1215. The SNMP implementation also supports SNMPv2c as defined in RFCs 1901 through 1907. SNMPv3 protocol data unit messages are also supported.

Enterprise MIBs, as provided on the Customer Documentation CD, define product-specific MIB objects and notifications. These MIBs are available in both SNMPv1 and SNMPv2 versions.

The *system* and *snmp* group objects in MIB-II, as defined in RFC 1213, are supported for both read and write access. In addition, the MIB includes a group of system-related objects under the *networkElement* branch.

The enterprise MIB provides full support for all management functions available on the system.

BTI SNMP enables:

- retrieval of system inventory information
- provisioning of equipment, facilities and services
- monitoring of faults through trap-based alarm notification and retrieval of active alarms and conditions
- retrieval of performance monitoring data and trap-based PM threshold crossing alerts

- administration management functions including software upgrades and database backup and restore

For more information on required MIBs for SNMPv1 and SNMPv2, see section [1.5, “MIB requirements”](#).

OSS integration

BTI can provide customers with direct access to network element SNMP MIBs for use for integration to OSS systems. Customers must note the following caveats:

- **Performance:** The MIBS are performance tested for use with the proNX 900 Node Controller proNX 9000 Network Manager tool. Customers are responsible for conducting their own testing to ensure that the NE interfaces meet the needs of their proposed usage. BTI makes no guarantees that any proposed usage will meet customer requirements.
- **Changes between releases:** SNMP MIBs are subject to change as support for new functionality is introduced. BTI strives to maintain backward compatibility of MIBs across releases but this is not guaranteed and BTI reserves the right to deprecate or remove support for obsolete MIB elements. OSS integrators must be careful not to rely on functionality that is marked as deprecated as it may be unsupported in a subsequent release. Customers that integrate directly to the MIBs are responsible for all OSS development and integration testing that may arise from MIB changes between releases of BTI software.

1.2 UDP ports for SNMP

The following table lists and describes the User Datagram Protocol (UDP) ports used by the BTI SNMP agent.

Table 1-1 UDP ports

Port number	Description
162	Default port used by the SNMP agent as the destination to which to send traps.
161	The port on which the BTI 7000 Series SNMP Agent listens for SNMP Get/Set requests.

Note The SNMP trap port number can be specified by the user rather than using the default 162 port. For environments where Network Address Translation or Firewalls, for example, may be in use.

1.3 Supported SNMP operations

The following request/response operations and messages are supported by the SNMP agent:

- *Get* — Allows the SNMP manager to retrieve one or more specific object values (on a device) from the SNMP agent. BTI's SNMP supports the use of the *Get* operation to retrieve objects with read access.
- *GetNext* — Allows the SNMP manager to retrieve the next object instance in lexicographical order relative to a specified object. When an SNMP manager wants to “walk” through all elements of a table on an agent, it performs a series of *GetNext* operations using the last returned object as the argument for the succeeding *GetNext* operation.
- *GetBulk* — Allows the SNMP manager to retrieve multiple rows of tabular objects in a single operation.
- *Set* — Allows the SNMP manager to send one or more specific object values to the SNMP agent. BTI's SNMP supports the use of the *Set* operation to create and delete table entries.
- *Trap* — Used by the agent to asynchronously notify the SNMP manager of an event.
- *Inform* — Traps sent by the agent for which acknowledgement is sent back.

When responding to a *Get*, *GetNext* or *GetBulk* request, the SNMP agent retrieves the value of the requested MIB object and responds to the SNMP manager with that value. Multiple values can be requested at the same time.

1.4 Usage guidelines

Use the *Get*, *GetNext* or *GetBulk* operations to read MIB objects, using a community string with read-only or read-write access.

Set time outs on *Get* requests to at least 10 seconds. If regularly polling objects on the SNMP interface, use a polling frequency no greater than once every 10 seconds.

Use the *Set* operation to edit existing object values or to create or delete table entries, using a community string with read-write access.

