



## PRODUCT DOCUMENTATION

### *BTI 7000 Series Management Communications Channel Solutions Guide*

**Part Number:** BT7A73EA  
**Document Version:** 01  
**Published:** March 2017  
**Type:** STANDARD

***product release 13.5***



# Contents

---

<b>Preface</b>	<b>vii</b>
<b>1.0 Management Communication Channels solution</b>	<b>1-1</b>
1.1 Management Communication Channels .....	1-2
1.1.1 GCC .....	1-2
1.1.1.1 GCC support on BTI 7000 Series modules .....	1-2
1.1.2 Optical Data Communications Channel (ODCC) on DOL .....	1-3
1.1.2.1 ODCC on DOL support on BTI 7000 Series modules .....	1-3
1.1.3 Optical Data Communications Channel (ODCC) on SCP OSC ports .....	1-3
1.1.3.1 Modules that support ODCC on SCP OSC .....	1-5
1.2 Supported MCC network configurations .....	1-6
1.2.1 GCC and ODCC on DOL supported configurations .....	1-6
1.2.1.1 Point-to-point configuration for GCC and ODCC on DOL .....	1-6
1.2.1.2 Ring configuration for GCC and ODCC on DOL .....	1-7
1.2.1.3 Management VLAN configuration for GCC .....	1-8
1.2.2 ODCC on SCP OSC supported configurations .....	1-8
1.2.2.1 Point-to-point configuration for ODCC on SCP OSC .....	1-9
1.2.2.2 Ring configuration for ODCC on SCP OSC .....	1-9
1.3 Management communication channel selection criteria .....	1-11
1.4 Management interfaces supported by the MCC .....	1-12
1.5 MCC release compatibility .....	1-13
<b>2.0 Management communications channel features</b>	<b>2-1</b>
2.1 Management communication channel solution features .....	2-2
2.1.1 GCC features .....	2-2
2.1.1.1 General Communications Channel .....	2-2
2.1.2 ODCC on DOL .....	2-2

2.1.3	ODCC on SCP OSC features .....	2-2
2.1.4	OSPF .....	2-3
<b>3.0</b>	<b>GCC and OSC specifications</b> .....	<b>3-1</b>
3.1	Standards .....	3-2
3.1.1	ITU Telecommunication standardization .....	3-2
3.1.2	RFC Standards .....	3-2
3.2	OSC optical specifications .....	3-4
3.2.1	1510 XR SFP (for OSC) specifications .....	3-4
3.2.2	CWDM ER SFP (for OSC) specifications .....	3-4
3.2.3	Multimode 1310 SR SFP optical specifications .....	3-6
<b>4.0</b>	<b>Network design guidelines</b> .....	<b>4-1</b>
4.1	Network design examples .....	4-2
4.1.1	Point-to-point or linear GCC applications .....	4-2
4.1.1.1	Site by site configuration planning and preparation .....	4-2
4.1.1.2	Site by site requirements .....	4-3
4.1.1.3	TL1 commands to implement this point-to-point scenario .....	4-5
4.1.2	Ring GCC applications .....	4-6
4.1.2.1	Site by site configuration planning and preparation .....	4-6
4.1.2.2	Site by site requirements .....	4-7
4.1.2.3	TL1 commands to implement this ring scenario .....	4-9
4.1.3	Point-to-point GCC with line protection .....	4-11
4.1.3.1	Site by site configuration planning and preparation .....	4-11
4.1.3.2	Site by site requirements .....	4-12
4.1.3.3	TL1 commands to implement this point-to-point GCC with line protection scenario .....	4-13
4.1.4	Dual-homed GCC application .....	4-14
4.1.4.1	Site by site configuration planning and preparation .....	4-14
4.1.4.2	Site by site requirements .....	4-15
4.1.4.3	TL1 commands to implement this dual-homed GCC scenario .....	4-17
4.1.5	Point-to-point or linear OSC applications .....	4-19
4.1.5.1	Site by site configuration planning and preparation .....	4-19
4.1.5.2	Site by site requirements .....	4-20
4.1.6	Ring OSC application .....	4-21
4.1.6.1	Site by site configuration planning and preparation .....	4-21
4.1.6.2	Site by site requirements .....	4-22
4.2	Management access and connectivity over IP networks .....	4-24
<b>5.0</b>	<b>Installing or replacing modules</b> .....	<b>5-1</b>
5.1	Install the System Control Processor module in a BTI 7060 .....	5-2
5.2	Install the System Control Processor module in a BTI 7200 .....	5-4
5.3	Installing SFP transceivers .....	5-6
5.4	Installing and fiberizing a Coupler/Splitter module .....	5-9
5.5	Replacing the System Control Processor module .....	5-11
5.6	Replacing SFP transceivers .....	5-14

5.7 Replacing Coupler/Splitters .....	5-18
---------------------------------------	------

## **6.0 Provisioning and activating GCC and ODCC on DOL** **6-1**

6.1 Provisioning GCC .....	6-2
6.1.1 GCC provisioning task list .....	6-2
6.1.2 GCC provisioning restrictions .....	6-2
6.1.3 Enabling GCC on an interface .....	6-3
6.2 Provisioning ODCC on DOL .....	6-4
6.2.1 ODCC on DOL provisioning task list .....	6-4
6.2.2 ODCC on DOL provisioning restrictions .....	6-4
6.2.3 Enabling ODCC on an interface .....	6-5
6.3 Configuring OSPF .....	6-6
6.3.1 Enabling OSPF on a shelf .....	6-6
6.3.2 Enabling OSPF on an interface .....	6-7
6.4 Managing GCC and ODCC on DOL services .....	6-9
6.4.1 Removing GCC and ODCC services from an interface .....	6-9
6.4.2 Restoring the GCC or ODCC to service .....	6-9
6.4.3 Deleting a GCC or ODCC service from an interface .....	6-10
6.5 Configuring GCC to Management VLAN Routing .....	6-11
6.6 Related TL1 provisioning commands .....	6-13
6.6.1 TL1 commands for provisioning GCC .....	6-13
6.6.2 TL1 commands for provisioning ODCC on DOL .....	6-13
6.6.3 TL1 commands for provisioning OSPF .....	6-14
6.7 Related CLI provisioning commands .....	6-15
6.7.1 CLI commands for provisioning GCC .....	6-15
6.7.2 CLI commands for provisioning OSPF .....	6-15
6.8 Related SNMP tables .....	6-17
6.8.1 Provisioning GCC, ODCC and OSPF using SNMP .....	6-17

## **7.0 Provisioning the OSC** **7-1**

7.1 Overview .....	7-2
7.2 Provisioning tasks .....	7-3
7.2.1 Enabling OSC ports .....	7-3
7.2.2 Provision management Ethernet settings .....	7-3
7.2.2.1 Provision Ethernet settings .....	7-3
7.2.2.2 Viewing Ethernet Info .....	7-4
7.2.3 Add static routes .....	7-4
7.2.4 Delete static routes .....	7-5

## **8.0 Managing communication channel solutions** **8-1**

8.1 Monitoring OSPF .....	8-2
8.1.1 Viewing the routing table .....	8-2
8.1.2 Viewing static routes .....	8-2
8.1.3 Filtering static routes .....	8-3
8.1.4 Viewing the OSPF Link State Database .....	8-3

8.1.5 Adding or removing display columns .....	8-4
8.1.6 Filtering the Link State Database .....	8-5
8.1.7 Viewing the OSPF Neighbors database .....	8-5
8.1.8 Adding or removing display columns .....	8-6
8.1.9 Filtering OSPF Neighbors .....	8-6
8.2 Related TL1 commands .....	8-7
8.2.1 TL1 commands for viewing the routing table .....	8-7
8.2.2 TL1 commands for viewing Neighbor entries .....	8-7
8.2.3 TL1 commands for viewing the Link State Database .....	8-7

---

## **9.0 Troubleshooting** **9-1**

9.1 Troubleshooting GCC communications .....	9-2
9.1.1 Checking physical connectivity .....	9-2
9.1.2 Checking OSPF .....	9-2
9.1.3 Checking Management Network Router .....	9-3
9.2 Troubleshooting OSC communications .....	9-4
9.2.1 Checking physical connectivity .....	9-4
9.2.2 Checking STP .....	9-4
9.3 Using Ping to check connectivity .....	9-5
9.4 OSCLOS (OSC Loss of Signal) .....	9-6
9.4.1 Clearing an OSCLOS OSC loss of signal alarm .....	9-8

---

## **Appendix A: Packet flow** **A-1**

---

## **Appendix B: Performance engineering** **B-1**

---

# Preface

---

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

## Audience

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

## Features of the BTI 7000 Series

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

## BTI 7000 Series common equipment

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

### BTI 7000 Series common equipment

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

**BTI 7000 Series common equipment (Continued)**

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

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

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

**Management software suite**

<b>proNX Management Suite</b>
proNX Service Manager (PSM)
proNX 900 Node Controller (proNX 900)



## Equipment compliance

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




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

## Organization of the BTI 7000 Series documentation

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

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

**Documentation conventions**

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

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

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

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

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

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

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

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

Copyright 1990-2001 Sleepycat Software. All rights reserved.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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



# 1.0 Management Communication Channels solution

---

This section describes the Management Communication Channels (MCC) solution that the BTI 7000 Series supports.

- 1.1, “Management Communication Channels”
- 1.2, “Supported MCC network configurations”
- 1.3, “Management communication channel selection criteria”
- 1.4, “Management interfaces supported by the MCC”
- 1.5, “MCC release compatibility”

# 1.1 Management Communication Channels

The Management Communication Channels (MCC) solution supported on the BTI 7000 Series allows network providers to remotely manage network elements using the General Communications Channel (GCC), the Optical Data Communications Channel (ODCC) on DOL modules, and the ODCC on the Optical Supervisory Channel (OSC) ports on the SCP.

The GCC, ODCC on DOL, and ODCC on SCP OSC support point-to-point and ring configurations. For more information refer to [1.2, “Supported MCC network configurations”](#).

The GCC, ODCC on DOL, and ODCC on SCP OSC are open communications channels that provide IP connectivity to BTI 7000 Series network elements, allowing network-management applications to be used for:

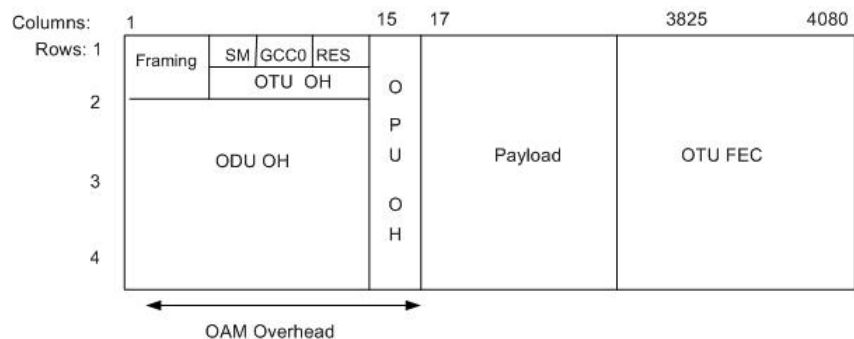
- Remote provisioning and inventory
- Network surveillance, including detection of link failures and equipment alarms
- Remote backup and restore of the configuration database
- Remote upgrade of system software
- Remote performance monitoring

## 1.1.1 GCC

The BTI 7000 Series uses the GCC (defined in ITU-T standard G.709-2003) to form an IP-based network for management communications.

Service Providers can use the GCC to manage their networks without impacting customer bandwidth, or using another wavelength on their fibers. The GCC0 bytes defined in the OTU1/ OTU2 overhead are used to form a 333 kilobits/second channel for the 8-Port Multiprotocol Muxponder - SDH.

**Figure 1-1 GCC in the OTN OTU2 frame structure**



### 1.1.1.1 GCC support on BTI 7000 Series modules

The following table lists the BTI 7000 Series modules that support GCC.



**Table 1-1 Supported GCC modules**

Module	PEC
10G Multiprotocol Transponder	BT7A49AB
Dual 10G Multiprotocol Transponder	BT7A49AA
	BT7A49AA-I02
8-Port Multiprotocol Muxponder - SONET	BT7A47JA
8-Port Multiprotocol Muxponder - SDH	BT7A47KA
8-Port Multiprotocol Muxponder - SDH CCAT	BT7A47MA
10-Port Multiprotocol Muxponder - SONET	BT7A48AA, BT7A48AA-I02
10-Port Multiprotocol Muxponder - SDH	BT7A48BA, BT7A48BA-I02
10-Port Multiprotocol Muxponder - SDH CCAT	BT7A48DA
packetVX Integrated Packet Services Module - 12/2	BT7A81AA
packetVX Integrated Packet Services Module - 24/2	BT7A81BA
packetVX Integrated Packet Services Module - 24/4	BT7A81CA

## 1.1.2 Optical Data Communications Channel (ODCC) on DOL

The ODCC on DOL is an OSC-supported data management communications link between dynamic optical layer (DOL) nodes. The ODCC can be configured to be part of a management communications network to support remote access to management interfaces of a BTI 7000 Series network element that is not directly connected to the management LAN:

- The ODCC on DOL can be manually provisioned, provided a supporting DOL OSC object exists.
- When In-service, the ODCC is enabled to serve as an unnumbered interface to the external-facing network management IP stack.
- When Out-of-service, the ODCC is disabled from performing its communication function.

### 1.1.2.1 ODCC on DOL support on BTI 7000 Series modules

The following table lists the BTI 7000 Series modules that support ODCC on DOL.

**Table 1-2 Supported ODCC on DOL modules**

Module	PEC
DWDM Line Amplifier (DLA2)	BT7A06CA
2D ROADM-on-a-blade (ROB2)	BT7A07AA
4D ROADM-on-a-blade (ROB4)	BT7A07BA

## 1.1.3 Optical Data Communications Channel (ODCC) on SCP OSC ports

The ODCC on SCP OSC is an OSC-supported data management communications link between nodes connected via the SCP OSC ports. The ODCC can be configured to be part of a

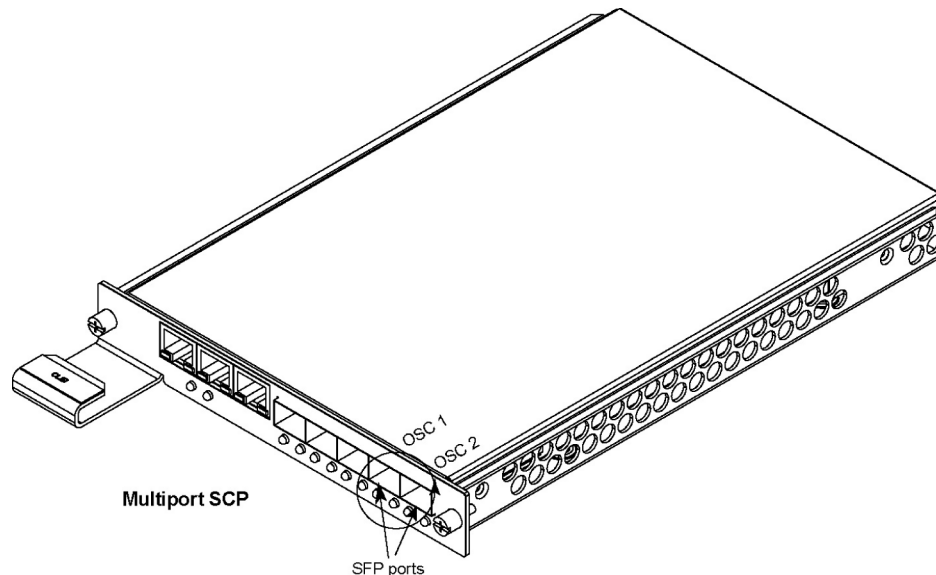
management communications network to support remote access to management interfaces of a BTI 7000 Series network element that is not directly connected to the management LAN:

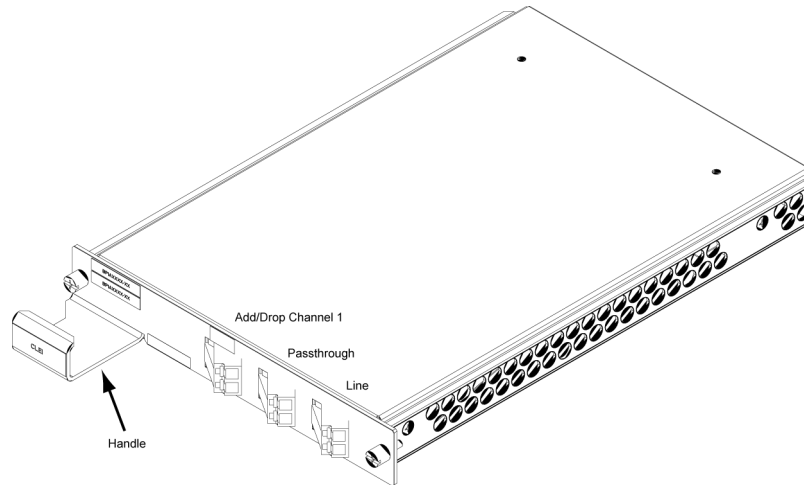
- The ODCC on SCP OSC can be manually provisioned by enabling the OSC ports.
- A coupler/splitter must be used to couple the OSC fiber with the transport fiber carrying the channel.
- When In-service, the ODCC is enabled to serve as an unnumbered interface to the external-facing network management IP stack.
- When Out-of-service, the ODCC is disabled from performing its communication function.

OSC is an additional wavelength usually outside the C-band (at 1510nm, 1610nm, or 1310nm) that carries management information. This wavelength is physically coupled and split from the transport fibers connecting a pair of network elements.

See the following figures:

**Figure 1-2 OSC ports on the SCP**



**Figure 1-3 OSC Coupler/Splitter**

### 1.1.3.1 Modules that support ODCC on SCP OSC

The following table lists the BTI 7000 Series modules that support ODCC on SCP OSC.

**Table 1-3 Supported ODCC on SCP OSC modules**

Module	PEC
BTI 7060/BTI 7200 Shelf Control Processor (SCP)	BT7A20CA
BTI 7030 Shelf Control Processor (SCP)	BT7A21BA

## 1.2 Supported MCC network configurations

---

BTI offers the following Management Communication Channels solution options:

- GCC
- ODCC on DOL
- ODCC on SCP OSC

### 1.2.1 GCC and ODCC on DOL supported configurations

The BTI 7000 Series supports the following configurations for GCC and ODCC on DOL:

- [1.2.1.1, “Point-to-point configuration for GCC and ODCC on DOL”](#)
- [1.2.1.2, “Ring configuration for GCC and ODCC on DOL”](#)
- [1.2.1.3, “Management VLAN configuration for GCC”](#)

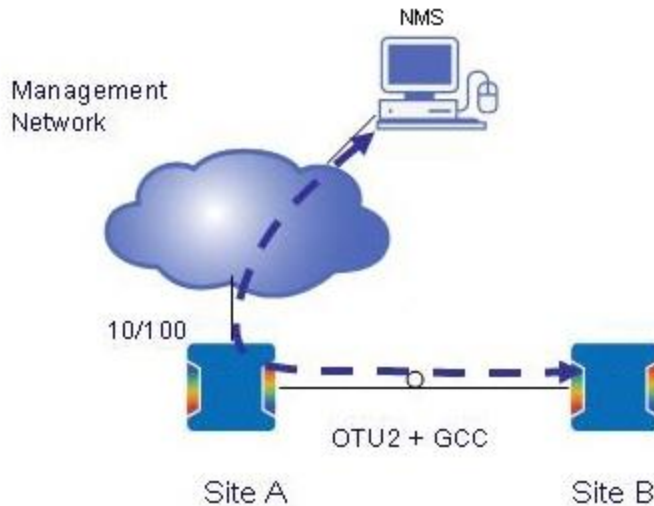
#### 1.2.1.1 Point-to-point configuration for GCC and ODCC on DOL

In a point-to-point configuration, each network element must include a minimum of one GCC- or one ODCC- capable port.

- **For GCC:** The port(s) must have the supported OTU line protocol and GCC overhead enabled.
- **For ODCC on DOL:** ODCC must be enabled on a DOL module.

The following example shows a GCC point-to-point network configuration. Site A connects to the management network through the management LAN port (10/100BaseT port on the MSI). Communication to site B is through site A and the GCC. Site A and Site B each have a unique IP address (on the different subnets) assigned allowing the management station to connect.

