



BTI7800 Series Software Configuration Guide

Release

4.5



Modified: 2019-02-04

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners.

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.

BT17800 Series Software Configuration Guide

4.5

Copyright © 2019 Juniper Networks, Inc. All rights reserved.

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <https://support.juniper.net/support/eula/>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

	About the Documentation	xiii
	Documentation and Release Notes	xiii
	Documentation Conventions	xiii
	Documentation Feedback	xv
	Requesting Technical Support	xvi
	Self-Help Online Tools and Resources	xvi
	Creating a Service Request with JTAC	xvii
Chapter 1	Getting Started	19
	About the BT17800 Series	19
	Prerequisites	19
	Optical Precautions	20
	Laser Safety	21
	Laser Safety: Automatic Power Shutdown	21
	APSD on the 96-Channel Amplifier	22
	Laser Safety: Automatic Power Reduction	23
	APR on 96-Channel Amplifier Modules	23
	Safety Rating and Label	24
	BT17800 Series Laser Output Ports	24
	Auto-Provisioning of BT17800 Equipment	25
	Pre-Provisioning of BT17800 Components	27
	Turning Up the Software on the BT17800	29
	Commissioning the BT17800 for the First Time	30
Chapter 2	Chassis Management	37
	Management Overview	37
	Constraints	39
	Chassis Management Module (CMM)	39
	CMM Overview	39
	CMM Failure or Removal	41
	CMM Replacement	41
	Dual CMM System	42
	Single CMM System	42
	Logging In to the CLI	44
	Logging In to the CMM Craft Ethernet or Craft Serial Ports	45
Chapter 3	User Accounts and Authentication	49
	Users and Access Privileges	49
	Users	49
	Access Privileges	49
	Adding a User Account	50
	Configuring User Session Parameters	51

	Resetting the Password for the admin User	52
	User Authentication and Authorization	52
	Local Authentication and Authorization	53
	RADIUS/TACACS+ Authentication and Authorization	53
	Authentication and Authorization Sequence	55
	Configuring the RADIUS/TACACS+ Server	56
	Provisioning RADIUS Authentication and Authorization	56
	Provisioning TACACS+ Authentication and Authorization	58
Chapter 4	System Provisioning	61
	Configuring General Administrative Parameters	61
	Configuring the Shared Management IP Address and Subnet	62
	Configuring the Default Gateway	64
	Configuring the Individual Management IP Addresses	65
	Configuring DNS Servers	66
	Configuring NTP Servers and Time Zones	67
	Configuring Management Sources	69
	Configuring Auto-Provisioning	70
	Configuring Auto-Reprovisioning	71
	Configuring Auto-Warm-Boot	72
	Configuring AINS	73
	Configuration Examples	74
	Setting the Autowizard	76
	Setting the Date and Time	77
	Configuring SNMP	78
Chapter 5	Module Provisioning	81
	Overview	81
	Universal Forwarding Modules	81
	UFM Location Identifiers	82
	UFM3 Location Identifiers	83
	UFM4 Location Identifiers	84
	UFM6 Location Identifiers	85
	Provisioning UFM Equipment	87
	Provisioning a UFM	87
	Provisioning a BTI Interface Card (BIC)	88
	Provisioning a Transceiver	89
	Replacing a UFM3 or a UFM4	91
	Qualifying Criteria	92
	Provisioning Changes	93
	Alarm Behavior	95
	Post-Upgrade Verification	95
	Configuring a Loopback on a UFM Interface	95
	Optical Modules	96
	Terminal Amplifier Module	97
	Provisioning a Terminal Amplifier Module	97
	Wavelength Protection Switch Module	97
	Provisioning a WPS Module	98
	Enabling and Disabling Modules	98
	Module Reload Times	99