The creation and deletion of table entries is governed by the use of RowStatus valued objects, which are contained in every table that supports creation and deletion. The RowStatus textual convention is defined in RFC 1903.

RowStatus objects support only the following values:

- *active* (to return a value when an object is read)
- *createAndGo* (to create a table entry)
- *destroy* (to delete a table entry).

Set requests only support setting objects in the same group or in the same row of a table. For example, it is not possible to set an object in the networkElement group in the same set request as editing an optical amplifier object, nor is it possible to edit optical amplifier objects in different rows of the oaTable.

1.5 MIB requirements

The following sections list the MIBs required to configure an SNMP Management station to manage a BTI 7000 Series systems using either SNMPv1 or SNMPv2 MIBs:

Important The MIB files for either SNMPv1 or SNMPv2 must be loaded into the SNMP Manager applications in the order listed in the following sections, but not both sets.

MIB requirements for SNMPv1

MIBs in SNMPv1 format are compatible with the specifications for SNMPv1 MIBs as defined by the following documents:

- RFC 1155 - *Structure and Identification of Management Information for TCP/IP-based Internets*
- RFC 1212 - *Concise MIB Definitions*
- RFC 1215 - *A Convention for Defining Traps for use with the SNMP*

For management of BTI BTI 7000 Series network elements using SNMPv1-compliant MIBs, the following enterprise MIBs must be loaded onto SNMP Manager applications in the order listed, except for bti-ol_v1.my and packetvx-bridge_v1.my which are optional and may be loaded in any order after bti7000_v1.my:

- BTI-MIB in the file 'bti-oid_v1.my'
- BTI-TC-MIB in the file 'bti-tc_v1.my'
- BTI-7000-MIB in the file 'bti7000_v1.my'
- BTI-OL-MIB in the file 'bti-ol_v1.my'
- BTI-PACKET-VX-BRIDGE-MIB in the file 'packetvx-bridge_v1.my'

Managing MIB-II functionality on the BTI 7000 Series (SNMPv1)

To manage MIB-II functionality on the BTI 7000 Series (optional), the management system must be loaded with the required MIB-II object definitions as provided in RFC 1213 - *Management Information Base for Network Management of TCP/IP-based Internets: MIB-II*.

Note All RFC documents are available from the Internet Engineering Task Force (IETF) at www.ietf.org.

MIB requirements for SNMPv2

MIBs in SNMPv2 format are compatible with the specifications for SNMPv2 MIBs as defined by the following documents:

- RFC 1902 - *Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2)*

- RFC 1903 - *Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2)*

For management of network elements using SNMPv2-compliant MIBs, the following enterprise MIBs must be loaded onto SNMP Manager applications in the order listed, except for bti-ol.my and packetvx-bridge.my which are optional and may be loaded in any order after bti7000.my:

- BTI-MIB in the file 'bti-oid.my'
- BTI-TC-MIB in the file 'bti-tc.my'
- BTI-7000-MIB in the file 'bti7000.my'
- BTI-OL-MIB in the file 'bti-ol.my'
- BTI-PACKET-VX-BRIDGE-MIB in the file 'packetvx-bridge.my'

Managing MIB-II functionality the BTI 7000 Series (SNMPv2)

To manage MIB-II functionality on the BTI 7000 Series (optional), the management system must be loaded with the required MIB-II object definitions as provided in RFC 1907 - *Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)*.

Note	All RFC documents are available from the Internet Engineering Task Force (IETF) at www.ietf.org .
-------------	---

1.5.1 MIB-II object hierarchy

For SNMPv2, the SNMP agent supports the system and snmp object groups in MIB-II as defined by RFC 1907.

The following illustration shows the object hierarchy of the system group of objects supported in this release.