<b>Note</b>	For an ODCC configuration, Sites A and B are connected by DOL (dynamic optical layer) line ports.
-------------	---

**Figure 1-4 Example point-to-point configuration for GCC**

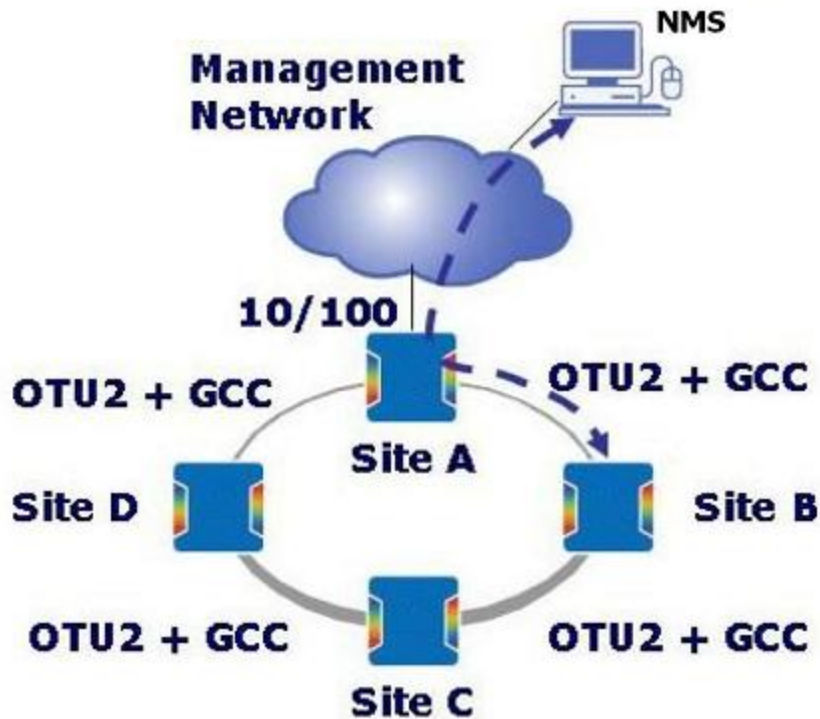
### 1.2.1.2 Ring configuration for GCC and ODCC on DOL

In a ring network configuration, each network element (NE) must include a minimum of two GCC-capable ports, or one ODCC-capable port.

- **For GCC:** The port(s) must have the supported OTU line protocol and GCC overhead enabled.
- **For ODCC on DOL:** ODCC must be enabled on the dynamic optical layer DOL module.

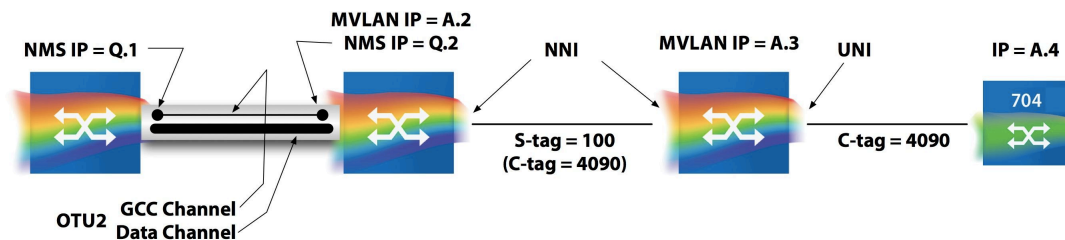
The following example shows a ring network configuration for GCC. In this example network configuration, site A connects to the management network through the management LAN port (10/100Base-T port on the MSI). Communication to sites B, C and D is through site A and the GCC. Each site has a unique IP address assigned allowing the management station to connect. OSPF routing protocol is used between BTI 7000 Series network elements to determine the optimal path to reach a specific NE. If a network element or link fails, management traffic is re-routed automatically.

<b>Note</b>	For an ODCC configuration, communication to sites B, C and D is through site A and the ODCC service.
-------------	--

**Figure 1-5 Ring configuration for GCC**

### 1.2.1.3 Management VLAN configuration for GCC

This section describes GCC to Management VLAN routing, as shown in the following figure.



In this scenario, traffic from a GCC link is routed across the Management VLAN with an ultimate destination of a NE on a customer VLAN on NE A.2. The GCC link is provisioned on interface tenGig 1/1/1 and routed over an NNI on port tenGig 1/1/2 which is part of the Management VLAN service.

## 1.2.2 ODCC on SCP OSC supported configurations

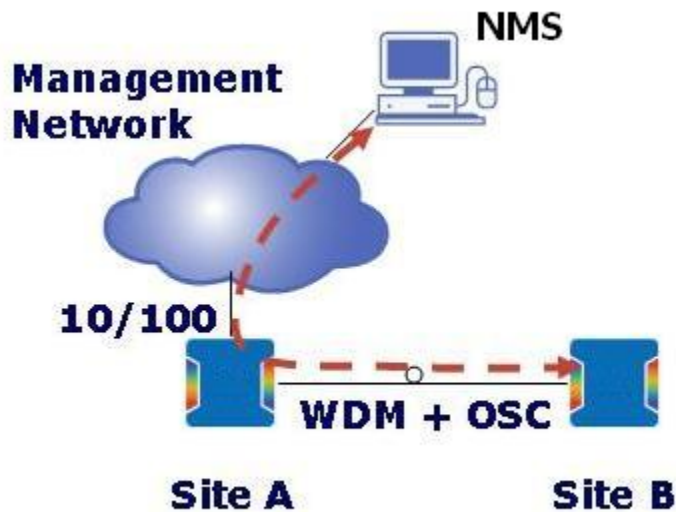
The BTI 7000 Series supports the following configurations for ODCC on SCP OSC:

- Point-to-point
- Ring

### 1.2.2.1 Point-to-point configuration for ODCC on SCP OSC

The following figure shows an example point-to-point configuration. In point-to-point network configurations, each NE must include an OSC SFP and coupler/splitter. Each NE must also have the OSC enabled through software. Site A is connected to the management network through the management LAN port (10/100 BaseT port on the MSI). Communication to site B is through site A and the OSC. Site A and Site B each have a unique IP address (on the same subnet) assigned allowing the management station to connect.

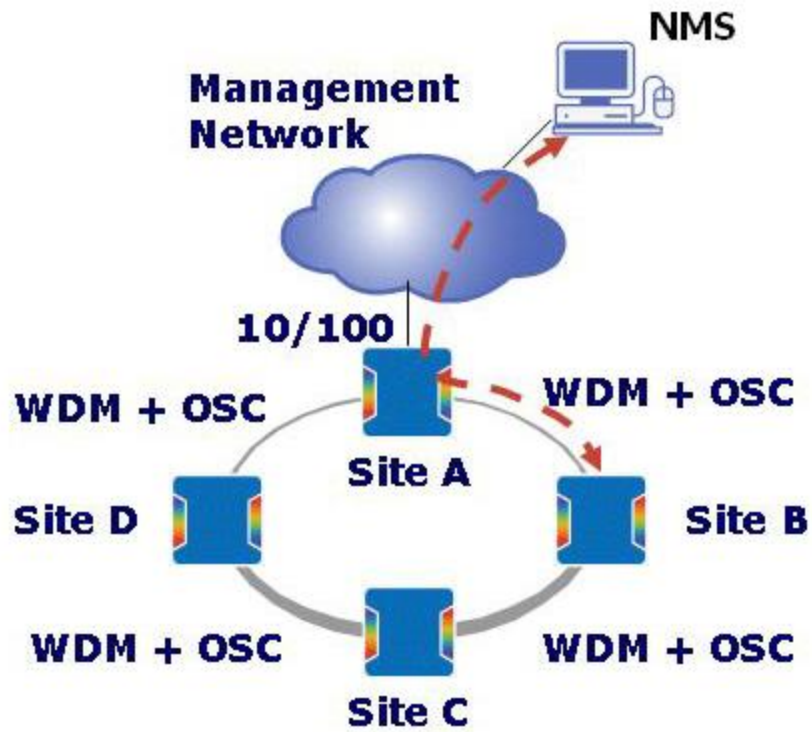
**Figure 1-6 Point-to-point configuration for OSC**



### 1.2.2.2 Ring configuration for ODCC on SCP OSC

The following figure shows an example ring configuration. In a ring configuration, each NE must include two OSC SFPs and a coupler/splitter. Each NE must also have both OSC ports enabled through software. Site A is connected to the management network through the management LAN port (10/100 BaseT port on the MSI). Communication to sites B, C and D is through site A and the OSC. Each site has a unique IP address assigned allowing the management station to connect. In the event of a network element or link failure, management traffic is switched along an alternate path automatically using STP protocol.

**Figure 1-7 Ring configuration for OSC**





## 1.3 Management communication channel selection criteria

The following table lists the channel selection criteria to consider when choosing a management communications option.

**Note** The channel options are listed in the order recommended.

**Table 1-4 MCC selection criteria**

Criteria		MVLAN	ODCC on SCP OSC	ODCC on DOL	GCC
Topology	Point-to-point	Y	Y	Y	Y
	Ring	Y	Y	Y	Y
	Mesh	Y	N	Y	Y
	Star (>2 legs)	Y	N	Y	Y
Module types in the network element (NE)	packetVX (PVX)	Y <sup>1</sup>	Y <sup>2</sup>	N	Y <sup>1</sup>
	dynamic optical layer (DOL)	N	N	Y	N
	OTU2	N	Y <sup>2</sup>	N	Y
	SCP	N	Y <sup>2</sup>	N	N
Forwarding	Bridging	Ethernet with STP	Ethernet with STP	not applicable	not applicable
	Routing	IP/OSPF	IP/OSPF	IP/OSPF	IP/OSPF
Speed	-	Up to 1Gb/s <sup>3</sup>	100Mb/s	1.3 Mb/s	1.3 Mb/s
Physical complexity	Additional components required	N	OSC SFPs Coupler/ Splitter	N	N
Fan-out	1-port	Y	Y	Y	Y
	2-ports	Y	Y	Y	Y
	> 2 ports	Y <sup>4</sup>	N	Y	Y

<sup>1</sup>With PVX modules present, either MVLAN or GCC can be run.

<sup>2</sup>OSC ports on SCP modules are available on all nodes regardless of card lineup.

<sup>3</sup>OSC is bandwidth dedicated to management traffic. MVLAN can be up to 1Gb/s ingressing on a PVX client-port UNI, or up to 100Mb/s ingressing on IP-NMS, but is subject to bandwidth sharing.

<sup>4</sup>MVLAN fanning out via > 2 ports requires four line ports, therefore a PVX 24/4 must be used.

<sup>5</sup>Applicable when configured for the OSI protocol.

## 1.4 Management interfaces supported by the MCC

---

Management Communication Channels can be configured and managed using the following interfaces:

MCC Channel	Supported Interface
GCC (General Communications Channel)	proNX 900 Node Controller
	SNMP
	TL1
	CLI
ODCC (Optical Data Communications Channel) on DOL	proNX 900 Node Controller
	SNMP
	TL1
ODCC (Optical Data Communications Channel) on SCP OSC	proNX 900 Node Controller
	SNMP
	TL1
Management VLAN	proNX 900 Node Controller
	SNMP
	CL1

## 1.5 MCC release compatibility

---

GCC and ODCC on SCP OSC are supported in BTI 7000 Series Release 7.1.0 and later.

ODCC on DOL is supported in BTI 7000 Series Release 9.2.0 and later.



## 2.0 Management communications channel features

---

This section describes the management features supported on BTI 7000 Series network elements.

- [2.1, “Management communication channel solution features”](#)

## 2.1 Management communication channel solution features

---

The Management Communication Channels (MCC) Solution supports the following remote management capabilities:

- Remote provisioning and inventory
- Network surveillance, including detection of link failures and equipment alarms
- Remote backup and restore of the configuration database
- Remote upgrade of system software
- Remote performance monitoring

GCC and OSC transport industry standard IPv4 traffic and support higher layer protocols, such as Telnet, TL1, SNMP, TFTP, FTP, NTP, and SYSLOG.

### 2.1.1 GCC features

The BTI 7000 Series GCC implementation is an IP routed solution. Each GCC interface is configured as an IP unnumbered interface. OSPF routing is used to determine the optimal paths for routing management traffic. Each network element requires a single IP address to support management communications.

#### 2.1.1.1 General Communications Channel

Certain modules feature an embedded GCC0 management channel (see [1.1.1, “GCC”](#)), which is an IP-routed solution that allows remote management of provisioning, software upgrade, and alarm and performance monitoring. To use the GCC0, you must enable and then provision it on a supporting module. For detailed information about how to provision the GCC0, and the applications and configurations it supports, see [Chapter 6, “Provisioning and activating GCC and ODCC on DOL”](#).

### 2.1.2 ODCC on DOL

BTI 7000 Series Dynamic Optical Layer (DOL) modules feature an embedded management channel (see [1.1.2, “Optical Data Communications Channel \(ODCC\) on DOL”](#)).

Similar to GCC, ODCC on DOL is an IP-routed solution that allows remote management of provisioning, software upgrade, and alarm and performance monitoring. To use ODCC on DOL, you must enable and then provision it on a supporting DOL module. For detailed information about how to provision ODCC on DOL, and the applications and configurations it supports, see [6.2, “Provisioning ODCC on DOL”](#).

### 2.1.3 ODCC on SCP OSC features

OSC implementation in the BTI 7000 Series is an Ethernet switched solution. Each OSC interface is a 100 Mbps Ethernet interface. Spanning tree protocol (STP) runs on the SCP frontplane ports (IP-NMS OSC1 and OSC2) to prevent broadcast storms in a bridged network when there are redundant paths between nodes.

STP (compliant with IEEE 802.1D) provides a failover mechanism in ring topologies when a network element or link fails. Each network element requires a single IP address to support management communications. Beginning at Release 9.3, the STP is always enabled. However, transmission of the STP BPDUs message from the NMS management LAN port to the external data management network can be provisioned ON or OFF.

**Spanning tree features:**

- STP runs on the management LAN port and enabled OSC ports.
- STP is enabled by default. Ensure that the IP-NMS port is disconnected until the system completes initialization.
- When STP is disabled:
  - The system does not send STP BPDUs from the IP-NMS port.
  - The IP-NMS port continues to forward and accept all traffic.

See [Appendix A, “Packet flow”](#) for more information.

## 2.1.4 OSPF

For the BTI 7000 Series, GCC and ODCC implementations conform to OSPF Version 2 specifications detailed in RFC 2328. Specifically it supports:

- Configurable OSPF Router ID
- Configurable OSPF Area ID
- Configurable parameters for OSPF Interfaces - Hello Interval, Priority, Transit, Delay, Retransmit Interval, Dead Interval, and Cost
- Route Redistribution - Non-OSPF routes such as Static, Connected, or Default, can be redistributed into OSPF
- Viewing OSPF Information - Viewing of the OSPF Link State Database, and OSPF Neighbor Table
- Routing Table - Viewing of the Routing Table

See [Appendix A, “Packet flow”](#) for more information on packet flow.





## 3.0 GCC and OSC specifications

---

This section describes the specifications and compliance that the Management Communication Channels supports.

- [3.1, “Standards”](#)
- [3.2, “OSC optical specifications”](#)

## 3.1 Standards

---

This section describes the standards GCC and OSC support. Information regarding the optical specifications of the Management Communication Channels Solution is also contained in the GCC and OSC specifications of the *Product Guide*.

### 3.1.1 ITU Telecommunication standardization

The BTI 7000 Series supports the frequency grid standards for CWDM and DWDM wavelengths listed in the following table. In addition, the GCC uses the GCC0 overhead bytes as defined in ITU-T G.709-2003.

**Table 3-1 ITU-T compliance**

Standard	Description
G.694.1	Spectral grids for WDM applications: DWDM frequency grid
G.694.2	Spectral grids for WDM applications: CWDM wavelength grid
G.709	Interfaces for the Optical Transport Network (OTN)

### 3.1.2 RFC Standards

The following table indicates the Request For Comments (RFC) standards supported by the BTI 7000 Series.

**Table 3-2 Supported RFC standards**

Protocol	RFC number	Description
IPv4	RFC 791	Internet Protocol
TCP	RFC 793	Transmission Control Protocol
UDP	RFC 768	User Datagram Protocol
ICMP	RFC 792	Internet Control Message Protocol
Telnet	RFC 854	Telnet Protocol Specification
	RFC 855	Telnet Option Specification
SSH-2	RFC 4251 and others	Secure Shell Protocol version 2
TFTP	RFC 1350	Trivial File Transfer Protocol
SNMPv1	RFCs 1155, 1157, 1212, 1213, and 121	Simple Network Management Protocol
SNMPv2c	RFCs 1901 through 1907	Simple Network Management Protocol
STP	RFC 2719	Framework Architecture for Signaling Transport

**Table 3-2 Supported RFC standards (Continued)**

<b>Protocol</b>	<b>RFC number</b>	<b>Description</b>
PPP		Compliant with IEEE 802.1d
	RFC 1172	Point-to-Point Protocol initial configuration options
	RFC 1570	PPP LCP Extensions
	RFC 1662	PPP in HDLC-like Framing
OSPFv2	RFC 2328	Open Shortest Path First

## 3.2 OSC optical specifications

The following sections provide specifications for Small Form-factor Pluggable transceivers (SFPs) supported for use in the OSC ports on the SCP.

### 3.2.1 1510 XR SFP (for OSC) specifications

The following table provides specifications for the 1510 XR SFP (for OSC) supported for use in the OSC ports on the SCP.

**Table 3-3 1510 XR SFP (for OSC) BP3AE1CX specifications**

Parameter	Min	Typ	Max	Units
Bit rate <sup>1</sup>	—	156	—	Mb/s
Transmitter				
Laser source	single-mode			
Tx center wavelength	1500	1511	1520	nm
Average operating power	1	—	5	dBm
Spectral width (-20 dB)	—	—	1	nm
Side mode suppression ratio	30	—	—	dB
Extinction ratio	10	—	—	dB
Receiver				
Rx operating wavelength	1100	—	1600	nm
Max Input (BER=1x10 <sup>-10</sup> )	-7	—	—	dBm
Rx sensitivity (BER=1x10 <sup>-10</sup> )	-43	—	—	dBm
Optical Return Loss	25	—	—	dB
Other				
Connector/Latch type	LC/Bail			

<sup>1</sup>Data rate ranges from 50 Mb/s to 266 Mb/s. However, device performance is not guaranteed.

### 3.2.2 CWDM ER SFP (for OSC) specifications

The following table provides specifications for the CWDM ER SFP (for OSC) supported for use in the OSC ports on the Multiport SCP.

**Table 3-4 CWDM ER SFP (for OSC) BP3AE1CE specifications**

Parameter	Min	Typ	Max	Units
Bit rate	50	156	266	Mb/s
<b>Transmitter</b>				
Laser source	single-mode			
Tx center wavelength	1511	—	1611	nm

**Table 3-4 CWDM ER SFP (for OSC) BP3AE1CE specifications (Continued)**

Parameter	Min	Typ	Max	Units
Tx center wavelength accuracy	-6.5	—	6.5	nm
Average operating power	0	—	5	dBm
Spectral width (-20 dB)	—	—	1	nm
Side mode suppression ratio	30	—	—	dB
Extinction ratio	10	—	—	dB
<b>Receiver</b>				
Rx operating wavelength	1100	—	1620	nm
Max Input (BER=1x10 <sup>-10</sup> )	-7	—	—	dBm
Rx sensitivity (BER=1x10 <sup>-10</sup> )	-34	-37	—	dBm
Optical Return Loss	25	—	—	dB
<b>Other</b>				
Connector/Latch type	LC/Bail			

### 3.2.3 Multimode 1310 SR SFP optical specifications

The following table provides specifications for the Multimode 1310 SR SFP supported for multishelf use.