Chapter 6	Transport Solutions	101
	UFM Interfaces	101
	Overview	101
	UFM6 Interface and Protocol Restrictions	107
	Multiplexed Interfaces	111
	Multiplexed Interfaces on UFM3 and UFM4	114
	Multiplexed Interfaces on UFM6	114
	Forward Error Correction (FEC) Types	115
	Provisioning a Transport Interface	116
	Provisioning an Optical Channel Interface	120
	Provisioning Transponding and Muxponding Cross-Connects	122
	Supported Cross-Connects	122
	Provisioning a Transponding Cross-Connect on a UFM3 or UFM4	136
	Provisioning a Transponding Cross-Connect on a UFM6	138
	Provisioning a Muxponding Cross-Connect on a UFM3 or UFM4	139
	Provisioning a Muxponding Cross-Connect on a UFM6	141
	Link Layer Discovery Protocol (LLDP) Snooping	144
	Configuring LLDP Snooping on an Ethernet Interface	145
	Supported LLDP TLVs	146
	Transport (UFM) Performance Monitoring	148
Chapter 7	Optical Networking Solutions	153
	Terminal Amplifier Solutions	153
	Provisioning a 96-Channel Amplifier Node	153
	Managing Optical Power	155
	Managing Optical Power in a Standard Point-to-Point Deployment	156
	Managing Optical Power in a 100-Gbps Coherent Point-to-Point Deployment	157
	Wavelength Protection Switch Solutions	159
	WPS4 Protection and Rapid Restoration Configurations	160
	Wavelength Protection Switch Unamplified Line Protection	161
	Wavelength Protection Switch Unamplified Channel Protection	162
	Wavelength Protection Switch Amplified Line Protection with an Unamplified Protection Path	162
	Wavelength Protection Switch Amplified Channel Protection with an Amplified Protection Path	163
	Wavelength Protection Switch Amplified Line Restoration with an Unamplified Protection Path	165
	Wavelength Protection Switch Amplified Line Restoration with an Amplified Protection Path	165
	Provisioning Wavelength Protection Groups and Ports	166
	Provisioning Wavelength Protection Groups	167
	Provisioning Wavelength Protection Ports	169
	Provisioning Customized LoLightRx Thresholds	172
	Provisioning Customized LoLightRx Threshold	172
	Performing User-Invoked Switches on the WPS4	174
	Manual Switch	174
	Forced Switch	174
	Lockout Switch	174

	Performing a Manual Wavelength Protection Switch	175
	Performing a Forced Wavelength Protection Switch	175
	Performing a Lockout Wavelength Protection Switch	176
	Wavelength Protection Switch Alarms	177
	Wavelength Protection Switch Performance Monitoring	177
Chapter 8	Multichassis System	179
	Multichassis System Configuration	179
	Setting Up a Multichassis System	180
	Converting a Multichassis System Into Two Single Chassis	184
	Replacing a Single CMM in a Satellite Chassis	186
	Replacing Both CMMs in a Satellite Chassis	187
Chapter 9	SNMP	189
	About SNMP	189
	Supported SNMP Functionality	190
	Specifications	190
	OSS Integration	191
	Supported MIBs	191
	Load Order	195
	Configuring SNMP	196
Chapter 10	NETCONF	199
	About NETCONF	199
	Supported Features	201
	Event Notification Streams	202
	Supported YANG Modules	202
Chapter 11	Performance Monitoring	205
	Statistics Collecting and Archiving	205
	Module and Device Statistics	205
	Optical and Physical Layer Statistics	206
	Protocol Statistics	210
	Effect of a Time Change on PMs	216
Chapter 12	Fault Monitoring and Reporting	217
	Fault Monitoring	217
	Fault Reporting	217
	Fault Hierarchy	218
	Fault Severity	218
	Alarms and Conditions	219
Chapter 13	Software and Firmware Upgrades	229
	Upgrading the Software	229
	Upgrading the CMM Firmware	234
	Upgrading the Re-timer Firmware on a UFM6	238
	Enabling Automatic CMM SHMM Firmware Upgrades	241
	Rolling Back a Software Upgrade	242

Chapter 14	Maintenance and Troubleshooting	245
	Monitoring Environmental Sensors	245
	System Event Logs	247
	Resetting the Database to the Factory-Default Configuration	249
	Backing Up the Configuration Database	249
	Restoring the Database from a Backup Without Affecting Service	251
	Restoring the Database from a Backup from the CLI	257
	Replacing the CMM in a Single CMM System	259
	Installing a Software Load on a CMM Using a System Repair Drive	261
	Uncommissioning a CMM	264
Chapter 15	Appendix	267
	Retrieving a BTI7800 Software Image	267
	Creating a BTI7800 System Repair Drive	269
	Using Linux to Create a BTI7800 System Repair Drive	270
	Using Mac OS X to Create a BTI7800 System Repair Drive	272
	Using Windows to Create a BTI7800 System Repair Drive	275
	BTI7800 Port Usage	277
	DWDM 50-GHz Wavelength Plan	278
	Interoperability with BTI7000 Series Network Elements	283
	Interoperability with BTI7000 Series Transponders	283
	Interoperability with BTI7000 Series Transponders in a Bookended Configuration	284
	Interworking with BTI7000 Series Transponder Clients	286
	Interoperability with BTI7000 Series Muxponders	287
	Interoperability with BTI7000 Series packetVX Modules	289