Figure 1-2 System group objects

```
internet
|
+--mgmt
|
+--mib-2
|
+--system
|
+--sysDescr
|
+--sysObjectID
|
+--sysUpTime
|
+--sysContact
|
```

```
+-sysName  
|  
+-sysLocation  
|  
+-sysServices
```

1.6 Special characters

In addition to the standard alphanumeric characters, the BTI 7000 Series supports the following special characters for SNMP:

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

Note When using “!” in a community string, a backslash “\” is required as an escape character, for example:

```
System1(config)# snmp community test\! access write
```

The following special characters are not supported for entry as special characters for the BTI 7000 Series:

" * , / : ; < > ? \ |

The @ symbol can be used as a separator in some passwords as follows:
<userid>:<password>@<IP address>. However, some FTP servers cannot handle the @ symbol, and its use should be avoided in FTP passwords.

1.7 Updates to the MIBs in this release

The following sections list updates made to the MIBs in this release.

BTI-MIB in the file 'bti-oid.my'

No changes in this release.

BTI-TC-MIB in the file 'bti-tc.my'

Modified to support the new ODU1_AIS alarm for ODU1-OTU2 muxponder pass-through connections.

BTI-7000-MIB in the file 'bti7000.my'

Modified to support E-NNI and the new ODU1_AIS alarm for ODU1-OTU2 muxponder pass-through connections.

BTI-OL-MIB in the file 'bti-ol.my'

No changes in this release.

BTI-PACKET-VX-BRIDGE-MIB in the file 'packetvx-bridge.my'

Modified to support E-NNI.

2.0 Provisioning SNMP

This section describes how to configure the Simple Network Management Protocol (SNMP) implementation for the BTI 7000 Series.

- [2.1, “About community strings”](#)
- [2.2, “About trap receivers”](#)

Before you begin

Important You must install and provision the BTI 7000 Series before configuring SNMP. This includes configuring IP connectivity between the Network Management System (NMS) and the BTI 7000 Series. For complete installation, operation and provisioning instructions, consult the documentation included on the BTI 7000 Series documentation CD.

2.1 About community strings

SNMP community strings validate access to MIB objects and function as embedded passwords. Up to 30 community strings can be provisioned on the BTI 7000 Series to allow the user to perform *Get* and *Set* operations. Both SNMPv1, and SNMPv2c protocols are supported for any provisioned community string.

The SNMPv3 protocol is supported with the following restrictions:

- Only the noAuthNoPriv level of user-based security is supported.
- Packet Authentication and Privacy are not supported.

Any community string provisioned for SNMPv1 or SNMPv2c can also be used as an SNMPv3 user according to the user-based security model for noAuthNoPriv messaging.

Two community strings are provisioned by default on new installations of BTI 7000 Series NEs:

- public - for read-only access
- private - for read/write access

The following sections provide instructions on how to create and delete community strings on the BTI 7000 Series using the proNX 900:

- [2.1.1, “Provisioning community strings”](#)
- [2.1.2, “Deleting community strings”](#)

For details on using the TL1 command line, see section [2.1.3, “Related TL1 commands for provisioning community strings”](#).

2.1.1 Provisioning community strings

Use this procedure to assign a community string and type of access.



- Step 1** To assign a community string, use the proNX 900 Node Controller. Right-click on the System object (the root object in the tree) in the Navigation Tree pane.
- Step 2** Select **Provision System** from the menu.
- Step 3** Select the **SNMP** tab. Click the **Add** button in the **Communities** portion of the window. The **Add SNMP Community** window is displayed.
- Step 4** In the **Add SNMP Community** window, enter any name or string (up to 20 alphanumeric characters are supported) in the **Community** field to identify the community string.
- Step 5** Select the type of Access from the drop-down menu. In this release, both read and read-write access are supported.

Read access provides read-only access using the get, getNext, or getBulk operations.

Read-write access provides full read and write access.

Step 6 Click **Apply** when you have finished and click the **Close** button.

2.1.2 Deleting community strings

Use this procedure to delete a community string from the SNMP manager.



Step 1 To delete a community string, right-click on the System object (the root object in the tree) in the Navigation Tree pane.

Step 2 Select **Provision System** from the menu.

Step 3 In the **Provision System** window, select the **SNMP** tab. Highlight the string you want to delete in the **Communities** portion of the window. Click the **Delete** button.