**Table 3-5 Multimode 1310 SR SFP BP3AE1MM optical specifications**

Parameter	Min	Typ	Max	Units
Bit rate	—	125	—	Mb/s
<b>Transmitter</b>				
Laser source	multimode			
Tx operating wavelength	1270	—	1380	nm
Average operating power	-20	—	-14	dBm
Spectral width (-20 dB)	—	—	200	nm
Extinction ratio	10	—	—	dB
<b>Receiver</b>				
Rx operating wavelength	1100	—	1600	nm
Max input (BER=2.5x10 <sup>-10</sup> )	-14	—	—	dBm
Rx sensitivity (BER=1x10 <sup>-10</sup> )	-30	—	—	dBm
Rx sensitivity (BER=1x10 <sup>-12</sup> )	-29	—	—	dBm
<b>Other</b>				
Connector/Latch type	LC/Bail			

## 4.0 Network design guidelines

---

This section provides information for running over IP.

- [4.1, “Network design examples”](#)
- [4.2, “Management access and connectivity over IP networks”](#)

## 4.1 Network design examples

---

This section contains a number of GCC and OSC network examples to help you extrapolate network design rules that apply to GCC and OSC applications.

Each network example contains planning and network requirements. Use these point-to-point, linear, and ring examples to help create more complex topologies.

This section covers the following topics:

- [4.1.1, “Point-to-point or linear GCC applications”](#)
- [4.1.2, “Ring GCC applications”](#)
- [4.1.3, “Point-to-point GCC with line protection”](#)
- [4.1.4, “Dual-homed GCC application”](#)
- [4.1.5, “Point-to-point or linear OSC applications”](#)
- [4.1.6, “Ring OSC application”](#)
- 

### 4.1.1 Point-to-point or linear GCC applications

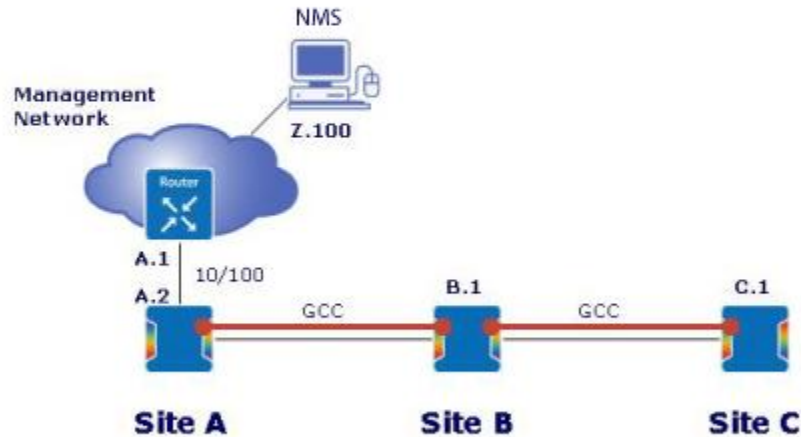
Using GCC in a point-to-point or linear application includes:

- BTI 7000 Series network elements managed from a local or a remote management station
- BTI 7000 Series network elements deployed in a linear span

#### 4.1.1.1 Site by site configuration planning and preparation

The following figure shows the Ethernet, IP address and subnet requirements for a point-to-point GCC application.



**Figure 4-1 Point-to-point GCC application**

In this example, three NEs are cascaded in a linear chain. The first NE at site A is directly connected to the management network using a 10/100BT Ethernet connection. Connectivity to sites B and C is provided using GCC between sites A and B and sites B and C, respectively.

Although this example shows three NEs in a linear chain, more NEs can be cascaded together as required. See [Appendix B, “Performance engineering”](#) for engineering limits.

### Preparation

Site-by-site deployment requires a number of IP addresses. Coordinate the IP address allocation with the IT group responsible for the day-to-day operation of the management network. In this example you need:

- IP address for the management station(s); for example, Z.100 in the figure above
- IP address and subnet masks for the various sites; for example, A.2, B.1, C.1 in the figure above
- default gateway address for Site A

#### 4.1.1.2 Site by site requirements

This section identifies the specific requirements for the network elements in this example. See the figure below for GCC requirements.

## Remote Management Station

Configure the remote management station with an IP address, subnet mask and default gateway on the management network. In this example, the IP address is Z.100 and the default gateway is Z.1.

## Near-end Site (Site A)

Connect the near end site to the management network using a 10/100BT Ethernet port on the MSI (management LAN port). Assign an IP address, subnet mask and default gateway to this port.

Ensure that the near-end site has a module supporting GCC functionality. Refer to [1.1.1, “GCC”](#). Set the line protocol of the module to OTU2. Enable GCC. This port does not require an IP address as BTI 7000 Series treats GCC interfaces as un-numbered interfaces.

Enable OSPF at Site A. Specify an area ID and router ID when enabling OSPF. If no area ID is specified the system uses a default area ID. You must specify a unique Router ID for the network element at site A. Configure OSPF to redistribute the configured default gateway so the NEs downstream forward the packets destined for the management network upstream to site A. Create an OSPF interface corresponding to the OTU2 interface.

## Other sites (Sites B and C)

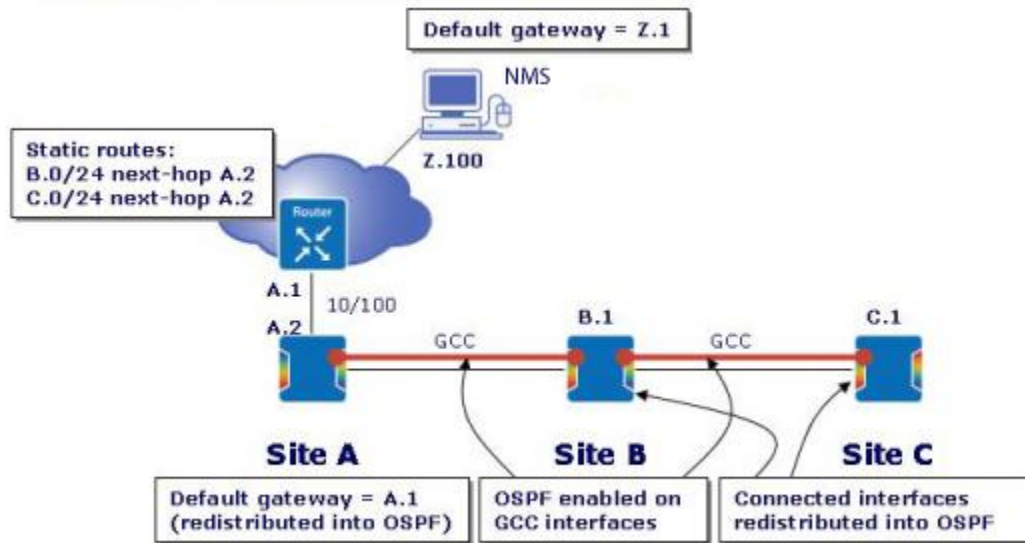
Connect sites B and C to the management network using GCC. Any communication to/from the management network will be through Site A. Configure sites B and C with unique IP addresses and subnet masks. When configuring sites B and C, assign the IP address and mask to the management LAN port (10/100BT port on MSI) even though this port is not physically connected.

Ensure site B has modules to support two OTU2 interfaces (see [1.1.1, “GCC”](#)). Ensure that site C has at least one module that supports an OTU2 interface. Configure OTU2 as the line protocol and enable GCC at Sites A, B, and C.

Enable OSPF at sites B and C. Ensure that the area ID is the same as the area ID set at site A. The router IDs at site B and C must be unique. Configure OSPF to redistribute connected interfaces. At sites B and C, create OSPF interfaces for the corresponding OTU2/GCC interfaces.

## Management Network Router

Configure static routes on the management network router to reach sites B and C. Coordinate the IP address allocation with the IT group responsible for the day-to-day operation of the management network.

**Figure 4-2 Point to point configuration details for GCC requirements**

#### 4.1.1.3 TL1 commands to implement this point-to-point scenario

##### Site A

##### 1 Set up IP address

```
ED-IP:SiteA:IP-NMS:100:::IPADDR=10.10.30.2,IPMASK=255.255.255.0;
```

##### 2 Setup Gateway to point to connected router

```
ED-SYS:SiteA::100:::GATEWAY=10.10.30.1;
```

##### 3 Enable GCC0 on the transponder's port

```
ENT-GCC0:SiteA:TPR-1-3-1:::FRATE,IP;;
```

##### 4 Redistribute Default Routes into OSPF

```
ENT-OSPF:SiteA:OSPF-1-5:100:::REDIST=ORIG;
```

##### 5 Create an OSPF interface associated with the transponder's GCC0 enabled port

```
ENT-OSPF-IF:SiteA:OSPF-1-3-1;
```

##### Site B

##### 1 Set up IP address

```
ED-IP:SiteB:IP-NMS:100:::IPADDR=20.10.30.1,IPMASK=255.255.255.0;
```

##### 2 No default gateway set

```
ED-SYS:SiteB::100:::GATEWAY=0.0.0.0;
```

##### 3 Enable GCC0 on the transponder's port

```
ENT-GCC0:SiteB:TPR-1-1-1::FRATE,IP;;
```

#### 4 Enable GCC0 on the transponder's port

```
ENT-GCC0:SiteB:TPR-1-2-1::FRATE,IP;;
```

#### 5 Redistribute connected interfaces into OSPF

```
ENT-OSPF:SiteB:OSPF-1-5:100::REDIST=CONN;
```

#### 6 Create an OSPF interface associated with the transponder's GCC0 enabled port

```
ENT-OSPF-IF:SiteB:OSPF-1-1-1;
```

#### 7 Create an OSPF interface associated with the transponder's GCC0 enabled port

```
ENT-OSPF-IF:SiteB:OSPF-1-2-1;
```

### Site C

#### 1 Set up IP address

```
ED-IP:SiteC:IP-NMS:100::IPADDR=30.10.30.1,IPMASK=255.255.255.0;
```

#### 2 No default gateway set

```
ED-SYS:SiteC::100::GATEWAY=0.0.0.0;
```

#### 3 Enable GCC0 on the transponder's port

```
ENT-GCC0:SiteC:TPR-1-6-1::FRATE,IP;;
```

#### 4 Redistribute connected interfaces into OSPF

```
ENT-OSPF:SiteC:OSPF-1-5:100::REDIST=CONN;
```

#### 5 Create an OSPF interface associated with the transponder's GCC0 enabled port

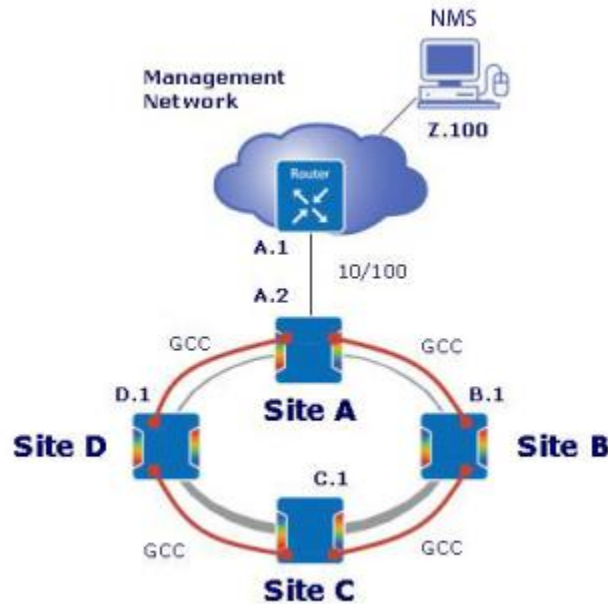
```
ENT-OSPF-IF:SiteC:OSPF-1-6-1;
```

## 4.1.2 Ring GCC applications

You can use GCC in a ring application to provides management system connectivity to all NEs in the ring. If the network fails (for example, fiber cut), you can maintain management communications.

### 4.1.2.1 Site by site configuration planning and preparation

The following figure shows a ring GCC example. In this example, four NEs are connected in a ring. The first NE at site A is directly connected to the management network using a 10/100BT Ethernet connection. Connectivity to sites B, C and D is provided using GCC between all sites.

**Figure 4-3 GCC ring example requirements**

Although this example shows four NEs in a ring, you can add more NEs as required. See [Appendix B, “Performance engineering”](#) for engineering limits.

### Preparation

Site-by-site deployment requires a number of IP addresses. Coordinate the IP address allocation with the IT group responsible for the day-to-day operation of the management network. In this example you need:

- IP address for the management station(s); for example, Z.100 in the figure above
- IP address and subnet masks for the various sites; for example, A.2, B.1, C.1. as in the figure above
- default gateway address for Site A

#### 4.1.2.2 Site by site requirements

This section identifies the specific requirements for the network elements in this example. See the figure below for GCC requirements.

#### Remote Management Station

Configure the remote management station with an IP address, subnet mask and default gateway on the management network. In this example, the IP address is Z.100 and the default gateway is Z.1.

### Near-end Site (Site A)

Connect the near end site to the management network using a 10/100BT Ethernet port on the MSI (management LAN port). Assign an IP address, subnet mask and default gateway to the port.

Ensure you have sufficient modules to support two OTU2 interfaces with GCC functionality in the near-end site. Refer to [1.1.1, “GCC”](#). Set the modules line protocol to OTU2 and enable GCC. The ports do not require an IP address as BTI 7000 Series treats GCC interfaces as un-numbered interfaces.

Enable OSPF at Site A. Specify an area ID and router ID when enabling OSPF. If no area ID is specified the system uses a default area ID (0.0.28.208). You must set a unique Router ID for the network element at site A.

Configure OSPF to redistribute the configured default gateway so the NEs downstream forward the packets destined for the management network upstream to site A. Enable GCC on OTU2 interfaces. Create an OSPF interface corresponding to each OTU2 interface.

### Other sites (Sites B, C and D)

Connect sites B, C and D to the management network using GCC. Any communication to and from the management network is through Site A. Configure sites B, C and D with unique IP addresses and subnet masks. When configuring sites B and C, assign the IP address and mask to the management LAN port (10/100BT port on MSI) even though this port is not physically connected.

Ensure sites B, C, and D, have enough modules to support two OTU2 interfaces per site. As at site A, configure OTU2 as the line protocol and enable GCC.

Enable OSPF at sites B, C and D. Ensure that the area ID is the same as the area ID set at site A. Ensure that the router IDs at site B, C and D are unique. Configure OSPF to redistribute connected interfaces if there are local subnets you want to advertise within the OSPF area (e.g. MVLAN or IP-Craft subnets). Otherwise, leave OSPF route redistribution set to 'None'.

<b>Note</b>	you do not need to set route redistribution to Connected in order to advertise the IP-NMS subnet within OSPF as this is done automatically.
-------------	---

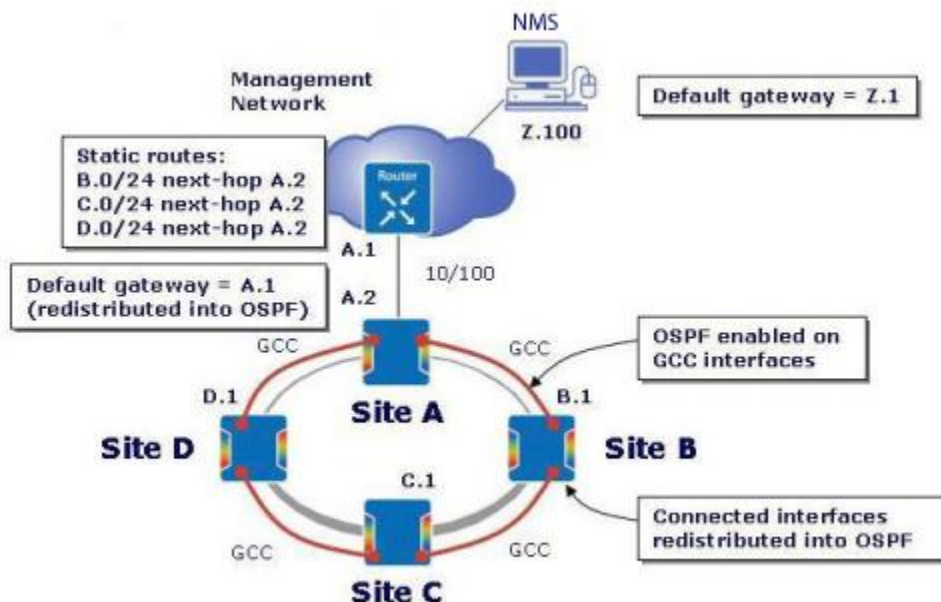
At sites B, C and D, create OSPF interfaces for the corresponding OTU2/GCC interfaces.

The OSPF protocol determines the best routes to sites B, C and D from site A. If there is a network failure, OSPF will select an alternative route to sites B, C and D.

### Management Network Router

Configure static routes on the management network router to reach sites B, C and D. Ensure you coordinate this with the IT group responsible for the day-to-day operations of the management network.

Figure 4-4 Ring GCC example configuration details for routing



#### 4.1.2.3 TL1 commands to implement this ring scenario

##### Site A

##### 1 Set up IP address

```
ED-IP:SiteA:IP-NMS:100:::IPADDR=10.10.30.2,IPMASK=255.255.255.0;
```

##### 2 Setup Gateway to point to connected router

```
ED-SYS:SiteA::100:::GATEWAY=10.10.30.1;
```

##### 3 Enable GCC0 on the transponder's port

```
ENT-GCC0:SiteA:TPR-1-3-1:::FRATE,IP;;
```

##### 4 Enable GCC0 on the transponder's port

```
ENT-GCC0:SiteA:TPR-1-3-3:::FRATE,IP;;
```

##### 5 Redistribute Default Routes into OSPF

```
ENT-OSPF:SiteA:OSPF-1-5:100:::REDIST=ORIG;
```

##### 6 Create an OSPF interface associated with the transponder's GCC0 enabled port

```
ENT-OSPF-IF:SiteA:OSPF-1-3-1;
```

##### 7 Create an OSPF interface associated with the transponder's GCC0 enabled port

```
ENT-OSPF-IF:SiteA:OSPF-1-3-3;
```

## Site B

### 1 Set up IP address

```
ED-IP:SiteB:IP-NMS:100:::IPADDR=20.10.30.1,IPMASK=255.255.255.0;
```

### 2 No default gateway set

```
ED-SYS:SiteB::100:::GATEWAY=0.0.0.0;
```

### 3 Enable GCC0 on the transponder's port

```
ENT-GCC0:SiteB:TPR-1-1-1:::FRATE,IP;;
```

### 4 Enable GCC0 on the transponder's port

```
ENT-GCC0:SiteB:TPR-1-2-1:::FRATE,IP;;
```

### 5 Redistribute connected interfaces into OSPF

```
ENT-OSPF:SiteB:OSPF-1-5:100:::REDIST=CONN;
```

### 6 Create an OSPF interface associated with the transponder's GCC0 enabled port

```
ENT-OSPF-IF:SiteB:OSPF-1-1-1;
```

### 7 Create an OSPF interface associated with the transponder's GCC0 enabled port

```
ENT-OSPF-IF:SiteB:OSPF-1-2-1;
```

## Site C

### 1 Set up IP address

```
ED-IP:SiteC:IP-NMS:100:::IPADDR=30.10.30.1,IPMASK=255.255.255.0;
```

### 2 No default gateway set

```
ED-SYS:SiteC::100:::GATEWAY=0.0.0.0;
```

### 3 Enable GCC0 on the transponder's port

```
ENT-GCC0:SiteC:TPR-1-6-1:::FRATE,IP;;
```

### 4 Enable GCC0 on the transponder's port

```
ENT-GCC0:SiteC:TPR-11-4-1:::FRATE,IP;;
```

### 5 Redistribute connected interfaces into OSPF

```
ENT-OSPF:SiteC:OSPF-1-5:100:::REDIST=CONN;
```

### 6 Create an OSPF interface associated with the transponder's GCC0 enabled port

```
ENT-OSPF-IF:SiteC:OSPF-1-6-1;
```

### 7 Create an OSPF interface associated with the transponder's GCC0 enabled port

```
ENT-OSPF-IF:SiteC:OSPF-11-4-1;
```

## Site D

### 1 Set up IP address



```
ED-IP:SiteD:IP-NMS:100:::IPADDR=40.10.30.1,IPMASK=255.255.255.0;
```

**2 No default gateway set**

```
ED-SYS:SiteD::100:::GATEWAY=0.0.0.0;
```

**3 Enable GCC0 on the transponder's port**

```
ENT-GCC0:SiteD:TPR-1-3-1:::FRATE,IP;;
```

**4 Enable GCC0 on the transponder's port**

```
ENT-GCC0:SiteD:TPR-1-3-3:::FRATE,IP;;
```

**5 Redistribute connected interfaces into OSPF**

```
ENT-OSPF:SiteD:OSPF-1-5:100:::REDIST=CONN;
```

**6 Create an OSPF interface associated with the transponder's GCC0 enabled port**

```
ENT-OSPF-IF:SiteD:OSPF-1-3-1;
```

**7 Create an OSPF interface associated with the transponder's GCC0 enabled port**

```
ENT-OSPF-IF:SiteD:OSPF-1-3-3;
```

### 4.1.3 Point-to-point GCC with line protection

This example illustrates how GCC communications works with 1+1 line protection. This type of configuration is typical when you have the Dual 10G Transponder in your network. See [4.1.3.1, “Site by site configuration planning and preparation”](#).