List of Figures

Chapter 1	Getting Started	19
	Figure 1: Laser Safety Warning Label with Text	24
	Figure 2: Laser Safety Warning Label Without Text	24
Chapter 2	Chassis Management	37
	Figure 3: CMM Module	40
Chapter 6	Transport Solutions	101
	Figure 4: UFM6 Client Ports	107
	Figure 5: LLDP Snooping	145
Chapter 7	Optical Networking Solutions	153
	Figure 6: 96-Channel Amplifier Application	153
Chapter 8	Multichassis System	179
	Figure 7: Multiple Chassis Expansion Port	179
Chapter 10	NETCONF	199
	Figure 8: NETCONF Layers	200
	Figure 9: Management Station to Network Element Communication Using NETCONF	200

List of Tables

	About the Documentation	xiii
	Table 1: Notice Icons	xiv
	Table 2: Text and Syntax Conventions	xiv
Chapter 1	Getting Started	19
	Table 3: Timing of APSD and APR Operations	21
	Table 4: Laser Output Ports	25
Chapter 2	Chassis Management	37
	Table 5: CMM Ports	40
	Table 6: CMM Replacement Scenarios in Single CMM Systems	43
	Table 7: Port Settings	46
Chapter 3	User Accounts and Authentication	49
	Table 8: BT17800 Access Privilege Groups	50
	Table 9: RADIUS Packets	53
	Table 10: TACACS+ Packets	54
Chapter 5	Module Provisioning	81
	Table 11: UFM Types	82
	Table 12: Reprovisioning When Replacing a UFM4 with a UFM3	93
	Table 13: Reprovisioning When Replacing a UFM3 with a UFM4	94
	Table 14: Module Reload Times	99
Chapter 6	Transport Solutions	101
	Table 15: UFM Interfaces	102
	Table 16: UFM6 Client Port Configurations	108
	Table 17: UFM6 Client QSFP+ Dual-Mode Subport Protocol Restrictions	110
	Table 18: UFM Multiplexed Interfaces	112
	Table 19: ODU2 (ODU2e) Subinterface Mapping Into an ODU4	112
	Table 20: ODU3 Subinterface Mapping Into an ODU4	113
	Table 21: FEC Types	115
	Table 22: UFM Cross-Connects	122
	Table 23: UFM6 Fixed Cross-Connect Mappings	125
	Table 24: Mandatory LLDP TLVs	146
	Table 25: UFM Performance Monitoring Counters	148
Chapter 7	Optical Networking Solutions	153
	Table 26: WPS4 Protection Switching Configurations	161
	Table 27: WPS4 Rapid Restoration Configurations	161
Chapter 9	SNMP	189
	Table 28: Standard MIBs	192

	Table 29: BTI7800 MIBs	195
Chapter 11	Performance Monitoring	205
	Table 30: Module and Device Statistics	205
	Table 31: Optical Statistics	206
	Table 32: OTU Protocol Statistics	210
	Table 33: ODU Protocol Statistics	211
	Table 34: SONET Protocol Statistics	211
	Table 35: SDH Protocol Statistics	212
	Table 36: Ethernet Layer 1 Statistics	213
	Table 37: Ethernet Layer 2 Statistics	213
	Table 38: Fibre Channel Statistics	215
Chapter 12	Fault Monitoring and Reporting	217
	Table 39: Fault Severity	218
	Table 40: Alarms and Conditions	219
Chapter 13	Software and Firmware Upgrades	229
	Table 41: UFM6 Re-timer Versions	238
Chapter 14	Maintenance and Troubleshooting	245
	Table 42: System Log Information	247
	Table 43: CLI Logging Commands	248
Chapter 15	Appendix	267
	Table 44: BTI7800 Port Usage	277
	Table 45: DWDM Wavelength Plan (50-GHz Spacing)	278

About the Documentation

- Documentation and Release Notes on page xiii
- Documentation Conventions on page xiii
- Documentation Feedback on page xv
- Requesting Technical Support on page xvi

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at <https://www.juniper.net/documentation/>.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at <https://www.juniper.net/books>.

Documentation Conventions

Table 1 on page xiv defines notice icons used in this guide.