Step 4 Click **Apply** when you have finished and click the **Close** button.

2.1.3 Related TL1 commands for provisioning community strings

The following table lists the TL1 commands used to provision community strings:

Table 2-1 Module provisioning commands

Action	TL1 command
Entering a new community string	ENT-SNMP-COMMUNITY: [TID]:<community>:CTAG::<access>;
Editing an existing community string	ED-SNMP-COMMUNITY: [TID]:<community>:CTAG::<access>;
Deleting a community string	DLT-SNMP-COMMUNITY:TID:<community>:CTAG;
Retrieving list of provisioned community strings	RTRV-SNMP-COMMUNITY:[TID]:[<community>]:CTAG;

For more information on TL1 commands, see the *TL1 Reference Guide*.

2.2 About trap receivers

Management stations provisioned to receive trap notifications are called trap receivers. Up to 30 trap receivers can be provisioned on the BTI 7000 Series. A notification for every alarm raise or clear event on the system is sent to each provisioned trap receiver. Traps are also sent for non-alarmed events such as database change messages and threshold crossing alerts. Trap receivers can be provisioned as either receiving SNMPv1, SNMPv2c, or SNMPv3 traps depending on what version of SNMP is supported by the trap receiver. Trap receivers must be provisioned with a community string and optionally may also be provisioned with a UDP port. The community string provisioned for the trap receiver does not need to correspond to any community string provisioned on the BTI 7000 Series for SNMPv1 or SNMPv2c traps. SNMPv3 traps must use a community string that has already been provisioned on the system.

Optionally, the receiver can be provisioned to receive Inform messages. When a trap receiver is provisioned to receive Inform messages, up to three traps are sent to the receiver at five-second intervals until acknowledgement is returned to the agent. Inform messages are supported only if the trap receiver is provisioned for message version SNMPv2.

The following sections provide instructions on how to create and delete trap receivers on the BTI 7000 Series using the proNX 900 Node Controller:

- [2.2.1, “Provisioning trap receivers”](#)
- [2.2.2, “Deleting trap receivers”](#)

For details on using the TL1 command line, see section [2.2.3, “Related TL1 commands for provisioning trap receivers”](#).

2.2.1 Provisioning trap receivers

Use this procedure to provision the destination IP address for each trap receiver on the BTI 7000 Series.



- Step 1** To provision a Trap Receiver, right-click on the System object (the root object in the tree) in the Navigation Tree pane.
- Step 2** Select Provision System from the menu.
- Step 3** Select the SNMP tab. Click the Add button in the Trap Receivers portion of the window.
- Step 4** In the Add SNMP Trap Receiver dialogue, enter:
- any name or string (up to 16 alphanumeric characters are supported) in the Trap Receiver ID field to identify the trap receiver.
 - a valid destination IP address for the trap receiver.
 - the name of the community string in the Community field to be inserted in the trap notification.

- the SNMP Version supported by the Trap Receiver.
- a UDP Port number, if required. The default is 162.
- select Inform as the notification type if desired. The default is Trap.

Step 5 Click Apply when you have finished and click the Close button.

2.2.2 Deleting trap receivers

Use this procedure to delete a trap receiver.



Step 1 To delete a Trap Receiver, right-click on the System object (the root object in the tree) in the Navigation Tree pane.

Step 2 Select Provision System from the menu.

Step 3 Select the SNMP tab. In the Trap Receivers portion of the window, select the Trap Receiver you want to delete. Click the Delete button.

Step 4 Click Apply when you have finished and click the Close button.