#### 4.1.3.1 Site by site configuration planning and preparation

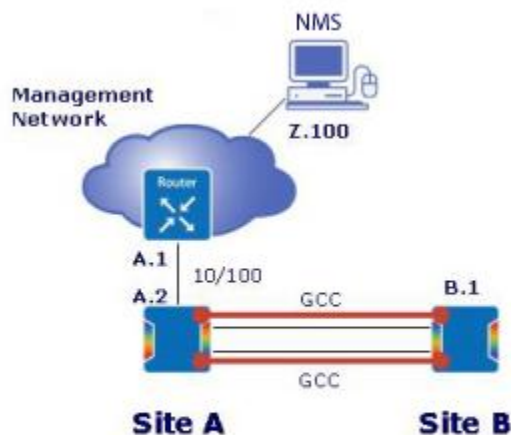
You can configure the GCC communications channel to be redundant or not to be redundant. If you do not configure the GCC communications channel to be redundant, then this configuration is identical to the point-point configuration described in the following figure. If GCC is configured to be redundant, then this configuration is identical to the ring configuration described in the previous section but with two NEs instead of four.

In the redundant configuration example shown the following figure, you must configure GCC between sites A and B. Otherwise GCC is not protected by the 1+1 line protection mechanism.

#### Preparation

Site-by-site deployment requires a number of IP addresses. Coordinate the IP address allocation with the IT group responsible for the day-to-day operation of the management network. In this example you need:

- IP addresses for the management station(s), for example, Z.100
- IP addresses and subnet masks for the various sites (for example, A.2, B.1)
- default gateway address for Site A

**Figure 4-5 Point to point GCC application with protection**

#### 4.1.3.2 Site by site requirements

This section identifies the specific requirements for the network elements in this example. See the figure below for GCC requirements.

##### Remote Management Station

Configure the remote management station with an IP address, subnet mask and default gateway provided by the IT group. In this example the IP address is Z.100 and the default gateway is Z.1.

##### Near-end Site (Site A)

Connect site A to the management network using a 10/100BT Ethernet port on the MSI (management LAN port). In this example, the IP address for this port is configured to A.2. The default gateway is set to A.1 (the address of the management network router).

Ensure that site A has two GCC-supporting OTU2 interfaces (refer to 1.1.1, “GCC”) that are connected to site B. Configure the two OTU2 interfaces for 1+1 line protection. Enable GCC for each OTU2 interface.

Enable OSPF at Site A. Specify an area ID and router ID after you enable OSPF. If no area ID is specified the system uses a default area ID. Ensure the Router ID for the network element at site A is unique. Configure OSPF to redistribute the configured default gateway so the downstream NE will forward packets destined for the management network upstream to site A. Create two OSPF interfaces corresponding to the two OTU2 interfaces.

##### Far end site (Site B)

Connect site B to the management network using site A. Set the IP address of management LAN port at Site B (in this example B.1) even though this port is not physically connected to anything at site B.

Ensure site B has two GCC-supporting OTU2 interfaces (refer to [1.1.1, “GCC”](#)) that are connected to site A. Configure the two OTU2 interfaces for 1+1 line protection. Enable GCC for each OTU2 interface.

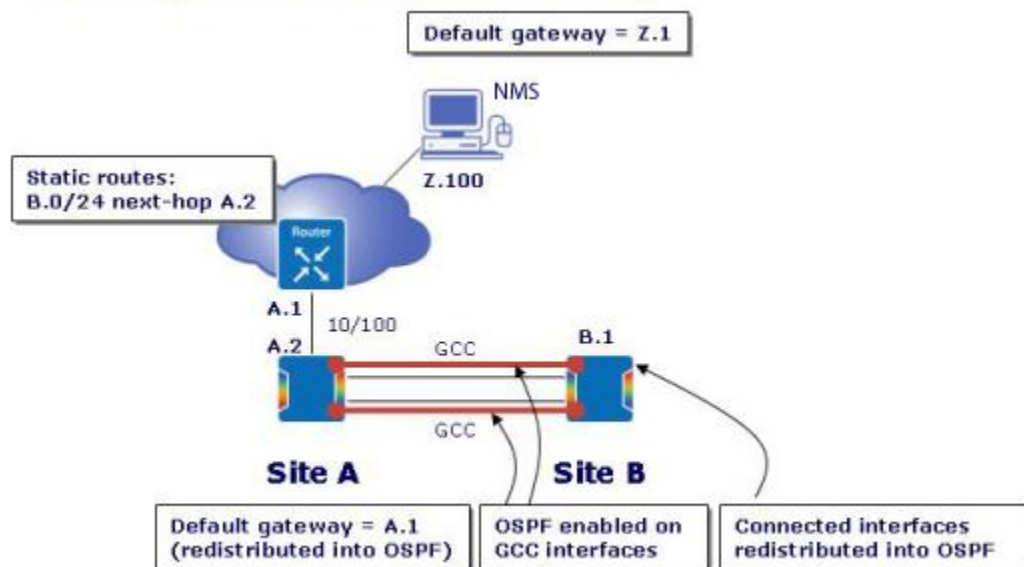
Enable OSPF at Site B. Specify an area ID and router ID after you enable OSPF. If no area ID is specified the system will use a default area ID. Create two OSPF interfaces corresponding to the two OTU2 interfaces.

The area IDs at sites A and B must be the same. Ensure that the Router ID for the network element at site B is unique. Configure OSPF to redistribute the connected interfaces.

### Management Network Router

Configure the management network router with a static route to reach site B. In this example (see figure below), B.0/24 next-hop A.2, where A.2 is the IP address of the management LAN port of the BTI 7000 Series network element at site A.

**Figure 4-6 PTP GCC application with protection - routing details**



### 4.1.3.3 TL1 commands to implement this point-to-point GCC with line protection scenario

#### Site A

##### 1 Set up IP address

```
ED-IP:SiteA:IP-NMS:100:::IPADDR=10.10.30.2,IPMASK=255.255.255.0;
```

##### 2 Setup Gateway to point to connected router

```
ED-SYS:SiteA::100:::GATEWAY=10.10.30.1;
```

**3 Enable GCC0 on the transponder's port**

```
ENT-GCC0:SiteA:TPR-1-3-1::FRATE,IP;;
```

**4 Enable GCC0 on the transponder's port**

```
ENT-GCC0:SiteA:TPR-1-3-3::FRATE,IP;;
```

**5 Redistribute Default Routes into OSPF**

```
ENT-OSPF:SiteA:OSPF-1-5:100::REDIST=ORIG;
```

**6 Create an OSPF interface associated with the transponder's GCC0 enabled port**

```
ENT-OSPF-IF:SiteA:OSPF-1-3-1;
```

**7 Create an OSPF interface associated with the transponder's GCC0 enabled port**

```
ENT-OSPF-IF:SiteA:OSPF-1-3-3;
```

**Site B****1 Set up IP address**

```
ED-IP:SiteB:IP-NMS:100::IPADDR=20.10.30.1,IPMASK=255.255.255.0;
```

**2 No default gateway set**

```
ED-SYS:SiteB::100::GATEWAY=0.0.0.0;;
```

**3 Enable GCC0 on the transponder's port**

```
ENT-GCC0:SiteB:TPR-1-1-1::FRATE,IP;;
```

**4 Enable GCC0 on the transponder's port**

```
ENT-GCC0:SiteB:TPR-1-2-1::FRATE,IP;;
```

**5 Redistribute connected interfaces into OSPF**

```
ENT-OSPF:SiteB:OSPF-1-5:100::REDIST=CONN;
```

**6 Create an OSPF interface associated with the transponder's GCC0 enabled port**

```
ENT-OSPF-IF:SiteB:OSPF-1-1-1;
```

**7 Create an OSPF interface associated with the transponder's GCC0 enabled port**

```
ENT-OSPF-IF:SiteB:OSPF-1-2-1;
```

## **4.1.4 Dual-homed GCC application**

The BTI 7000 Series supports dual-homed GCC application for networks where management communications must be maintained in the event of any network failures. See [4.1.4.2, “Site by site requirements”](#) for a dual-homed ring example.

### **4.1.4.1 Site by site configuration planning and preparation**

In this configuration, the network of BTI 7000 Series elements is connected to the management network at two points (dual-homed), specifically at sites A and D. See [4.1.4.2, “Site by site requirements”](#). All sites are interconnected using GCC connections over OTU2 interfaces.

## Preparation

Coordinate the IP address allocation with the IT group responsible for the day-to-day operation of the management network. In this example you need:

- IP addresses for the management station(s), for example, Z.100
- IP addresses and subnet masks for the various sites (for example, A.2, B.1, C.1 and D.1)
- Default gateway addresses for Sites A and D

### 4.1.4.2 Site by site requirements

This section identifies the specific requirements for the network elements in this example. See the figure below for GCC requirements.

#### Remote Management Station

Configure the remote management station with the IP address, subnet mask and default gateway provided by the IT group. In this example the IP address is Z.100 and the default gateway is Z.1.

#### Sites directly connected to the Management Network (Sites A and D)

Connect sites A and D to the management network using 10/100BT Ethernet connections from the MSI (management LAN port). Configure these IP addresses, and subnet masks for the interfaces. You do not require default gateways if you enable OSPF on these interfaces.

Ensure sites A and D have sufficient OTU2-capable modules to connect to adjacent sites. In this example, site A requires two OTU2 ports to connect to sites D and B, respectively. Enable the GCC on the OTU2 interfaces.

Enable OSPF at Sites A and D. Specify an area ID and router ID after you enable OSPF. If no area ID is specified, the system uses a default area ID. Set unique Router IDs for the network elements at sites A and D. The area ID must be the same at sites A and D.

Create OSPF interfaces for all interfaces (GCC and management LAN port) at sites A and D (this is unlike previous examples where you require OSPF interfaces only for GCC interface).

By creating an OSPF interface for the management LAN port, the management network automatically learns of failures within the network of BTI 7000 Series network elements. This provides failure recovery if site A or site D fails.

#### Other Sites (Sites B and C)

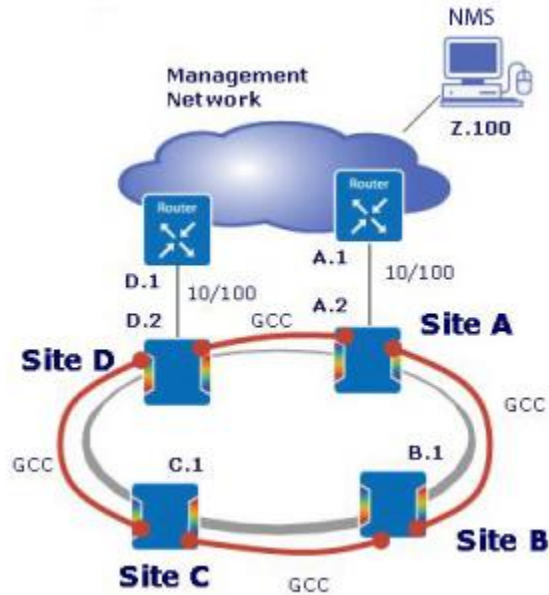
Configure site B and site C IP addresses B.1 and C.1. Ensure that the sites have OTU2 capable modules. Enable GCC on all OTU2 interfaces.

Enable OSPF at sites B and C. The area ID must match the area ID for sites A and D. Unique router IDs should be specified for sites B and C. Create OSPF interfaces for the corresponding OTU2 interfaces.

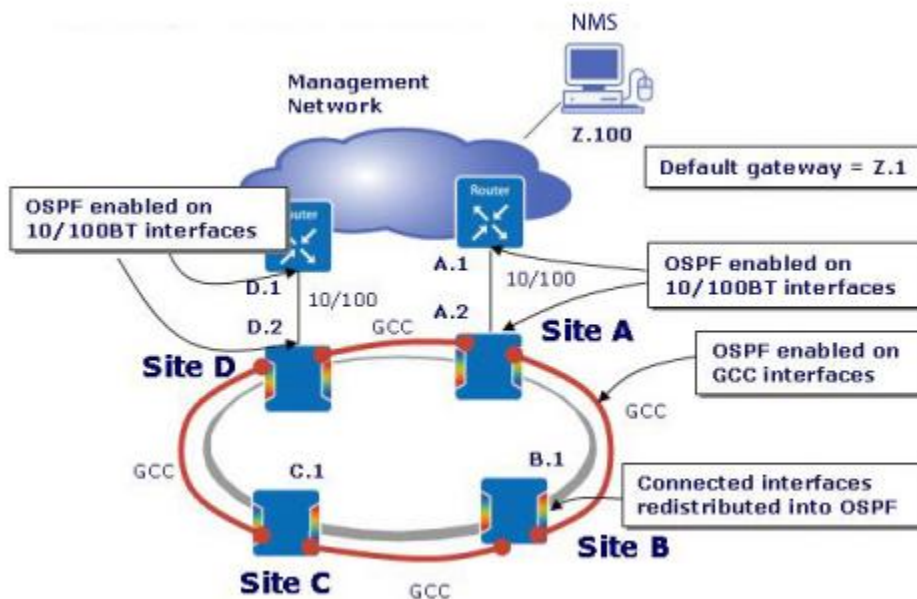
## Management Network Routers

Static routes are not required on the management network routers. Instead, you must run the OSPF protocol on the Ethernet interfaces connecting to the BTI 7000 Series network elements at Sites A and D. The area ID must match the area ID used within the BTI 7000 Series network.

**Figure 4-7 Dual-homed GCC application requirements**



**Figure 4-8 Dual-homed GCC application - continued**



### 4.1.4.3 TL1 commands to implement this dual-homed GCC scenario

#### Site A

**1 Set up IP address**

```
ED-IP:SiteA:IP-NMS:100:::IPADDR=10.10.30.2,IPMASK=255.255.255.0;
```

**2 No default gateway set**

```
ED-SYS:SiteA::100:::GATEWAY=0.0.0.0;
```

**3 Enable GCC0 on the transponder's port**

```
ENT-GCC0:SiteA:TPR-1-3-1:::FRATE,IP;;
```

**4 Enable GCC0 on the transponder's port**

```
ENT-GCC0:SiteA:TPR-1-3-3:::FRATE,IP;;
```

**5 Set route redistribution to “NONE” (no external interfaces)**

```
ENT-OSPF:SiteA:OSPF-1-5:100:::REDIST=NONE;
```

**6 Create an OSPF interface associated with the transponder's GCC0 enabled port**

```
ENT-OSPF-IF:SiteA:OSPF-1-3-1;
```

**7 Create an OSPF interface associated with the transponder's GCC0 enabled port**

```
ENT-OSPF-IF:SiteA:OSPF-1-3-3;
```

**8 Create an OSPF interface associated with the IP-NMS port**

```
ENT-OSPF-IF:SiteA:OSPF-1-5-1;
```

#### Site B

**1 Set up IP address**

```
ED-IP:SiteB:IP-NMS:100:::IPADDR=20.10.30.1,IPMASK=255.255.255.0;
```

**2 No default gateway set**

```
ED-SYS:SiteB::100:::GATEWAY=0.0.0.0;
```

**3 Enable GCC0 on the transponder's port**

```
ENT-GCC0:SiteB:TPR-1-1-1:::FRATE,IP;;
```

**4 Enable GCC0 on the transponder's port**

```
ENT-GCC0:SiteB:TPR-1-2-1:::FRATE,IP;;
```

**5 Redistribute connected interfaces into OSPF**

```
ENT-OSPF:SiteB:OSPF-1-5:100:::REDIST=CONN;
```

**6 Create an OSPF interface associated with the transponder's GCC0 enabled port**

```
ENT-OSPF-IF:SiteB:OSPF-1-1-1;
```

**7 Create an OSPF interface associated with the transponder's GCC0 enabled port**

```
ENT-OSPF-IF:SiteB:OSPF-1-2-1;
```

## Site C

### 1 Set up IP address

```
ED-IP:SiteC:IP-NMS:100:::IPADDR=30.10.30.2,IPMASK=255.255.255.0;
```

### 2 No default gateway set

```
ED-SYS:SiteC::100:::GATEWAY=0.0.0.0;
```

### 3 Enable GCC0 on the transponder's port

```
ENT-GCC0:SiteC:TPR-1-6-1:::FRATE,IP;;
```

### 4 Enable GCC0 on the transponder's port

```
ENT-GCC0:SiteC:TPR-11-4-1:::FRATE,IP;;
```

### 5 Redistribute connected interfaces into OSPF

```
ENT-OSPF:SiteC:OSPF-1-5:100:::REDIST=CONN;
```

### 6 Create an OSPF interface associated with the transponder's GCC0 enabled port

```
ENT-OSPF-IF:SiteC:OSPF-1-6-1;
```

### 7 Create an OSPF interface associated with the transponder's GCC0 enabled port

```
ENT-OSPF-IF:SiteC:OSPF-11-4-1;
```

## Site D

### 1 Set up IP address

```
D-IP:SiteD:IP-NMS:100:::IPADDR=40.10.30.2,IPMASK=255.255.255.0;
```

### 2 No default gateway set

```
ED-SYS:SiteD::100:::GATEWAY=0.0.0.0;
```

### 3 Enable GCC0 on the transponder's port

```
ENT-GCC0:SiteD:TPR-1-3-1:::FRATE,IP;;
```

### 4 Enable GCC0 on the transponder's port

```
ENT-GCC0:SiteD:TPR-1-3-3:::FRATE,IP;;
```

### 5 Set route redistribution to “NONE” (no external interfaces)

```
ENT-OSPF:SiteD:OSPF-1-5:100:::REDIST=NONE;
```

### 6 Create an OSPF interface associated with the transponder's GCC0 enabled port

```
ENT-OSPF-IF:SiteD:OSPF-1-3-1;
```

### 7 Create an OSPF interface associated with the transponder's GCC0 enabled port

```
ENT-OSPF-IF:SiteD:OSPF-1-3-3;
```

### 8 Create an OSPF interface associated with the IP-NMS port



ENT-OSPF-IF:SiteD:OSPF-1-5-1;

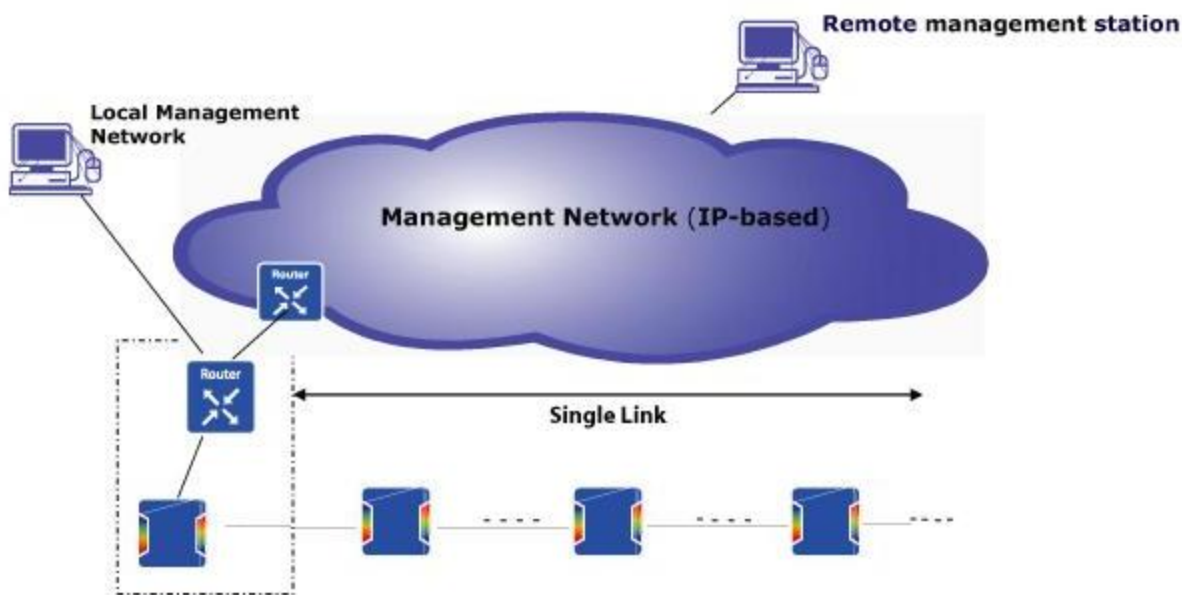
### 4.1.5 Point-to-point or linear OSC applications

The point-to-point OSC application includes:

- BTI 7000 Series network elements managed from a local or a remote management station
- BTI 7000 Series network elements deployed in a linear span
- Out-of-band management communications to BTI 7000 Series systems along the link

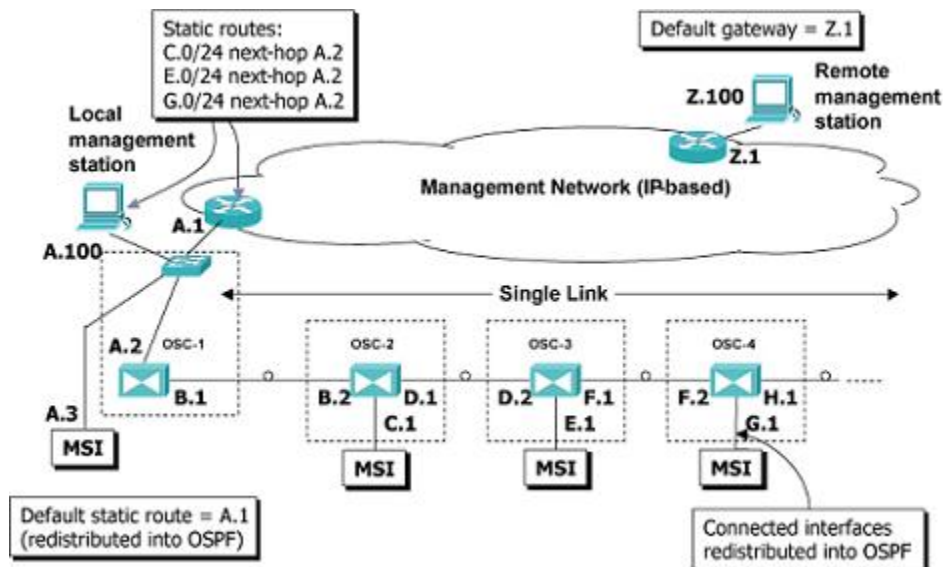
The following figure shows the single-homed OSC application.