Table 1: Notice Icons







Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Table 2 on page xiv defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the configure command: user@host> configure
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> show chassis alarms No alarms currently active
<i>Italic text like this</i>	<ul style="list-style-type: none"> Introduces or emphasizes important new terms. Identifies guide names. Identifies RFC and Internet draft titles. 	<ul style="list-style-type: none"> A policy <i>term</i> is a named structure that defines match conditions and actions. <i>Junos OS CLI User Guide</i> RFC 1997, <i>BGP Communities Attribute</i>
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# set system domain-name <i>domain-name</i>

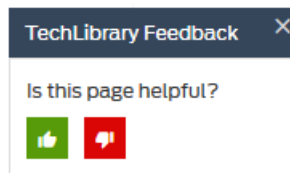
Table 2: Text and Syntax Conventions (continued)

Convention	Description	Examples
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none">To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level.The console port is labeled CONSOLE.
< > (angle brackets)	Encloses optional keywords or variables.	stub <default-metric <i>metric</i>>;
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	broadcast multicast (<i>string1</i> <i>string2</i> <i>string3</i>)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[] (square brackets)	Encloses a variable for which you can substitute one or more values.	community name members [<i>community-ids</i>]
Indentation and braces ({ })	Identifies a level in the configuration hierarchy.	<pre>[edit] routing-options { static { route default { nexthop <i>address</i>; retain; } } }</pre>
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none">In the Logical Interfaces box, select All Interfaces.To cancel the configuration, click Cancel.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select Protocols>Ospf .

Documentation Feedback

We encourage you to provide feedback so that we can improve our documentation. You can use either of the following methods:

- Online feedback system—Click TechLibrary Feedback, on the lower right of any page on the [Juniper Networks TechLibrary](#) site, and do one of the following:



- Click the thumbs-up icon if the information on the page was helpful to you.
- Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide feedback.
- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <https://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <https://www.juniper.net/customers/support/>
- Search for known bugs: <https://prsearch.juniper.net/>
- Find product documentation: <https://www.juniper.net/documentation/>
- Find solutions and answer questions using our Knowledge Base: <https://kb.juniper.net/>
- Download the latest versions of software and review release notes: <https://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://kb.juniper.net/InfoCenter/>

- Join and participate in the Juniper Networks Community Forum:
<https://www.juniper.net/company/communities/>
- Create a service request online: <https://myjuniper.juniper.net>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://entitlementsearch.juniper.net/entitlementsearch/>

Creating a Service Request with JTAC

You can create a service request with JTAC on the Web or by telephone.

- Visit <https://myjuniper.juniper.net>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <https://support.juniper.net/support/requesting-support/>.

CHAPTER 1

Getting Started

- [About the BTI7800 Series on page 19](#)
- [Prerequisites on page 19](#)
- [Optical Precautions on page 20](#)
- [Laser Safety on page 21](#)
- [Auto-Provisioning of BTI7800 Equipment on page 25](#)
- [Pre-Provisioning of BTI7800 Components on page 27](#)
- [Turning Up the Software on the BTI7800 on page 29](#)
- [Commissioning the BTI7800 for the First Time on page 30](#)

About the BTI7800 Series

The BTI7800 Series platform provides high-density optical and transport solutions with industry-leading scale and performance. It comes in different form factors ranging from 1U for smaller remote sites to 14U for larger data centers. All chassis variants support the same universal service modules that transpond and muxpond traffic on 10-Gbps and 100-Gbps interfaces including 100-Gbps coherent DWDM. For higher fan-out, multiple BTI7800s can be connected together in a multichassis configuration.

Together with its ROADM capabilities, the BTI7800 Series provides a complete end-to-end optical transport solution that can scale from 10 Gbps to nx100 Gbps. The flexible hardware and software design allows a service module to be configured for different services on different combinations of 10-Gbps, 100-Gbps, and nx100-Gbps interfaces.

Management of the chassis is performed on the Chassis Management Modules (CMMs), which reside in their own dedicated slots in the chassis. The CMMs can be deployed in pairs for redundancy and perform management and control plane functions for the system, including booting the various service modules with the appropriate software images.

Each BTI7800 chassis is shipped with software pre-installed on the CMMs. The software includes a commissioning utility that allows you to bring the system up quickly.

Prerequisites

The following prerequisites are necessary before you install and configure the BTI7800:

- All chassis and common equipment are installed with terminated and labeled power cables, power plant and fusing is installed, and LAN cables between the chassis and the local switch are labeled.
- Installation team has access to all tools and additional equipment required to perform the procedures in this guide: screw drivers, optical power meter, fiber cleaning kit, label maker, RJ45 cable (or serial cable if preferred), spare attenuation pads (3dB, 5dB, 10dB, 15dB), optical spectrum analyzer (OSA) if required.
- The installation team has a copy of the installation and commissioning report. This report can be obtained from the engineer responsible for the network design.
- The installation team has access to a copy of this guide and reviewed the safety and fiber management sections.