2.2.3 Related TL1 commands for provisioning trap receivers

The following table lists the TL1 commands used to provision trap receivers:

Table 2-2 Module provisioning commands

Action	TL1 command
Entering a new trap receiver	ENT-SNMP-TRAPRCV:[TID]:<rcvid>: [CTAG]::<ipaddr>,<community>,<version> : [PORT=<port>],[NOTIFYTYPE=<notiftype>], [TTL=<ttnl>];
Editing an existing trap receiver	ED-SNMP-TRAPRCV:[TID]:<rcvid>:[CTAG]:: [<ipaddr>],[<community>],[<version>] : [PORT=<port>],[NOTIFYTYPE=<notiftype>], [TTL=<ttnl>];
Deleting a trap receiver	DLT-SNMP-TRAPRCV:[TID]:<rcvid>:CTAG;
Retrieving list of provisioned trap receivers	RTRV-SNMP-TRAPRCV:[TID]:[<rcvid>]:CTAG;

For more information on TL1 commands, see the *TL1 Reference Guide*.

3.0 Protection group pairs

This section describes how to use objects in the `xcvrProtGrpTable` of the BTI 7000 Series MIB for the management of provisioned optical transceiver protection group pairings.

This contains the following:

- [3.1, “Protection groups”](#)
- [3.2, “Protection Group Pair Objects”](#)

3.1 Protection groups

The wavelength conversion module type supports the configuration of two transceiver ports in a 1+1 unidirectional, non-revertive protection arrangement.

The protection model borrows from those provided by Telcordia, GR-253-CORE for SONET LTE protection switching. However, the protection switching capability is not a SONET line-switched, or path-switched device. The protection switching capability is a customized physical-layer switching solution.

The wavelength conversion modules with protection switching do not use, or insert, any data into the K bytes of the SONET frame. Additionally, the protection switching feature is supported not only for transceivers receiving SONET signals, but also for facilities of any of the approved signal protocols. The trigger for an automatic protection switch is the optical loss of signal (LOS).

Provisioning rules

Two transceiver ports (that is, ports 1 and 3 as well as ports 2 and 4) on a transponder module can be provisioned as a protection pair, using the protection group pairing objects:

- 1 The working and protecting transceivers must be provisioned with the same protocol.
- 2 Both the working and the protecting transceivers must not be provisioned in an existing protection pair.

The protecting transceiver must not be involved in any provisioned cross connects on the wavelength conversion module.

Cross connects and protection group pairs

It is recommended to configure cross connects on the wavelength conversion ports prior to provisioning protection group pairs.

Protected port order

Port 4 protects port 2, or vice versa.

Port 3 protects port 1, or vice versa.

Any attempt to delete a transceiver port is rejected if that transceiver is currently involved in a protection pair. The protection provisioned and cross connects, if they exist, must be deleted before deleting the transceiver port.

Provisioned protection pairs can be deleted. If a protection pair is deleted during a forced switch or a lockout, then the forced switch and lockout are released when the protection pair is deleted.

3.2 Protection Group Pair Objects

A listing of provisioned protection group pairs is contained in the `xcvrProtGrpTable` of the MIB. When retrieved, this table provides one row for each transceiver port protection group pair provisioned on the BTI 7000 Series.

To create a protection group, a new row of the `xcvrProtGrpTable` must be created. To delete a protection group, the corresponding row of the table must be destroyed.

The following table lists the objects in each entry of the `xcvrProtGrpTable`.

Table 3-1 Protection group pairing objects

Object name	Access ^a	Range	Description	Object OID
<code>xcvrProtGrpWorkTypeldx</code>	NA	1 wt	The specific type of wavelength conversion function of the transceiver port that serves as the working port for the protection group.	1.3.6.1.4.1.
		2 wr		18070.2.2.1.10.
		3 wm		1.1.1
		4 tpr		
<code>xcvrProtGrpWorkShelfldx</code>	NA	1, 11, 21 or 31	The number of the shelf of the transceiver port that serves as the working port for the protection group.	1.3.6.1.4.1. 18070.2.2.1.10. 1.1.2
<code>xcvrProtGrpWorkSlotldx</code>	NA	1 to 20	The number of the slot of the transceiver port that serves as the working port for the protection group.	1.3.6.1.4.1. 18070.2.2.1.10. 1.1.3
<code>xcvrProtGrpWorkldx</code>	NA	1 to 4	The number of the port of the transceiver port that serves as the working port for the protection group.	1.3.6.1.4.1. 18070.2.2.1.10. 1.1.4
<code>xcvrProtGrpProtTypeldx</code>	NA	1 wt	The specific type of wavelength conversion function of the transceiver port that serves as the protection port for the protection group.	1.3.6.1.4.1.
		2 wr		18070.2.2.1.10.
		3 wm		1.1.5
		4 tpr		
<code>xcvrProtGrpProtShelfldx</code>	NA	1, 11, 21 or 31	The number of the shelf of the transceiver port that serves as the protection port for the protection group.	1.3.6.1.4.1. 18070.2.2.1.10. 1.1.6
<code>xcvrProtGrpProtSlotldx</code>	NA	1 to 20	The number of the slot of the transceiver port that serves as the protection port for the protection group.	1.3.6.1.4.1. 18070.2.2.1.10. 1.1.7
<code>xcvrProtGrpProtlldx</code>	NA	1 to 4	The number of the port of the transceiver port that serves as the protection	1.3.6.1.4.1. 18070.2.2.1.10. 1.1.8