**Figure 4-9 Single-homed OSC application**



#### 4.1.5.1 Site by site configuration planning and preparation

The following figure shows an example of site-by-site configuration planning requirements.

**Figure 4-10 Ethernet, IP Address and subnet requirements**

## Preparation

The following sections list the specific requirements for the different elements in an OSC application.

Obtain the following from the IT group responsible for the day-to-day operation of the management network:

- IP addresses for the management stations. For an example, see Z.100 and A.100 in the figure in 4.1.4.2, “Site by site requirements”.
- IP addresses and default gateway for the SCP modules at the various sites. For an example, see A.2, A.3, A.4, A.5 in the figure in 4.1.5.2, “Site by site requirements”.

**Note** All management LAN port addresses must be on the same subnet.

## 4.1.5.2 Site by site requirements

### Remote Management Station

Configure the local management station with an IP address, mask and default gateway (if not already set). The figure in 4.1.5.1, “Site by site configuration planning and preparation” shows the following: IP address = A.100, mask = 255.255.255.0, and gateway = A.1.

### Local management station

Configure the local management station with an IP address, mask and default gateway (if not already set). The figure in 4.1.5.1, “Site by site configuration planning and preparation” shows the following: IP address = A.100, mask = 255.255.255.0, and gateway = A.1.

### Near-end Site (Site 1)

Configure the following at the end site:

- One physical connection to the management LAN port at the end site for the MSI port.
- IP address and default gateway for the SCP module. For example, the figure in [4.1.5.1, “Site by site configuration planning and preparation”](#) shows IP addresses = A.2, masks =255.255.255.0, and the gateway = A.1.
- The OSC2 optical port on the SCP module connects to A.3 on the OSC1 optical port on the SCP module at the next site.

<b>Note</b>	The optical connections from the OSC ports on the SCP module are physically routed through the OSC coupler/splitter module for transport to the adjacent NEs.
-------------	---

The following connections are required at the near end site:

- Connect the Management LAN port on the MSI to the border router.
- Connect the OSC2 port on the SCP to the OSC1 port on the SCP at the next site.

### Line sites (Site 2, 3, 4)

IP address and default gateway for the SCP module. For example, the following figure shows IP addresses = A.3, masks =255.255.255.0, and the gateway = A.1 for site 2.

The following connections are required at a line site:

- Connect the OSC1 port on the SCP to the OSC2 port on the SCP at the previous site.
- Connect the OSC2 port on the SCP to the OSC1 port on the SCP at the next site.

### Far end site (Site n)

IP address for the SCP module.

The following connections are required at the far end site:

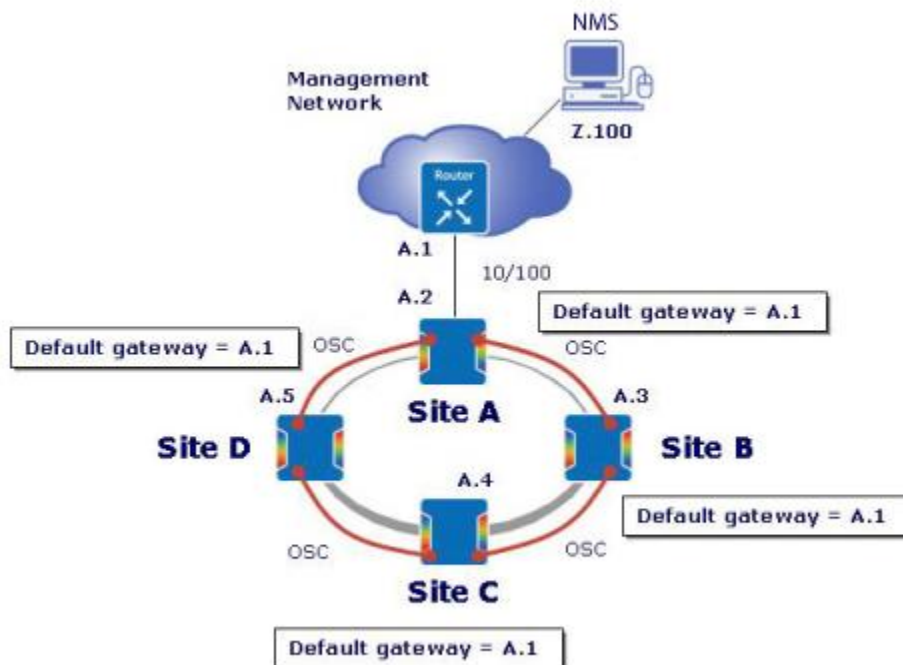
- Connect the OSC1 port on the SCP to the OSC2 port on the SCP at the previous site.

## 4.1.6 Ring OSC application

You can use the OSC in ring applications. The BTI 7000 Series supports STP to break loops in ring configurations and to re-route management communications traffic in the event of a network failure.

### 4.1.6.1 Site by site configuration planning and preparation

The following figure shows an OSC ring configuration.

**Figure 4-11 OSC ring configuration**

### Preparation

Obtain the following from the IT group responsible for the day-to-day operation of the management network:

- IP addresses for the management station, for example, Z.100.
- IP addresses and default gateway for the BTI 7000 Series network elements at the various sites (for example, A.2, A.3, A.4, A.5).

**Note** All IP addresses must be on the same subnet.

### 4.1.6.2 Site by site requirements

#### Remote Management Station

Configure the remote management station with an IP address, subnet mask and default gateway you obtain from the IT group. In this example, (see figure in [4.1.6.1, “Site by site configuration planning and preparation”](#)) the IP address is Z.100 and the default gateway is Z.1.

#### Near-end Site (Site A)

Configure site-A with an IP address, subnet mask and default gateway. In this example, the IP address is A.2 and the default gateway is A.1.

The OSC ports on the SCP must be equipped with OSC SFPs for communication to sites B and D. Two coupler/splitters, or a dual coupler/splitter are required to couple the OSC signal onto the traffic carrying fiber.

Enable the OSC. STP is enabled by default.

### **Other sites (Sites B, C and D)**

Configure sites B, C and D with IP addresses, subnet masks and default gateways. In this example, the IP addresses for the 3 sites are: A.3, A.4 and A.5, respectively. Configure all sites with the same default gateway, in this example A.1.

The OSC ports on the SCP must be equipped with OSC SFPs for communication to the adjacent sites. Two coupler/splitters, or a dual coupler/splitter are also required to couple the OSC signal onto the traffic-carrying fiber.

Enable the OSC. STP is enabled by default.

### **Management Network Router**

No configuration is required on the management network router.

## 4.2 Management access and connectivity over IP networks

---

BTI 7000 Series network elements can be managed using TCP/IP protocols. In addition, transfers of software files or configuration databases can be performed using FTP. The TCP/UDP ports for these protocols are listed the following table.

**Table 4-1 Management access ports**

Port number	Service	Configurable	Closeable	Service can be stopped	Usage
161	SNMP	No	No	No	SNMP management, proNX 900
3022	SSH - TL1	No	No	No	SSH mode TL1 protocol over an encrypted link
3082	TL1 ( proNX 900)	No	No	No	proNX 900 TL1 interface (exclusive to proNX 900)
3083	Telnet - TL1 (user)	No	No	No	TL1 ASCII user interface
3084	Telnet - CLI	No	No	No	CLI user interface
8022	SSH - CLI	No	No	No	SSH CLI
20, 21	FTP client	No	NA	NA	System upgrades (outbound only)
162	SNMP traps	Yes	NA	NA	SNMP alarm reporting (outbound only)

## 5.0 Installing or replacing modules

---

This section describes how to install, connect and replace modules.

- [t-CE\\_install\\_7060\\_SCP.xml](#)
- [t-CE\\_install\\_7200\\_SCP.xml](#)
- 5.3, “Installing SFP transceivers”
- 5.4, “Installing and fibering a Coupler/Splitter module”
- 5.5, “Replacing the System Control Processor module”
- 5.6, “Replacing SFP transceivers”
- 5.7, “Replacing Coupler/Splitters”

## 5.1 Install the System Control Processor module in a BTI 7060

Use this procedure to install the BTI 7060 System Control Processor (SCP) module.

### What you need

- Slot-head or Phillips screwdriver
- Electrostatic discharge (ESD) wrist strap
- BTI 7060 SCP module

### Prerequisites

- The BTI 7060 MSI module and the BTI 7060 Cooling Unit module are already installed.

### Installation procedure

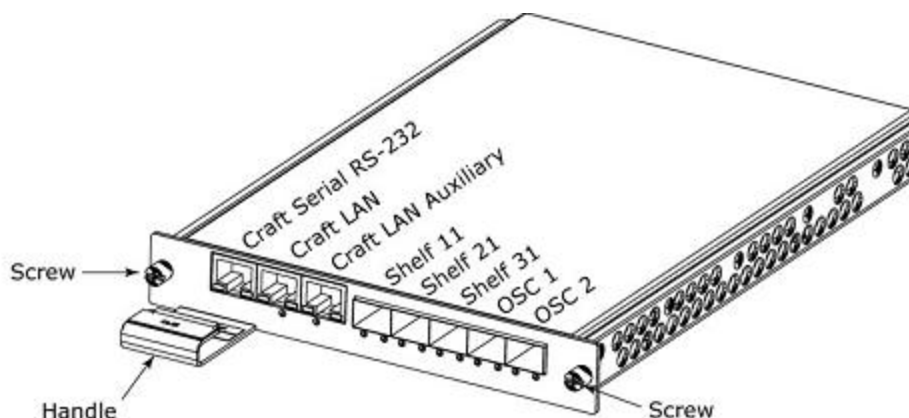


**Caution**

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

The following figure shows an SCP module and its key features for this procedure.

**Figure 5-1 SCP module**



**Note** The SCP module must be installed in slot five of the main shelf.

Follow these steps to install an SCP module:



**Step 1 Insert module**

- a) Align the SCP module with the guides in slot five.
- b) Slide the module straight into the slot.

**Step 2 Tighten faceplate screws**

- a) Facing the front of the shelf, align the module with its two mounting holes.
- b) Using a slot-head or Phillips screwdriver, carefully tighten the faceplate screws in sequence:
  - c) Partially tighten one screw.
  - d) Partially tighten the other screw.
  - e) Fully tighten the first screw.
  - f) Fully tighten the remaining screw.

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

You have successfully completed this procedure.

## 5.2 Install the System Control Processor module in a BTI 7200

Use this procedure to install the System Control Processor (SCP) module in a BTI 7200 shelf.

### What you need

- Slot-head or Phillips screwdriver
- Electrostatic discharge (ESD) wrist strap
- SCP module

### Prerequisites

- The Cooling Unit, MSI, and CCM modules are already installed.

### Installation procedure

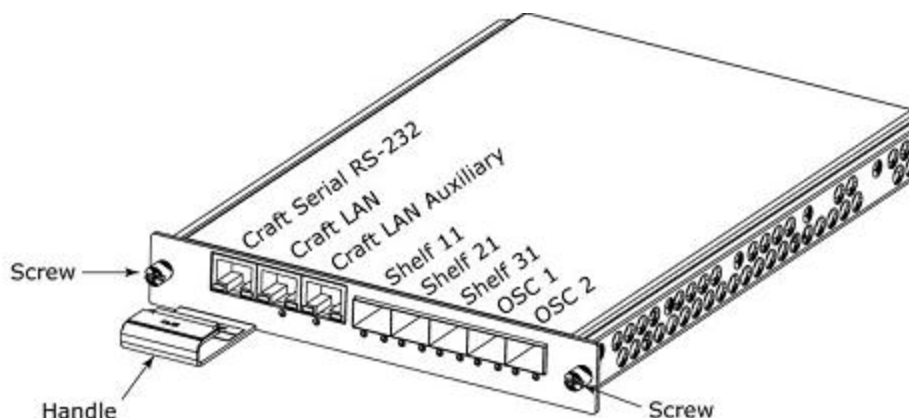


#### Caution

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

The following figure shows an SCP module and its key features for this procedure.

**Figure 5-2 SCP module**



**Note** The SCP module must be installed in slot one of the main shelf.

Follow these steps to install an SCP module:

**Step 1 Insert module**

- a) Align the SCP module with the guides in slot one.
- b) Slide the module straight into the slot.

**Step 2 Tighten faceplate screws**

- a) Facing the front of the shelf, align the module with its two mounting holes.
- b) Using a slot-head or Phillips screwdriver, carefully tighten the faceplate screws in sequence:
  - c) Partially tighten one screw.
  - d) Partially tighten the other screw.
  - e) Fully tighten the first screw.
  - f) Fully tighten the remaining screw.

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

You have successfully completed this procedure. It may take several minutes for the SCP to come fully into service, indicated by a green "Active" LED, and an unlit "Fail" LED.

## 5.3 Installing SFP transceivers

Use this procedure to install small form factor pluggable (SFP) transceivers.

### What you need

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

### Prerequisites

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

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

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



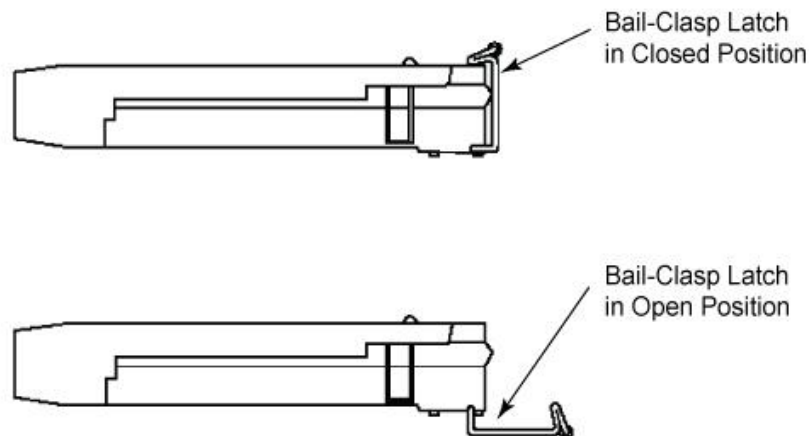
**Caution**

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

### SFP transceiver

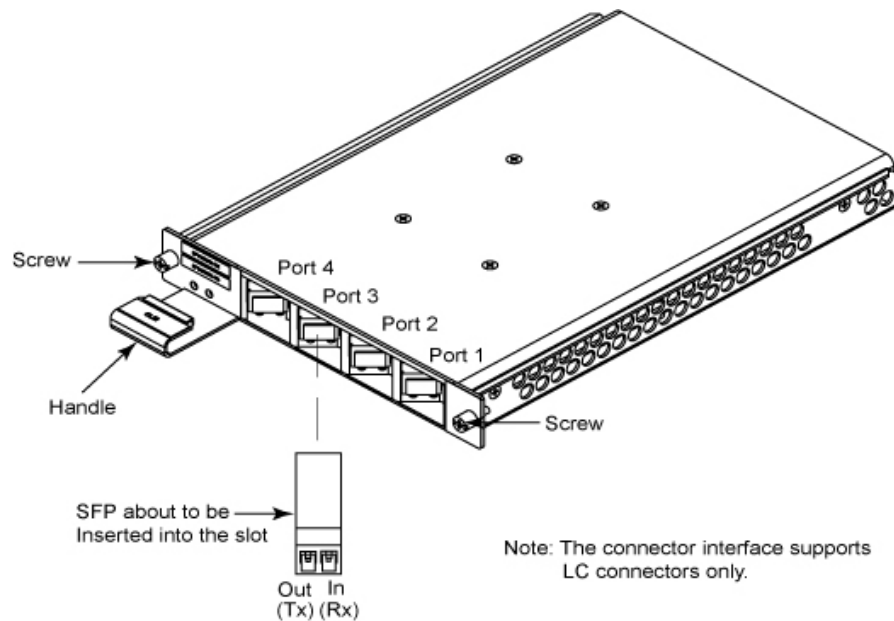
The following figure shows a typical SFP transceiver with a bale-clasp latch.

#### SFP transceiver with a bale-clasp latch



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

### SFP insertion



### Installation procedure

Follow these steps to install an SFP transceiver:

#### Step 1 Insert the SFP Transceiver

**Note** SFP transceiver ports are numbered one through four starting on the right side of the wavelength conversion module.

- a) Hold the transceiver so that the optical connectors face you and the product label is visible.
- b) Ensure that the latch is in the closed position.
- c) Align the transceiver to the port in which it is being inserted.
- d) Carefully slide the transceiver straight into the port until it clicks.
  - If the red Fail LED turns on, there is a transceiver fault. For information about clearing the fault, see the *Alarm and Troubleshooting Guide*.
  - If the yellow LOS LED turns on, there is no valid modulated signal connected to the transceiver. This condition clears once a valid modulated signal is connected.
- e) Remove the plastic protective cover, if fitted.

#### Step 2 Clean the Ends of the Fiber Optic Cables

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

#### Step 3 Connect the Input and Output Optical Cables

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

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

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

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

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

You have successfully completed this procedure.

## 5.4 Installing and fibering a Coupler/Splitter module

Use this procedure to install and connect a BTI 7000 Series coupler/splitter module on the BTI 7000 Series main shelf.

### What you need

- Slot-head or Phillips screwdriver
- Electrostatic discharge (ESD) wrist strap
- Coupler/splitter module
- Isopropyl alcohol and lint-free pads

### Prerequisites

- None



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

### Installation procedure

Follow these steps to install a coupler/splitter module:

#### Step 1 At the shelf:

- a) If a module is in the slot in which you want to install the module and its coupler/splitter assembly, do the following. Otherwise, go to step 2.
- b) Facing the front of the shelf, locate the module screws.
- c) Using a slot-head or Phillips screwdriver, unfasten module screws.
- d) Using the handle, carefully pull the module out.

#### Step 2 Insert the module and its Coupler/Splitter assembly.

- a) Align the module and its coupler/splitter assembly to the slot in which the module is being inserted.
- b) Carefully push the module straight into the slot.

#### Step 3 Attach the faceplate screws.

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

- Fully tighten the center support screw.
- Fully tighten the other screw.

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

**Step 4 Clean the ends of the fiber optic cables.**

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

**Step 5 Connect the fiber optic cables.**



## 5.5 Replacing the System Control Processor module

Use this procedure to replace the SCP.

### What you need

- Slot-head or Phillips screwdriver
- Electrostatic discharge (ESD) wrist strap
- SCP module

### Prerequisites

- None

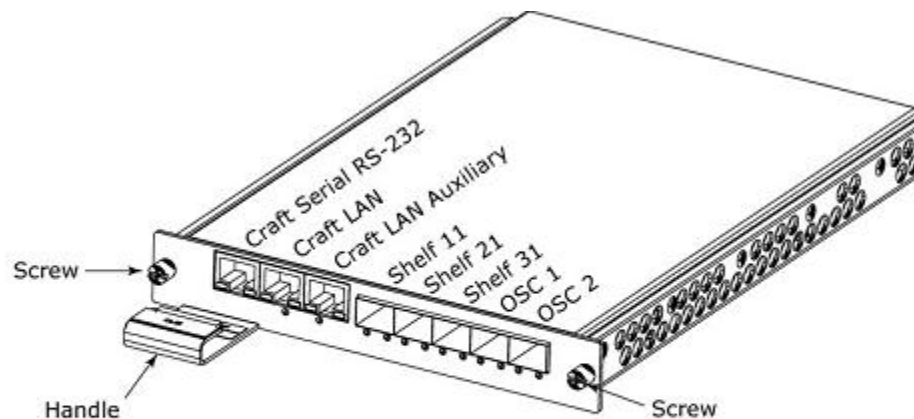


**Caution**

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

The following figure shows an SCP module and its key features for this procedure.

**Figure 5-5 SCP module**



### Replacement procedure

Follow these steps to replace the SCP module:

#### Step 1 Determine whether the SCP is still functioning

If any of the following conditions apply, the SCP is not functioning:

- CONTCOM (Control Communications) alarm raised against all modules

- REPLUNITFAIL (Equipment Failure) alarm raised against all modules
- No LEDs lit on the SCP
- All LEDs lit on the MSI and SCP for more than five minutes
- Unable to successfully log in to the BTI 7000 Series through the management or craft LAN ports or the craft serial port (assuming your PC connection is working correctly)

Based on the status of the above conditions, proceed as follows:

- If the SCP is still functioning, go to the next step.
- If the SCP is not functioning, go to step 3.

### **Step 2 Perform a Remote Database Backup**

- a) Before removing the System Control Processor (SCP) module, perform a remote database backup. For further details refer to the *BTI 7000 Series Operation Solutions Guide*.
- b) Continue with the next step after the database backup is completed.

### **Step 3 Disable the office alarms**

Disconnect the office alarms connector on the MSI to avoid multiple audible and visual alarms from being raised when booting the SCP.

### **Step 4 At the shelf:**

- a) Disconnect SCP Cables.
- b) Disconnect the SCP cables from the faceplate of the module. These include the following:
  - Craft LAN cable
  - Craft serial cable

### **Step 5 Remove Faceplate Screws**

- a) Facing the front of the shelf, locate the SCP module screws.
- b) Using a slot-head or Phillips screwdriver, loosen and remove the two screws.

### **Step 6 Remove module**

Grasp the handles on the front of the SCP module and firmly pull the module straight out.

<b>Note</b>	After the SCP is removed, all TL1 sessions are terminated as connectivity to the SCP is lost.
-------------	---

### **Step 7 Replace SCP**

- a) Align the replacement SCP to the guides of the slot in which the module is being replaced.

- b) Carefully push the module straight into the slot.
- c) Push with sufficient pressure to feel the backplane connector snap into place.

**Step 8 Replace Faceplate Screws**

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

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

**Step 9 Reconnect the SCP Cables**

Reconnect the SCP cables to the faceplate of the module.

**Step 10 Log in to the new SCP using proNX 900 Node Controller or TL1 directly**

If you did not perform the remote database backup as instructed in step 2, perform the backup before going to the next step.

**Step 11 Determine whether the system database needs to be restored**

- If it was necessary to perform a remote database backup before replacing the SCP, go to the next step.
- If performing an SCP upgrade, see the *Upgrade Guide*.

**Step 12 Restore the system database**

Restore the database to service using a backup file. Once the database is restored, go to the next step.

**Step 13 Re-enable the office alarms**

Reconnect the office alarm connector to the MSI. This re-establishes the office alarm connectivity.

You have successfully completed this procedure.

## 5.6 Replacing SFP transceivers

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

### What you need

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

### Prerequisites

- None

#### Note

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

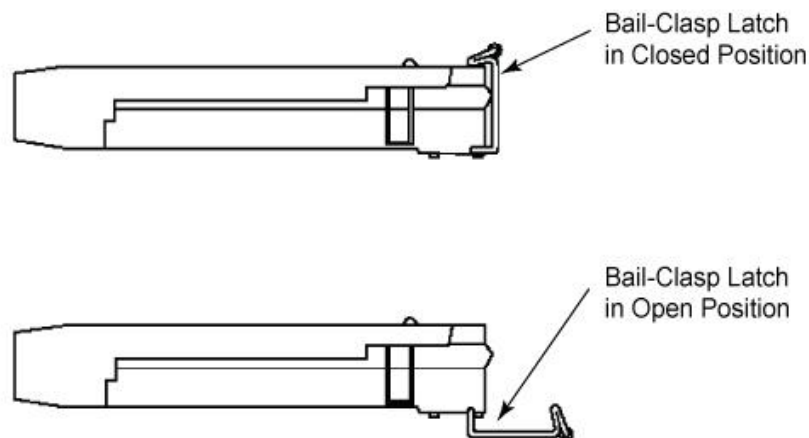


#### Caution

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

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

### SFP transceiver key features

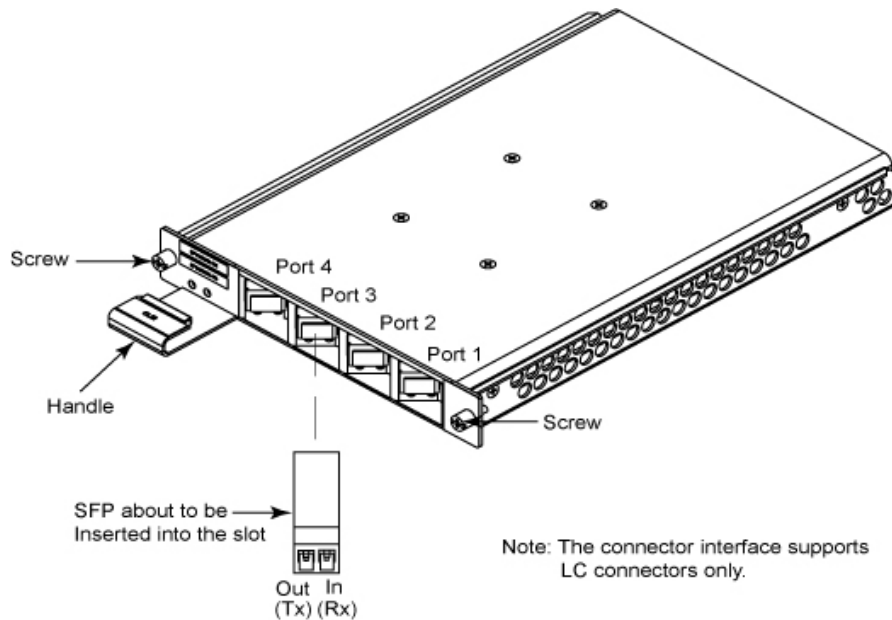


#### Note

SFPs for the expansion shelf interface (ESI) module are inserted upside down.

The following figures show an SFP transceiver about to be inserted into its slot.

## SFP insertion



## Precautions

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

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

## Replacement procedure

Follow these steps to replace an SFP transceiver:

### Step 1 Reroute Traffic

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

### Step 2 Remove SFP port from service

The port must be taken out of service. For information, see "RMV-XCVR" in the *TL1 Reference Guide*.

### Step 3 Move Cables

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

#### **Step 4 Disconnect Optical Cables**

Disconnect the optical cables from the optical ports of the SFP transceiver.

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

#### **Step 5 Disengage Latch Handle**

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

#### **Step 6 Remove Transceiver**

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

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

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

#### **Step 7 Insert the SFP transceiver**

- a) Hold the SFP transceiver so that the optical connectors face you and the product label is visible.
- b) Ensure that the latch handle is in the closed position. For a bale-clasp latch, this is in the upright position.
- c) Align the SFP transceiver to the port in which the transceiver is being inserted.
- d) Carefully slide the SFP transceiver straight into the port until it clicks.

**Note** If the SFP port is provisioned and the replacement SFP has the same the wavelength, the SFP missing alarm (REPLUNITMISS) clears.

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

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

#### **Step 8 Clean the Ends of the Fiber Optic Cables**

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

#### **Step 9 Connect the Optical Cables**

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

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

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

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

#### **Step 10 Restore SFP port to service**

Restore the port to service. For information, see "RST-XCVR" in the *TL1 Reference Guide*.

#### **Step 11 Replace Cables**

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

You have successfully completed this procedure.

## 5.7 Replacing Coupler/Splitters

---

Use this procedure to replace the 1310 nm and C-Band Coupler/Splitter (CS) (BP1A38AA) module.

### What you need

- Slot-head or Phillips screwdriver
- Electrostatic discharge (ESD) wrist strap
- Replacement coupler/splitter module
- Isopropyl alcohol and lint-free pads

### Prerequisites

- None



**Caution**

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

### Replacement procedure

Follow these steps to replace a coupler/splitter module:

#### Step 1 Reroute Traffic

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

#### Step 2 Move Cables

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

#### Step 3 Disconnect Optical Cables

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

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

#### Step 4 Loosen Faceplate Screws

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

#### Step 5 Remove Coupler/Splitter module



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

**Note** An equipment missing alarm appears once you remove the coupler/splitter module.

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

#### **Step 6 Replace Coupler/Splitter module**

- a) Align the replacement coupler/splitter module to the slot in which the module is being replaced.
- b) Carefully push the module straight into the slot.

#### **Step 7 Replace Faceplate Screws**

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

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

#### **Step 8 Reconnect Optical Cables**

Clean the optical cables and then connect them to the module.

#### **Step 9 Replace Cables**

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



## 6.0 Provisioning and activating GCC and ODCC on DOL

---

This section describes how to provision and activate GCC and ODCC on DOL services.

- [6.1, “Provisioning GCC”](#)
- [6.2, “Provisioning ODCC on DOL”](#)
- [6.3, “Configuring OSPF”](#)
- [6.4, “Managing GCC and ODCC on DOL services”](#)
- [6.5, “Configuring GCC to Management VLAN Routing”](#)
- [6.6, “Related TL1 provisioning commands”](#)
- [6.7, “Related CLI provisioning commands”](#)
- [6.8, “Related SNMP tables”](#)

## 6.1 Provisioning GCC

---

You can use the proNX 900 Node Controller, the TL1 command interface, the CLI command interface, or SNMP to provision GCC. This section provides GCC provisioning instructions using the proNX 900 Node Controller:

- For a list of the TL1 commands used to provision GCC refer to [6.6.1, “TL1 commands for provisioning GCC”](#).
- For a list of the CLI commands used to provision GCC refer to [6.7.1, “CLI commands for provisioning GCC”](#)
- For a list of the MIB tables used to provision GCC refer to [6.8.1, “Provisioning GCC, ODCC and OSPF using SNMP”](#)

### 6.1.1 GCC provisioning task list

To provision and activate GCC, perform the following tasks in the order presented:

- [6.1.3, “Enabling GCC on an interface”](#)
- [6.3.1, “Enabling OSPF on a shelf”](#)
- [6.3.2, “Enabling OSPF on an interface”](#)

Use the following tasks to manage GCC:

- [6.4.1, “Removing GCC and ODCC services from an interface”](#)
- [6.4.2, “Restoring the GCC or ODCC to service”](#)
- [6.4.3, “Deleting a GCC or ODCC service from an interface”](#)

### 6.1.2 GCC provisioning restrictions

The following rules apply to GCC:

- GCC is only available on the modules identified in [1.1.1, “GCC”](#).
- The line protocol of the module must be set to OTU2 provisioned with FEC/EFEC before you can provision GCC.
- The line protocol can not be changed if GCC is provisioned. You must delete GCC from the port before you can modify the line protocol.
- The module and port must be provisioned before GCC is provisioned.
- The module's administrative state cannot be changed to Out-Of-Service if GCC is provisioned on a port and the administrative state is In-Service. You must remove GCC from service before you can remove the module from service.
- A port cannot be deleted if GCC is provisioned on it. GCC must be deleted first.
- You cannot add static IP routes over GCC interfaces.

- You must provision GCC for both line side ports on a protection pair.
- Do not provision GCC on more than one client port when provisioning a line-side protection pair.

### 6.1.3 Enabling GCC on an interface

Use this procedure to enable GCC on a supported module.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

The supported module must be provisioned to use an OTN protocol. See [1.1.1, “GCC”](#).

**Note** There are no IP addresses associated with GCC.

Follow these steps to enable GCC on a supported module:

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

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

**Step 3** On the **GCC0** tab, enable GCC0

- a) In the GCC0 Mode: drop- down menu, select Full Rate (1.3 Mbps) or Low Rate (192 kbps - ).

**Note** Performing a software upgrade is not possible over a Low Rate connection. A Low Rate connection is only useful for supervisory or monitoring functions.

- b) Click **Apply**.

- c) Click **Close**.

You have successfully completed this procedure. The next step is to configure OSPF. Refer to [6.3, “Configuring OSPF”](#).

**For TL1 Users:** Use the command ENT-GCC0 to enable the GCC0 on a port of a module. See the *TL1 Reference Guide* for information.

**For GCC on packetVX users:** Use the INTERFACE GCC command to enter the GCC Configuration Mode. See the *BTI 7000 Series (including packetVX ) Command Line Interface Reference Guide*. Also see the *packetVX Solutions Guide*.

## 6.2 Provisioning ODCC on DOL

---

You can use the proNX 900 Node Controller, the TL1 command interface, or SNMP to provision ODCC on DOL. This section provides ODCC on DOL provisioning instructions using the proNX 900 Node Controller:

- For a list of the TL1 commands used to provision ODCC on DOL refer to [6.6.2, “TL1 commands for provisioning ODCC on DOL”](#).
- For a list of the MIB tables used to provision ODCC on DOL refer to [6.8.1, “Provisioning GCC, ODCC and OSPF using SNMP”](#)

### 6.2.1 ODCC on DOL provisioning task list

To provision and activate ODCC, perform the following tasks in the order presented:

- [6.2.3, “Enabling ODCC on an interface”](#)
- [6.3.1, “Enabling OSPF on a shelf”](#)
- [6.3.2, “Enabling OSPF on an interface”](#)

Use the following tasks to manage ODCC:

- [6.4.1, “Removing GCC and ODCC services from an interface”](#)
- [6.4.2, “Restoring the GCC or ODCC to service”](#)
- [6.4.3, “Deleting a GCC or ODCC service from an interface”](#)

### 6.2.2 ODCC on DOL provisioning restrictions

The following rules apply to ODCC:

- ODCC on DOL is supported on only DOL modules. [1.1.2.1, “ODCC on DOL support on BTI 7000 Series modules”](#).
- The line port of the module must be set to DOL.
- Only one ODCC can be provisioned per DOL module.
- At the time of provisioning the ODCC, if the administrative status of the supporting OSC object is Out-of-service, the default administrative status of the ODCC is set to Out-of-service.
- If OSPF is provisioned on the network element, the ODCC can be added as an OSPF interface, and the administrative status can be set to In- or Out-of-service.
- The ODCC object cannot be de-provisioned if the ODCC is still provisioned as an OSPF interface.
- The ODCC does not support auto- or de-provisioning.

### 6.2.3 Enabling ODCC on an interface

Use this procedure to enable ODCC on a supported module.



- A module provisioned to use the DOL protocol must exist.
- Only one ODCC can be provisioned per OSC object .

**Note** There are no IP addresses associated with ODCC.

Follow these steps to enable ODCC on a supported module:

- Step 1** In the toolbar, select the System Configuration icon.  
The list of shelves appears in the Navigation pane.
- Step 2** From the Navigation pane, right-click a DOL module type.  
The main view of the shelf displays in the right pane.
- Step 3** From the Navigation pane, right-click a DOL module type and click **View OSC Info**.  
The **Provision OSC:<module shelf-slot-port>** dialogue appears.
- Step 4** Click **ODCC**, and select **Enable ODCC**.
- Step 5** Click **OK**.

You have successfully completed this procedure. The next step is to configure OSPF. Refer to [6.3, “Configuring OSPF”](#)


**For TL1 Users:** Use the command ENT-ODCC to enable the ODCC on a port of a module. See the *TL1 Reference Guide* for information.

## 6.3 Configuring OSPF

---

This section describes how to enable OSPF on a GCC and ODCC shelf and interface. The steps for configuring OSPF for GCC and ODCC are the same.

### 6.3.1 Enabling OSPF on a shelf

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

#### Prerequisites

- **GCC:** The supported module must have OTU2 protocol provisioned with FEC/EFEC.
- **ODCC:** The supported DOL module must be provisioned.

#### Enabling OSPFv2 on a shelf

Follow these steps to enable OSPF on a shelf:

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

**Step 2** From the Navigation panel, right-click the system identifier and click **Provision OSPF**.  
The **Provision System** dialog appears.

**Step 3** In the **Provision System** dialog, click the **IP Networking** tab.  
The following tabs appear: **OSPF**, **OSPF Interfaces**, **LSDB**, **OSPF Neighbors**, and **STP**.

**Step 4** Click the **OSPF** tab.

- a) In the **General** area, click **Router ID** or **Default router ID**. If you select **Router ID**, enter the router ID. The **Default Router ID** is the address of the management LAN port.
- b) In the **Route Redistribution** box, select one of the following options:
  - **None** — disable redistribution
  - **Static** — redistribute static routes
  - **Connected** — redistribute connected networks
  - **Default Originate** — redistribute default routes
  - **Default Originate and Static** — redistribute static and default routes
  - **Default Originate and Connected** — redistribute connected and default routes
  - **Static and Connected** — redistribute static and connected routes
  - **All** — redistribute connected, static and default routes



**Step 5** Type an **Area ID**. If no value is entered, the system uses the default area ID of 0.0.20.208.

- a) Click **Apply**.
- b) Click **Close**.

**Note** If you enter an incorrect value, an error warning indicating the problem appears.

You have successfully completed this procedure.

**For TL1 Users:** Use the command ENT-OSPF to enable the OSPF on a shelf. See the *TL1 Reference Guide* for information.

**For GCC on packetVX users:** Use the INTERFACE GCC command to enter the GCC Configuration Mode. See the *BTI 7000 Series and packetVX Command Line Interface Reference Guide*. Also see the *packetVX Solutions Guide*.

## 6.3.2 Enabling OSPF on an interface

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

### Prerequisites

- **GCC:** The supported module must have OTU2 protocol provisioned with FEC/EFEC.
- **ODCC:** The supported DOL module must be provisioned.

### Enabling OSPFv2 on an interface

Follow these steps to enable OSPF on an interface:

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

**Step 2** From the Navigation panel, right-click the system identifier and click **Provision OSPF**. The **Provision System** dialog appears.

**Step 3** In the **Provision System** dialog, click the **IP Networking** tab. The following tabs appear: **OSPF**, **OSPF Interfaces**, **LSDB**, **OSPF Neighbors**, and **STP**.

**Step 4** Click the **OSPF Interfaces** tab.

- a) Click **Add**. The **Add OSPF Interface** dialog appears.
- b) In the **Source** list, select a GCC- or ODCC- interface. Only enabled GCC or ODCC interfaces appear in this list.

**Step 5** Save the changes.

- a) Click **Apply**.
- b) Click **Close**.

You have successfully completed this procedure.