Table 3-1 Protection group pairing objects (Continued)

Object name	Access ^a	Range	Description	Object OID
			port for the protection group.	
xcvrProtGrpId	RWC	0 to 32 printable ASCII character string	Textual data recorded by the user to describe the provisioned transceiver protection group in a manner useful to the user.	1.3.6.1.4.1.18070.2.2.1.10.1.1.9
xcvrProtGrpRowStatus	RWC	1 active 4 create and go 6 destroy	Used to control the addition and deletion of entries in the transceiver protection group table, which in turn controls provisioning and deprovisioning of optical transceiver protection groups.	1.3.6.1.4.1.18070.2.2.1.10.1.1.100

a. Access levels include: NA = Not Accessible, W = Writable, R = Readable, and C = Create.

4.0 Fault and event management

This section describes the MIB objects that are used for fault and event management of the BTI 7000 Series.

This contains the following:

- 4.1, “Trap support in SNMP”
- 4.2, “Viewing standing conditions”
- 4.3, “Decoding trap events”

4.1 Trap support in SNMP

The BTI 7000 Series supports three types of SNMP traps:

- Event traps
- Condition traps
- Database change traps

Event traps

The SNMP interface supports event trap reporting. Various event traps are defined in the BTI 7000 Series MIB. For example, when the operational status of equipment (for example, a shelf or module) or an entity such as an amplifier occurs, an event trap notification is generated by the BTI 7000 Series. This eliminates the need to poll the system for status change events. In addition, there are event traps defined to inform of inventory changes, such as removals and additions of equipment.

Condition traps

All fault detection and fault condition reporting can be performed through the SNMP interface. In general, all BTI 7000 Series alarms are reported against equipment or an entity such as an amplifier.

When a fault is detected on a network element and continues to exist for a minimum time period, it raises a fault condition, that is an indication of whether or not this particular fault currently exists on the NE. When the fault is resolved, the fault condition is cleared (that is, removed from the system).

For more information about BTI 7000 Series alarms, see the *Alarm and Troubleshooting Guide*.

Database change traps

When a provisioning or database change is made on the system, a database change trap is sent, signifying that an update has been made to the persisted database on the system.

4.2 Viewing standing conditions

Active standing conditions table

The active standing conditions table enables a user to view all active conditions (not just newly reported or acknowledged traps) using SNMP. All active conditions and alarms raised on the BTI 7000 Series can be retrieved from the actCondTable.