**For TL1 Users:** Use the command ENT-OSPF-IF to enable the OSPF on an interface. See the *TL1 Reference Guide* for information.

**For GCC on packetVX users:** Use the INTERFACE GCC command to enter the GCC Configuration Mode. See the *BTI 7000 Series (including packetVX ) Command Line Interface Reference Guide*. Also see the *packetVX Solutions Guide*.

## 6.4 Managing GCC and ODCC on DOL services

This section describes how to manage provisioned GCC and ODCC on DOL services on a port. The steps for managing these services are the same.

To manage GCC and ODCC services, perform the following tasks:

- 6.4.1, “Removing GCC and ODCC services from an interface”
- 6.4.2, “Restoring the GCC or ODCC to service”
- 6.4.3, “Deleting a GCC or ODCC service from an interface”

### 6.4.1 Removing GCC and ODCC services from an interface

Use this procedure to disable a GCC or ODCC service from a port. This procedure stops the service, but does not delete the provisioning.



#### Removing GCC service from a port

- Step 1** In the Navigation pane, right-click a GCC- or ODCC- capable port, and then click **Provision Port**.
- Step 2** In the **Provision Port** dialog, click the tab for the GCC or ODCC service.
- Step 3** Click the **Remove** button.
- a) Click **Apply**.
  - b) Click **Close**.

You have successfully completed this procedure.

**For TL1 Users:** Use the command RMV-GCC0 or RMV-ODCC to disable the particular service on a port. See the *TL1 Reference Guide* for information.

**For GCC on packetVX users:** Use the INTERFACE GCC command to enter the GCC Configuration Mode. See the *BTI 7000 Series (including packetVX ) Command Line Interface Reference Guide*. Also see the *packetVX Solutions Guide*.

### 6.4.2 Restoring the GCC or ODCC to service

Use this procedure to restore a GCC or ODCC service on a port.



#### Restoring GCC service on a port

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

**Step 2** In the **Provision port** dialog, click the tab for the GCC or ODCC service.

**Step 3** Click the **Restore** button.

a) Click **Apply**.

b) Click **Close**.

You have successfully completed this procedure.

**For TL1 Users:** Use the command RST-GCC0 or RST-ODCC to restore service to the on a port. See the *TL1 Reference Guide* for information.

**For GCC on packetVX users:** Use the INTERFACE GCC command to enter the GCC Configuration Mode. See the *BTI 7000 Series (including packetVX ) Command Line Interface Reference Guide*. Also see the *packetVX Solutions Guide*.

### 6.4.3 Deleting a GCC or ODCC service from an interface

Use this procedure to delete GCC or ODCC from service on a port.



#### Deleting GCC on a port

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

**Step 2** In the **Provision Port** dialog, click the tab for the particular service.

**Step 3** From the **GCC0 Mode** or **ODCC Modedrop**-down menu, select **Disabled**.

a) Click **Apply**.

b) Click **Close**.

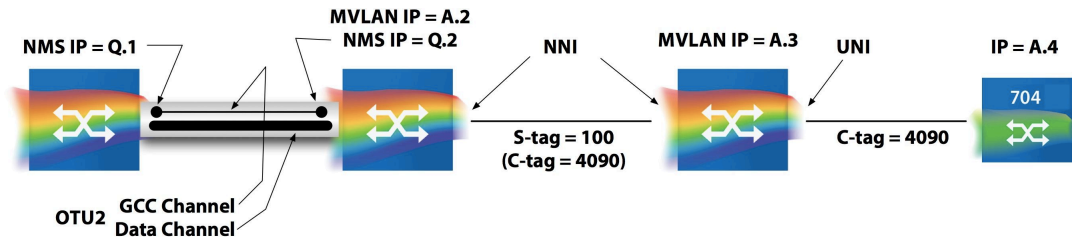
You have successfully completed this procedure.

**For TL1 Users:** Use the command DLT-GCC0 or DLT-ODCC to remove the service from a port. See the *TL1 Reference Guide* for information.

**For GCC on packetVX users:** Use the INTERFACE GCC command to enter the GCC Configuration Mode. See the *BTI 7000 Series (including packetVX ) Command Line Interface Reference Guide*. Also see the *packetVX Solutions Guide*.

## 6.5 Configuring GCC to Management VLAN Routing

This procedure describes how to configure GCC to Management VLAN routing, as shown in the following figure.



In this scenario, traffic from a GCC link is routed across the Management VLAN with an ultimate destination of a node on a customer VLAN on node A.2. The GCC link is provisioned on interface tenGig 1/1/1 and routed over an NNI on port tenGig 1/1/2 which is part of the Management VLAN service.

### Step 1 Create interface GCC TenGigE 1/1/1

To create the interface, enter the following command:

```
BTI7000:sw1(config)# interface ten 1/1/1
BTI7000:sw1(config-if TenGigE 1/1/1)# shut
BTI7000:sw1(config-if TenGigE 1/1/1)# line-mapping otu2-gfp1
BTI7000:sw1(config-if TenGigE 1/1/1)# no shut
BTI7000:sw1(config-if TenGigE 1/1/1)# exit
BTI7000:sw1(config)# int gcc ten 1/1/1
```

### Step 2 Exit configuration mode

To exit, enter the following command:

```
BTI7000:sw1(config-gcc TenGigE 1/1/1)# exit
```

### Step 3 Create NNI TenGigE 1/1/2

To create the NNI Ten GigE 1/1/2, enter the following command:

```
BTI7000:sw1(config)# nni ten 1/1/2
```

### Step 4 Exit configuration mode

To exit, enter the following command:

```
BTI7000:sw1(config-nni ten 1/1~)# exit
```

### Step 5 Create the management VLAN Eservice

To create the management VLAN, enter the following command:

```
BTI7000:sw1(config)# eservice mgmtvlan type MGMTVLAN
```

**Step 6 Assign the VLAN ID and IP address to the management VLAN service and associate an NNI with it**

To create the NNI TenGigE 1/1/2, enter the following command:

```
BTI7000:sw1(config-eservice)# s-vlan 100
BTI7000:sw1(config-eservice)# ip 192.168.1.9/24
BTI7000:sw1(config-eservice)# nni ten 1/1/2
```

You have successfully completed this procedure.

## 6.6 Related TL1 provisioning commands

This section lists the TL1 commands used to provisioning GCC, ODCC and OSPF. For more information on BTI TL1 commands, refer to the *BTI 7000 Series TL1 Reference Guide*.

### 6.6.1 TL1 commands for provisioning GCC

The following table lists the TL1 commands used to provision and activate GCC.

**Table 6-1 GCC provisioning commands**

Action	TL1 command
Entering new equipment	ENT-GCC0:[TID]:<aid>:CTAG:::[<mode>]: [<pst>],[<sst>];
Editing GCC configuration	ED-GCC0:[TID]:<aid>:CTAG:::[<mode>]: [<pst>],[<sst>];
Removing GCC from service	RMV-GCC0:[TID]:<aid>:[CTAG];
Restoring GCC	RST-GCC0:[TID]:<aid>:[CTAG];
Retrieving GCC	RTRV-GCC0:[TID]:[<aid>]:[CTAG];
Retrieving GCC PMs	RTRV-PM-GCC0:[TID]:<aid>:[CTAG];
Deleting equipment	DLT-EQPT:[TID]:<aid>:[CTAG][:::[ [CMDMDE=<cmdmde>]]];

### 6.6.2 TL1 commands for provisioning ODCC on DOL

The following table lists the TL1 commands used to provision and activate ODCC. For detailed information about these commands, refer to the *BTI 7000 Series TL1 Reference Guide*.

**Table 6-2 ODCC provisioning commands**

Action	TL1 command
Entering new equipment	ENT-ODCC:[TID]:[<aid>]:[CTAG]::::[<pst>;
Editing ODCC configuration	ED-ODCC: [TID]:[<aid>]:[CTAG]::::[<pst>;
Removing ODCC from service	RMV-ODCC:[TID]:<aid>:[CTAG];
Restoring ODCC	RST-ODCC:[TID]:<aid>:[CTAG];
Deleting equipment	DLT-ODCC:[TID]:[<aid>]:[CTAG];

### 6.6.3 TL1 commands for provisioning OSPF

The following table lists the TL1 commands used to provision OSPF:

**Table 6-3 OSPF provisioning commands**

Action	TL1 command
Provisioning OSPF	ENT-OSPF:[TID]:<aid>:[CTAG]:: [RTRID=<rtrid>][,REDIST=<redist>] [,AREAID=<areaid>][,STUB=<stub>][:[<pst>] [,<sst>]];
Modify OSPF settings	ED-OSPF:[TID]:<aid>:[CTAG]:: [RTRID=<rtrid>][,REDIST=<redist>] [,AREAID=<areaid>][,STUB=<stub>][:[<pst>] [,<sst>]];
Retrieving OSPF parameters	RTRV-OSPF:[TID]:[<aid>]:CTAG;
Retrieving OSPF information	RTRV-OSPF-IF:[TID]:[<aid>]:[CTAG]:;
Retrieving OSPF Link State Database	RTRV-OSPF-LSDB:[TID]:[<aid>]:[CTAG]:;
Retrieving OSPF service neighbor database	RTRV-OSPF-NGHBR:[TID]:[<aid>]:[CTAG]:;
Restoring OSPF	RST-OSPF:[TID]:<aid>:[CTAG]:;
Restore an interface to service	RST-OSPF-IF:[TID]:[<aid>]:[CTAG]:;
Remove OSPF	RMV-OSPF:[TID]:<aid>:[CTAG]:;
Remove OSPF interface	RMV-OSPF-IF:[TID]:[<aid>]:[CTAG]:;
Deleting OSPF	DLT-OSPF:[TID]:<aid>:CTAG:: [CMDMDE=<cmdmde>];
Adding OSPF IP interfaces	ENT-OSPF-IF:[TID]:<aid>:CTAG::<areaid>;
Deleting OSPF IP interfaces	DLT-OSPF-IF:[TID]:<aid>:CTAG:: [CMDMDE=<cmdmde>];
Change OSPF interface	ED-OSPF-IF:[TID]:<aid>:[CTAG]:: [PRIORITY=<priority>][,HELLOINT=<helloint>] [,DEADINT=<deadint>][,RETRINT=<retrint>] [,TRSTDEL=<trstdel>][,COST=<cost>] [:[<pst>][,<sst>]];



## 6.7 Related CLI provisioning commands

This section lists the CLI commands used to provision GCC and OSPF. For more information on provisioning GCC and OSPF using the CLI refer to the *BTI 7000 Series packetVX Solutions Guide*.

### 6.7.1 CLI commands for provisioning GCC

The following table lists the CLI commands used to provision and activate GCC.

**Table 6-4 GCC global configuration mode commands**

Action	CLI command
Displaying information for all interfaces, all GCC interfaces, or a specific GCC interface	<code>show interfaces [gcc [&lt;interface-type&gt; &lt;interface-id&gt;]]</code>
Adding or deleting a GCC interface	<code>[no] interface gcc &lt;interface-type&gt; &lt;interface-id&gt;</code>

**Table 6-5 GCC configuration mode commands**

Action	CLI command
Enabling or disabling GCC	<code>admin-state enable disable or [no] shutdown</code>
Setting the GCC line rate	<code>rate low full</code>
Adding OSPF to the GCC interface, or entering OSPF interface configuration mode	<code>ospf</code>
Displaying information for the GCC interface	<code>show</code>

### 6.7.2 CLI commands for provisioning OSPF

The following table lists the CLI commands used to provision OSPF for a GCC interface:

**Table 6-6 OSPF global configuration mode commands**

Action	CLI command
Creating OSPF and setting the area-id, or entering OSPF configuration mode	<code>ospf [area-id &lt;area-id&gt; default]</code>
Deleting OSPF	<code>no ospf</code>
Displaying OSPF information	<code>show ospf</code>
Displaying the OSPF link state database	<code>show ospf database [detail]</code>
Displaying OSPF information for all interfaces or for a specific GCC interface	<code>show ospf interface [gcc &lt;interface-type&gt; &lt;interface-id&gt;]</code>
Displaying OSPF neighbor information	<code>show ospf neighbor [detail]</code>

**Table 6-7 OSPF configuration mode commands**

Action	CLI command
Enabling or disabling OSPF	admin-state enable disable or [no] shutdown
Setting the area type	area-type default stub
Setting route redistribution	redistribution none all conn orig  orig_conn orig_stat stat stat_conn no redistribution
Setting the router ID	router-id <ip-addr>
Displaying OSPF information	show

**Table 6-8 OSPF interface configuration mode commands**

Action	CLI command
Enabling and disabling the OSPF interface	admin-state enable disable or [no] shutdown
Setting the interface cost	cost {1..65535} no cost sets the cost to the default value of 10
Setting the dead-interval	dead-interval {1..65535} in seconds no dead-interval sets the dead-interval to the default value of 40
Setting the hello-interval	hello-interval {1..65535} in seconds no hello-interval sets the hello-interval to the default value of 10
Setting the retransmit-interval	retransmit-interval {1..3600} in seconds no retransmit-interval sets the retransmit- interval to the default value of 5
Setting the priority of the interface	priority {1..255} no priority sets the priority to the default value of 1
Setting the transmit-delay	transmit-delay {0..3600} in seconds no transmit-delay sets the transmit-delay to the default value of 1
Displaying OSPF interface information	show

## 6.8 Related SNMP tables

This section lists the SNMP tables used to provision GCC, ODCC, and OSPF.

### 6.8.1 Provisioning GCC, ODCC and OSPF using SNMP

The following SNMP tables are used to provision GCC, ODCC and OSPF:

**Table 6-9 GCC, ODCC and OSPF SNMP provisioning tables**

Tables	Description
<b>GCC tables</b>	
gcc0ConfigTable	SNMP for GCC is implemented as a single SNMP table with a single GCC entry that contains the GCC0 configuration information of an interface. This entry must correspond to an OTN port capable of supporting GCC.
<b>ODCC tables</b>	
odccTable	Used to provision and administer the OSC data communications channel on an optical layer OSC object which is used for management communications.
<b>OSPF tables</b>	
ospfGeneralTable	Contains general OSPF parameters for the network element. Only one entry can exist in the table at a time.
ospfIfTable	Describes the interfaces from the viewpoint of OSPF.
ospfLsdbTable	Contains the link state advertisements from all of the areas to which the device is attached.
ospfNbrTable	Describes all non-virtual neighbors of the OSPF router.



## 7.0 Provisioning the OSC

---

This section describes how to provision the Optical Supervisory Channel (OSC).

- [7.1, “Overview”](#)
- [7.2, “Provisioning tasks”](#)

## 7.1 Overview

---

The OSC is integrated on the System Control Processor (SCP) and uses SFPs to provide OSC functionality for remote shelf management.

When OSC is provisioned, the BTI 7000 Series auto-creates two IP interfaces. The two OSC ports share the IP address of the BTI 7000 Series management LAN port.

You can modify the IP address, Subnet Mask and Gateway address of the Management Ethernet port on the Main Shelf Interface (MSI). The Management Ethernet port allows you to connect the system to an Ethernet hub or switch.

## 7.2 Provisioning tasks

To provision the OSC, perform the following tasks, enable OSC ports in the Management Ethernet tab of the Provision System dialog box.

STP is enabled or disabled globally on the whole system. STP is enabled by default and applies to the OSC ports and the MSI port.

The Management Ethernet dialog consists of two tabs:

- **Basic** — for enabling OSC
- **Advanced** — for configuring the IP address of an OSC port and for configuring and viewing advanced IP interface parameters for an OSC ports

### 7.2.1 Enabling OSC ports

Use this procedure to enable OSC ports.



**Step 1** In the Navigation pane, right-click on BTI 7000 Series, and click **Provision System**.

**Step 2** Click the **Management Ethernet** tab.

**Step 3** In the **Provision System** dialog, click the **Basic** tab.

**Step 4** On the **Basic** tab, in **OSC Settings**, enable the OSC port(s).

- **Enable OSC 1 Port** — enables OSC functionality on the SCP. The OSC port is IS when it is enabled.
- **Enable OSC 2 Port** — enables OSC functionality on the SCP. The OSC port is IS when it is enabled.

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

You have successfully completed this procedure.

### 7.2.2 Provision management Ethernet settings

The SCP provides OSC functionality for remote shelf management. The SCP has two SFP-based OSC ports supporting 1310, 1511, and 1611 nm channels for DWDM applications and 1451 nm channels for CWDM applications. The OSC integrated on the SCP must be combined with a separate Coupler/Splitter module for full functionality.

**Caution** Changing the craft Ethernet port settings may result in temporary loss of connection to the BTI 7000 Series network element.

#### 7.2.2.1 Provision Ethernet settings

Use this procedure to provision the Ethernet settings on the management LAN port.

**Step 1** In the Navigation pane, right-click on BTI 7000 Series, and click **Provision System**.

**Step 2** In the **Provision System** dialog, click the **Management Ethernet** tab.

**Step 3** On the **Advanced** tab, enter a valid IP address, mask, and default gateway.

**Step 4** Click **Apply** and **Close**.

You have successfully completed this procedure.

### 7.2.2.2 Viewing Ethernet Info

Use this procedure to view the Ethernet Info and OSC Settings on the Management Ethernet Port.

**Step 1** In the Navigation pane, right-click on BTI 7000 Series, and click **Provision System**.

**Step 2** In the **Provision System** dialog, click the **Management Ethernet** tab.

**Step 3** Click the **Advanced** tab.

The table below lists the information that is displayed.

**Step 4** Click **Close**.

You have successfully completed this procedure.

Parameter	Description
MAC Address	Standardized data link layer address that is required for every port or device that connects to a LAN. Other devices in the network use these addresses to locate specific ports in the network.
Broadcast Address	A special address reserved for sending a message to all stations.
Interface Speed	Displays the media rate at which the BTI 7000 Series is connecting to a NE via the Management Ethernet port.
MTU size	Maximum packet size, in bytes, that the Craft Ethernet interface can handle.

### 7.2.3 Add static routes

A static route is a predefined route to a specific network and/or a device such as a host. Use this procedure to provision a static route.

**Step 1** In the physical view window of the proNX 900, right-click on the SCP, and select **Provision Static Routes**.

**Step 2** In the **Static Routes** tab, click **Add**.

**Step 3** In the **Add Static Route** dialog box, enter:

- the IP address of the destination network in the **Network** field. This address must be a valid network address. An example of a network IP address is 10.1.1.0.



- the subnet mask of the destination network in the **Mask** field. An example of a Mask is 255.255.255.0.
- the IP address of the next hop router in the **Next Hop** field.
- a weight for the route in the **Admin Distance** field (optional). Based on this weight (a number) the route may or may not be preferred. The admin Distance range is 1 to 254. If you do not specify a number, the administrative distance is set to 1 by default.

**Step 4** Click **Apply** and **Close**.

## 7.2.4 Delete static routes

Use this procedure to delete a static route.

**Step 1** In the physical view window of the proNX 900, right-click on the SCP, and select **Provision Static Routes**.

**Step 2** In the **Static Routes** tab, select the static route to be deleted and click the **Delete** button.



## 8.0 Managing communication channel solutions

---

This section contains:

- [8.1, “Monitoring OSPF”](#)
- [8.2, “Related TL1 commands”](#)

## 8.1 Monitoring OSPF

---

### 8.1.1 Viewing the routing table

The routing table list indicates the best route to all destinations. The entries represent each destination network known to the system.

The routing table can be viewed from the proNX 900 Node Controller or by using the TL1 command RTVR-ROUTE-ALL.

The routing table provides the following data on both static and learned routes:

Parameter	Description
IP address	The destination network address.
Mask	The Net Mask of the destination network.
Next Hop	The IP address of the next hop router or the AID of the exiting interface.
Protocol	OSPF, Static or Connected
Type	<b>Direct</b> — Route to a directly connected (sub-)network <b>Indirect</b> — Route to a non-local host, network or sub-network <b>Invalid</b> — Route that is not valid
Preferred	Yes or No
Cost	The value, based on hop count, assigned to a path or link.
Admin Distance	The administrative distance parameter selects the best path to a destination network. Lower values are preferred over higher values.

### 8.1.2 Viewing static routes

A static route is a predefined route to a specific network and/or a device such as a host. Use this procedure to view the static routes that have been provisioned on the system.

**Step 1** In the physical view window of the proNX 900, right-click on the SCP, and select **Provision Static Routes**.

The Static Routes table is displayed.

Parameter	TL1 command
IP address	The destination network address.
Mask	The Net Mask of the destination network.
Next Hop	The IP address of the next hop router or the AID of the exiting interface.

Parameter	TL1 command
Protocol	Static
Type	<b>Direct</b> — Route to a directly connected (sub-)network <b>Indirect</b> — Route to a non-local host, network or sub-network <b>Invalid</b> — Route that is not valid
Preferred	Yes or No
Cost	The value, based on hop count, assigned to a path or link.
Admin Distance	The administrative distance parameter selects the best path to a destination network. Lower values are preferred over higher values.

### 8.1.3 Filtering static routes

You may need to filter the data in the static routes table if it contains many routes. The entries in the static route table correspond to each destination known to the system. You can filter the static routes table entries using the following criteria:

- IP Address
- Mask
- Type
- Next Hop
- Preferred
- Protocol

See [8.1.2, “Viewing static routes”](#) for descriptions of each of these parameters.

### 8.1.4 Viewing the OSPF Link State Database

The OSPF LSDB is a list of link-state entries of all other routers in the network. It shows the network topology.

For details on using the TL1 command line, see [8.1.7, “Viewing the OSPF Neighbors database”](#).

Follow these steps to view the routing table:

**Step 1** In the Navigation pane, right-click on the NE identifier, and click **Provision System**.

**Step 2** In the **Provision System** dialog, click the **IP Networking** tab.

**Step 3** On the **IP Networking** tab, click the **Advanced** tab, and then click the **LSDB** tab.

**Step 4** On the **LSDB** tab, click the **Refresh** button.

The LSDB list is refreshed and displays the LSDB entries.

**Step 5** Use the **Filter** button to refine the list of entries.

**Step 6** Use the **Columns** button to add or remove columns to the list.

You have successfully completed this procedure.

The LSDB list provides the following network topology information:

Parameter	Description
Area ID	This 32-bit number identifies the Area from which a Link State Advertisement was received.
Type	The type of link state advertisement: ROUTER NETWORK SUMMARY ASSUMMARY ASEXTERNAL
ID	The Link State ID contains either a Router ID or an IP Address.
Router ID	This 32-bit number uniquely identifies the originating router in the Autonomous System.
Seq #	The sequence number. A 32-bit signed integer value that is presented in HEX format. The range is 0x80000000 to 0xFFFFFFFF.
Age	The age in seconds.
Checksum	The checksum parameter.

### 8.1.5 Adding or removing display columns

When viewing the LSDB entries, you may wish to add or remove columns in the display.



**Step 1** To remove a column category, select a category in the **Display Columns** list and click **Remove**. Shift-click to select multiple categories.

**Step 2** To add a column category, select a category in the **Hidden Columns** list and click **Add**. Shift-click to select multiple categories.

**Step 3** Click **OK** to save your changes.

You have successfully completed this procedure.

## 8.1.6 Filtering the Link State Database

You may need to filter the data in the LSDB if it contains many entries. The entries in the LSDB list all other routers in the network. You can filter the LSDB entries using the following criteria:

- Type
- Router ID
- Area ID
- LSA ID

See 8.1.7, “[Viewing the OSPF Neighbors database](#)” for descriptions of each of these parameters.

## 8.1.7 Viewing the OSPF Neighbors database

The OSPF Neighbors database lists discovered neighbors in the network.

Follow these steps to view the OSPF Neighbor database:

**Step 1** In the Navigation pane, right-click on the NE identifier, and click **Provision System**.

**Step 2** In the **Provision System** dialog, click the **IP Networking** tab, and then click the **OSPF Neighbors** tab.

**Step 3** On the **OSPF Neighbors** tab, click the **Refresh** button.

The OSPF Neighbors list is refreshed and displays the entries.

**Step 4** Use the **Filter** button to refine the list of entries.

**Step 5** Use the **Columns** button to add or remove columns to the list.

You have successfully completed this procedure.

The OSPF Neighbors list provides the following data on discovered neighbors:

Parameter	Description
IP address	The IP address this neighbor is using in its IP Source Address.
Router ID	This 32-bit integer (like an IP address) uniquely identifies the neighboring router in the Autonomous System.
State	The state of the Neighbor. Possible states are: DOWN ATTEMPT INIT TWOWAY EXSTART EXCHANGE

Parameter	Description
	LOADING
	FULL
Priority	This is used in the Designated Router Election. A value of 0 signifies that the neighbor is not eligible to become the designated router on this particular network.

### 8.1.8 Adding or removing display columns

When viewing the routing table entries, you may wish to add or remove columns in the display.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

- Step 1** To remove a column category, select a category in the Display Columns list and click **Remove**. Shift-click to select multiple categories.
- Step 2** To add a column category, select a category in the Hidden Columns list and click Add. Shift-click to select multiple categories.
- Step 3** Click **OK** to save your changes.

You have successfully completed this procedure.

### 8.1.9 Filtering OSPF Neighbors

You may need to filter the data in the Neighbors table if it contains many entries. You can filter the Neighbors table entries using the following criteria:

- Type
- Router ID
- Area ID
- LSA ID

See 8.1.7, “[Viewing the OSPF Neighbors database](#)” for descriptions of each of these parameters.

For information on TL1 commands, refer to the *TL1 Reference Guide*.



## 8.2 Related TL1 commands

For information on TL1 commands, refer to the *TL1 Reference Guide*.

### 8.2.1 TL1 commands for viewing the routing table

The following table lists the TL1 commands used to view the routing table:

Action	TL1 command
Retrieving all routes	RTRV-ROUTE-ALL:[TID]:CTAG;
Retrieving connected routes	RTRV-ROUTE-CONN:[TID]:CTAG;
Retrieving OSPF routes	RTRV-ROUTE-OSPF:[TID]:CTAG;
Retrieving static routes	RTRV-ROUTE-STATIC:[TID]:CTAG;

### 8.2.2 TL1 commands for viewing Neighbor entries

The following table lists the TL1 command used to view the Neighbor database entries:

Action	TL1 command
Retrieving OSPF Neighbors	RTRV-OSPF-NGHBR:[TID]:[<aid>]:CTAG;

### 8.2.3 TL1 commands for viewing the Link State Database

The following table lists the TL1 command used to view the Link State Database entries:

Action	TL1 command
Retrieving OSPF LSDB information	RTRV-OSPF-LSDB:[TID]:[<aid>]:CTAG;



## 9.0 Troubleshooting

---

This section describes troubleshooting the Management Communication Channels Solution.

- [9.1, “Troubleshooting GCC communications”](#)
- [9.2, “Troubleshooting OSC communications”](#)
- [9.3, “Using Ping to check connectivity”](#)
- [9.4, “OSCLOS \(OSC Loss of Signal\)”](#)

## 9.1 Troubleshooting GCC communications

---

Perform the following checks.

### 9.1.1 Checking physical connectivity

Check the physical connections. GCC is down if the underlying OTU2 interface is in a failed state. Check the corresponding OTU2 interfaces for LOS or LOF alarms. If you have a LOS or LOF alarm, follow the appropriate alarm clearing procedures in the *Alarm and Troubleshooting Guide*. If you have a OSCLOS alarm, see [9.4, “OSCLOS \(OSC Loss of Signal\)”](#).

If the interfaces are alarm-free, use the 'ping' command to test the connectivity. Ensure that the remote management station can successfully ping every network element in the system. A ping command failure for any network element may indicate where a problem exists.

Use the ping command to test connectivity within the network of BTI 7000 Series network elements, or from a BTI 7000 Series network element back to the remote management station. See [9.3, “Using Ping to check connectivity”](#).

### 9.1.2 Checking OSPF

Check the default gateway setting on the system connected to the management network. Network configurations require a default gateway, unless an OSPF interface has been created for the management LAN port.

Check that the default gateway has been redistributed into OSPF, unless an OSPF interface has been created for the management LAN port. The default gateway is redistributed into OSPF only if redistribute is set for default originate.

Check the OSPF setting to ensure OSPF is enabled, and that OSPF interfaces have been created as required for the ports.

Query the routing table to confirm that routes to each network element exist, and that a default route to the management network exists.

Query the OSPF neighbors to confirm that the adjacent network elements are visible. The OSPF neighbor state should be reported as FULL. See [8.1.7, “Viewing the OSPF Neighbors database”](#).

Query the OSPF link-state database to confirm that each network element has the correct topological view of the network. The database should contain:

- router entries for each network element
- network entries for each link - network LSAs are not listed in LSDB when GCC links are point to point un-numbered
- external entries for each default gateway or static route

See [8.1.4, “Viewing the OSPF Link State Database”](#).

### 9.1.3 Checking Management Network Router

Check to ensure that the management network router is configured correctly. In many of the examples described in [4.1, “Network design examples”](#), the management network router needs several static routes configured. In the dual-homing example, the management network router needs OSPF enabled on the 10/100BT port connected the management LAN port on the BTI 7000 Series network element.

For more information about alarm clearing and troubleshooting, see the *Alarm and Troubleshooting Guide*.

## 9.2 Troubleshooting OSC communications

---

Perform the following checks.

### 9.2.1 Checking physical connectivity

Check the physical connectivity. Check for OSCLOS alarms. If there is an OSCLOS alarm, follow the alarm clearing procedure.

If the OSC interfaces are alarm-free, use the ping command to check connectivity. The remote management station must be able to ping every network element. A ping command failure for any network element may indicate where a problem exists.

Use the ping command to test connectivity within the network of BTI 7000 Series network elements, or from a BTI 7000 Series network element back to the remote management station. See [9.3, “Using Ping to check connectivity”](#).

### 9.2.2 Checking STP

Check the IP and default gateway setting on the BTI 7000 Series network elements. All NEs require a unique IP address residing on the same subnet. All NEs must have the same default gateway. Confirm that the default gateway is the address of the management network router.

Check to see if Spanning Tree Protocol (STP) is still enabled. STP is enabled by default but may have been disabled. STP must be enabled in ring configurations.

Determine if STP has been disabled on the MSI management port. Even if STP is enabled on the OSC channel, it can be disabled on the MSI management port. BTI recommends that STP be enabled on the MSI management port.

<b>Note</b>	Careful network planning is required if STP is disabled on the MSI management port. This setting can cause a network loop if two or more NEs are connected to the network and the same NEs are also connected together via OSC.
-------------	---

Check the OSC port forwarding state through software. An OSC port may be blocking or forwarding. In a point-to-point or linear configuration, all of the OSC ports must be forwarding. In a ring configuration, one of the OSC ports in the ring must be blocking.

## 9.3 Using Ping to check connectivity

Use ping to confirm the live connectivity of the Ethernet interface on the OSC or SCP.



**Step 1** In the Navigation pane, right-click on the module, and click **Ping**.

**Step 2** In the **IP Address** field, enter the IP address of the interface you want to test.

**Step 3** Click **Ping**.

**Step 4** View the results in the **Results** portion of the **Ping** window.

Results for external IP interfaces:

If the ping to an external IP interface is unsuccessful, check:

- physical connectivity of the interface
- provisioning of the interface
- the routing table to see if the interface is listed

You have successfully completed this procedure.

## 9.4 OSCLOS (OSC Loss of Signal)

### Problem Description

There is a loss of signal to one of the optical IP interfaces of the Optical Supervisory Channel (OSC) module, or the optical IP interfaces of the System Control Processor (SCP) module.

#### LED behavior for BTI 7060/BTI 7200

Location	Shelf LEDs		System LEDs		
	Trouble	Power	Critical	Major	Minor
MSI	ON	ON	OFF	ON	OFF

#### LED behavior for BTI 7030

Location	Fail	Active	Fan Fail	Critical	Major	Minor
SCP	OFF	ON	OFF	OFF	ON	OFF

#### LED behavior for OSC on the SCP module

Location	module LEDs		
	Fail	Active	Fault
SCP	OFF	ON	ON

### Impact

Major alarm - service is not affected

### Affected AIDs

IP-1-5-(1,2)



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



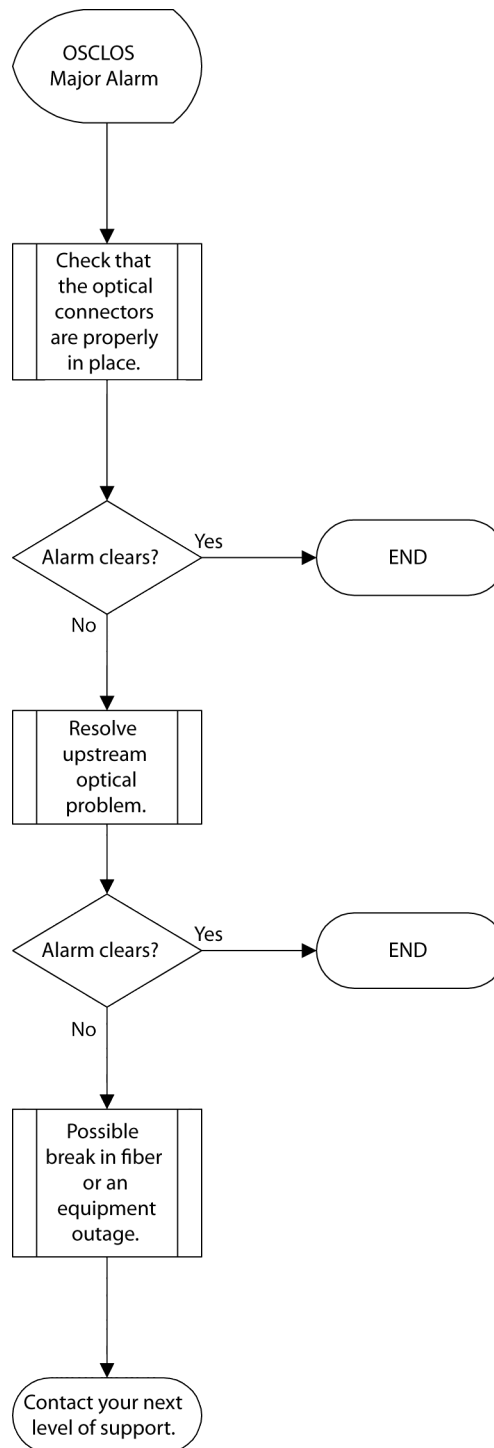
Use an ESD wrist strap whenever you open the equipment, particularly when you are handling modules as well as SFP and XFP transceivers. To work properly, the wrist strap must make good contact at both ends (that is, with your skin at one end and with the chassis at the other).



**Flow chart**

The following figure shows a flow chart of the activities that can be part of this alarm clearing procedure. Use the flow chart to understand the context of the alarm. Use the procedure to clear the alarm.

**Figure 9-1 Clearing an OSCLOS alarm**



### 9.4.1 Clearing an OSCLOS OSC loss of signal alarm

Use this procedure to clear an OSCLOS alarm.

**Step 1** Check optical connectors

There may be a problem with the optical connectors at the OSC module or the SCP module:

- If the alarm clears, you have completed this procedure.
- If the alarm does not clear, go to the next step.

**Step 2** Check upstream equipment

There may be a problem with the upstream equipment. Resolve any upstream problem:

- If the alarm clears, you have completed this procedure.
- If the alarm does not clear, go to the next step.

**Step 3** Possible fiber break in input fiber span

A break in the fiber cable can cause a loss of signal. Contact your next level of support to determine if there is a break in the fiber span.



## Appendix A: Packet flow

---

This appendix presents examples of how packets flow through an Optical Supervisory Channel (OSC) network and a General Communication Channel (GCC). The information is presented in the following sections:

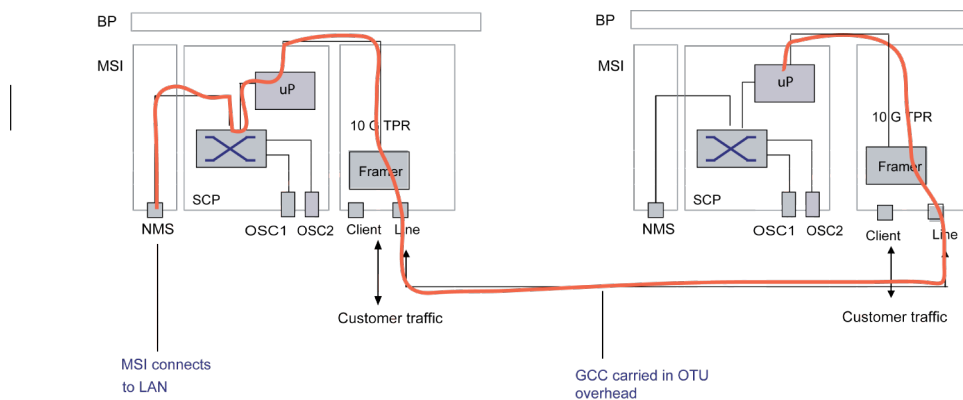
- [A.1, “GCC packet flow example”](#)
- [A.2, “OSC packet flow example”](#)

## A.1 GCC packet flow example

The following discussion illustrates how a packet travels from a management station to a remote network element:

- 1** Packets from a remote management station enter through the management LAN port of the Main Shelf Interface (MSI) module at the near-end BTI 7000 Series site.
- 2** The packet proceeds through a switch and microprocessor on the SCP to a Dual 10G Multiprotocol Transponder line site where the packet is transmitted in OTU2 overhead.
- 3** The packet is then routed through the Dual 10G Multiprotocol Transponder to the next site.
- 4** At the next line site, the signal is separated from the other traffic and routed to the SCP where the packet information is processed.

### Figure A-1 GCC packet flow

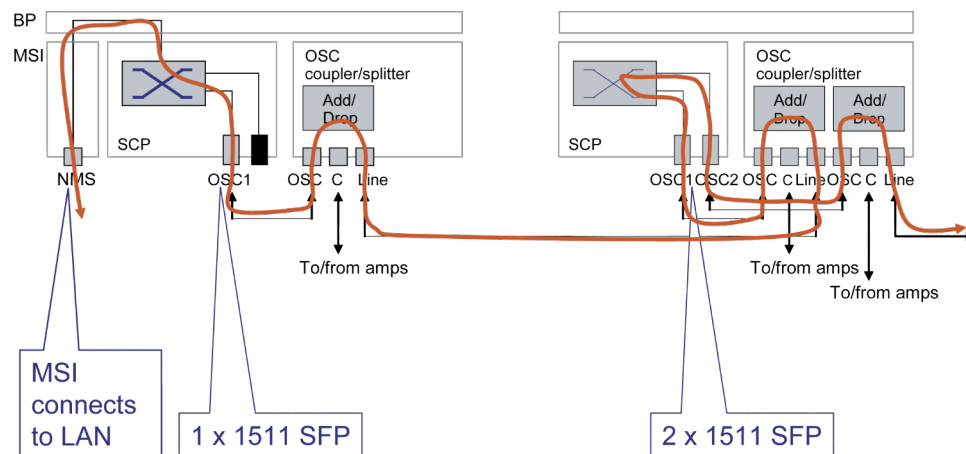


## A.2 OSC packet flow example

The following discussion illustrates how a packet travels from a remote management station to a line site:

- 1 Packets from a remote management station enter through the management LAN port of the Main Shelf Interface (MSI) module at the near-end BTI 7000 Series site.
- 2 The packet proceeds through a switch on the SCP module to both the OSC1 and OSC2 ports on the SCP where the packet is transmitted as a 1511 nm signal.
- 3 The packet is then sent through the standalone single coupler/splitter module to be sent out to the next line site.
- 4 At the next line site, the 1511 nm OSC signal is separated from the other wavelengths and routed to the SCP where the packet information is processed.

**Figure A-2 SCP OSC packet flow**







## Appendix B: Performance engineering

---

This appendix provides an overview of Optical Supervisory Channel (OSC) performance engineering. The information is presented in the following section:

- [B.1, “Throughput and scalability”](#)

## B.1 Throughput and scalability

---

### B.1.1 Engineering limits

The software is designed to accommodate the number of objects that are indicated in the following table.

Object	Limits
OSPF area	1
OSPF object	1
OSPF interfaces	32
LSDB	512
Routes	256
Neighbors	16

### B.1.2 Latency

The OSC has a latency of less than 1.5 ms.





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

*BT7A73EA*  
*01*  
*March 2017*  
*STANDARD*

***product release 13.5***