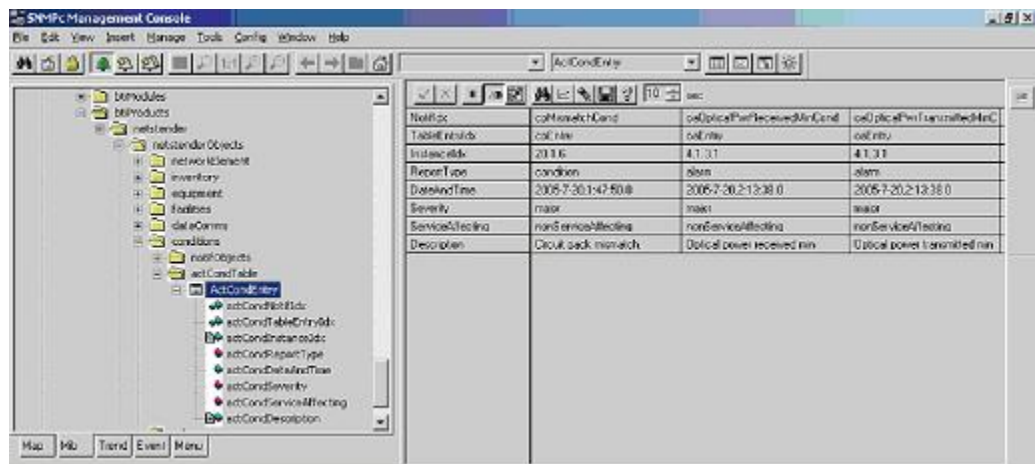
Interpreting active conditions using an SNMP browser

Figure 4-1 shows active alarms and conditions on the BTI 7000 Series retrieved using an SNMP browser. The active conditions are retrieved by ‘walking’ the actCondTable in the MIB. Each table entry provides information on one active condition and includes data on the type of alarm or condition, the equipment and/or entity on the equipment (port, for example) affected, and the location of the equipment (shelf and slot number). For example, the table listing as shown in Figure 4-1 provides the following information on the ‘cpMismatchCond’ condition:

- The NotifIdx is an index referring to the type of condition or alarm. ‘cpMismatchCond’ in this case refers to a module mismatch.
- The TableEntryIdx, cpEntry identifies the equipment or entity type against which the alarm or condition is raised (in this case, a module). For a complete list of modules, refer to the bti-tc.my MIB.
- The InstanceIdx is an object ID display string that indicates the specific object and location (shelf and slot) and in some cases, also the port, against which the alarm or condition is raised. In this example, the string is 20.1.6:
 - where 20 corresponds to the module
 - where 1 corresponds to shelf 1
 - where 6 corresponds to slot 6 in shelf 1
- ReportType indicates if the entry refers to a non-alarmed condition or alarm. In this case, the cpMismatchCond is a condition.
- DateAndTime refers to the date and time the condition or alarm was initially raised.
- Severity indicates whether the condition or alarm is minor, major or critical. In this example, the condition is Major.
- ServiceAffecting indicates whether the condition or alarm impacts the ability of the affected equipment to provide service. In this case, the condition is not service affecting.
- Description provides the condition or alarm code in full text. ‘cpMismatchCond’ refers to a module mismatch condition.

Note In Figure 4-1, each row of the actCondTable is actually displayed as a column.

Figure 4-1 Active Conditions as shown in an SNMP browser

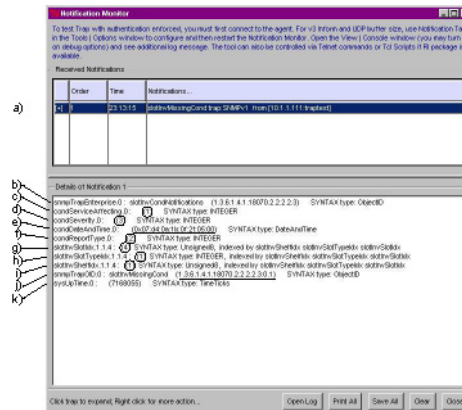


4.3 Decoding trap events

Using an event browser and the BTI-7000-MIB, it is possible to interpret trap notifications sent from SNMP agents.

The following table shows a typical equipment missing trap raise event.

Figure 4-2 Annotated trap raise event



The following section provides information on how to interpret trap notifications using the BTI-7000-MIB.

Received Notifications

- 1 slotInvMissingCond trap - indicates that a Slot Inventory Missing trap is being reported. This line also shows that the trap received was in SNMPv1 format, that it was received from a node with IP address 10.1.1.114 and that the community string read from the trap message was 'traptest'.
- 2 snmpTrapEnterprise.0: slotInvCondNotifications - indicates that a Slot Inventory trap is being reported.
- 3 condServiceAffecting 1 - this object indicates that this is a non-service affecting condition. Possible values are 1 (non-service affecting) or 2 (service affecting).
- 4 condSeverity 3 - indicates that the trap severity is major. Possible values are:
 - minor 2
 - major 3
 - critical 4
 - notAlarmed 5
 - notReported 6
- 5 condDateandTime (0x07:d4:0a:1b:0f:2f:05:00) - this hexadecimal sequence of numbers indicates when this trap notification was raised - 2004/10/27 at 15h:47m:05s. Date and time

5.0 Performance monitoring

This section describes MIB objects that are used for performance management activities. Performance monitoring statistics are collected for a number of provisioned entities on the system, including optical amplifiers, optical transceiver ports, SONET facilities, SDH facilities, and Gigabit Ethernet services.

Supported performance metric (PM) activities include the retrieval of current and historical PM statistics, initializing PM counts, and setting PM count thresholds that are used for threshold crossing alerts.

This contains the following:

- [5.1, “PM support in SNMP”](#)

5.1 PM support in SNMP

The monitoring of performance metrics (PMs) can be performed through the SNMP interface.

Tables are used to organize the available PM data. For each type of monitored entity or service, there is a table for accessing current PM data, and a second table for accessing PM data from earlier collection intervals, also known as historical data. For monitored entities that support threshold crossing alerts, a third table is provided for management of the threshold data.

5.1.1 Organization of PM table indices, values, and qualifiers

The columns of each PM table include a series of indices that are followed by a number of PM values. After each PM value, two qualifiers are also provided that designate a time stamp and bin validity. Some of the PM values also have a fourth associated object that initializes the count as explained below. The threshold tables also have a series of indices and a number of columns for the thresholds of the various monitored statistics.

PM table indices

The PM table indices provide specific information about the entity that is provisioned, such as, entity type, shelf, slot, port number, PM interval type, and interval number for historical PMs only.

The PM interval type identifies the length of the PM interval for which the monitored value is collected. The interval type of 15-minute and 1-day are supported for current and historical PMs and for thresholds. There is also an untimed PM interval type, of indefinite duration, that is supported only in the current PM table.

The interval number is used for the historical PM tables only. Historical PM bins are numbered with an interval, or index number, in reverse chronological order. the most recently completed interval is one, and older counts are numbered with higher interval numbers.

PM value

The PM value can be one of three types:

FixedX10 — This BTI-defined textual convention is integer based and represents a gauge value to one decimal place accuracy. It is generally used to convey values for physical-type PM quantities.

Unsigned32 — This convention is used for anomalous event counts, such as coding violations, or errored seconds.

Unsigned64 — This BTI-defined textual convention is counter 64-based but is zero-based to convey values for non-anomalous event counts or statistics, such as octet or frame counts.

Each PM value object supported is also followed by two qualifier objects:

- time stamp
- validity

Time stamp

The time stamp object indicates the date and time of the PM interval. For physical-type PMs, the PM value represents a snapshot reading taken at a specific time. For these PMs, the time stamp for current PMs is always the time that the PM value was requested.

For historical physical PM values, the time stamp indicates the beginning of the interval period.

For counter type PM values, however, the time stamp always indicates the time at the beginning of the collection interval for both current and historical PM values.

Bin validity

The bin validity object indicates the completeness of the 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.

There are three possible bin validity qualifiers:

- **complete** indicates that the collection interval completes normally.
- **notAvailable** indicates that there is no PM collection during the interval, when
 - PM collection software fails to collect PMs for the entire duration of the collection interval, or
 - equipment is out-of-service for the interval.
- **partialCount** indicates that PM collection occurred for some but not all of the collection period. This validity qualifier applies to counter type PMs only.



Part Number:
Document Version:
Published:
Type:

BT7A74AA
01
March 2017
STANDARD

product release 13.5