Optical Precautions

- Terminate all laser transceiver outputs properly before connecting laser inputs.
- Disconnect the input end of an optical fiber jumper cable before disconnecting the output end.
- Handle glass fiber with care. Glass fiber can be broken if mishandled.
- Protect skin from exposed glass fiber. It can penetrate the skin.
- The BTI7800 Series equipment should be used in a controlled access area. Limit the number of personnel who have access to the optical transmission systems. Personnel should be properly trained on laser safety and authorized, if access to laser emissions is required.
- Limit the use of laser test equipment to authorized, trained personnel during installation and service. This precaution includes using optical loss test (OLT) set, optical spectrum analyzer (OSA), and optical time domain reflectometer (OTDR) equipment.
- Exclude any unauthorized personnel from the immediate laser radiation area during service and installation when there is a possibility that the system might become energized. Consider the immediate service area to be a temporary laser-controlled area.
- The BTI7800 Series system functions in the 850-nm to 1620-nm wavelength window that is considered invisible radiation. Laser light being emitted by a fiber, a pigtail, or a bulkhead connector cannot be seen by the naked eye. Use appropriate eye protection during fiber-optic system installation or maintenance whenever there is potential for laser radiation exposure, as recommended by the company's health and safety procedures. Observe this precaution whether or not warning labels have been posted.
- During installation or service, a broken optical fiber or non-terminated connector should only be viewed with an indirect image converter or with a filtered optical instrument of optical density sufficient to reduce the exposure levels below the appropriate maximum permissible exposure, unless it has been verified that all optical transmitters are turned off and will remain off during the installation or service operation.
- During all splicing operations that require viewing the end of a fiber of an SG3a, SG3b or SG4 optical-fiber communication systems, the laser source on the fiber involved

shall be de-energized or viewing the systems incorporating personal protection shall be employed. A responsible person(s) shall verify that the system is de-energized before splicing proceeds. Where applicable, ensure compliance with lockout/tagout requirements of OSHA Standard 29 CFR Part 1910.147.

Laser Safety



CAUTION: USE OF CONTROLS OR ADJUSTMENTS OR PERFORMANCE OF PROCEDURES OTHER THAN THOSE SPECIFIED IN THIS GUIDE MIGHT RESULT IN HAZARDOUS RADIATION EXPOSURE.

Due to the potential safety hazard that is posed by high power outputs of optical modules, the BT17800 supports automatic power shutdown (APSD) and automatic power reduction (APR) to shut off or reduce the output powers when a fiber is cut.

Table 3: Timing of APSD and APR Operations

Laser Safety Mechanism	Activation Time	Output Level After Activation
APR	< 2.0 seconds	< 20 dBm
APSD	< 2.0 seconds	< 20 dBm

- [Laser Safety: Automatic Power Shutdown on page 21](#)
- [Laser Safety: Automatic Power Reduction on page 23](#)
- [Safety Rating and Label on page 24](#)

Laser Safety: Automatic Power Shutdown

Automatic power shutdown (APSD) applies to fiber spans between optical equipment. When a fiber is cut, APSD causes both ends to automatically shut down its high power lasers, allowing maintenance personnel to repair or reconnect the fiber safely. Once the span fibers are repaired or reconnected, the lasers are automatically turned back on and traffic is automatically restored.



WARNING: APSD is performed in software on the service module and is disabled whenever the service module undergoes a warm or cold reload. In a cold reload, the lasers are turned off and are in a safe state. In a warm reload, however, the lasers remain on while APSD is disabled.

Without being limited to the foregoing, a service module might undergo a warm reload in the following situations:

- The user issues an operator command that warm reloads the service module.
 - The user issues an operator command that cold or warm reloads the Chassis Management Module (CMM) in a single CMM system.
 - The user performs a software upgrade of the chassis.
 - The user restores a configuration database to the chassis.
 - The user replaces the CMM in the chassis. See [“CMM Replacement” on page 41](#).
 - Any situation where a CMM fails in a single CMM system or where both CMMs fail in a dual CMM system. See [“CMM Failure or Removal” on page 41](#).
-

- [APSD on the 96-Channel Amplifier on page 22](#)

APSD on the 96-Channel Amplifier

The 96-Channel Amplifier is capable of emitting high output powers. To guard against accidental exposure to high-powered lasers, the 96-Channel Amplifier supports automatic power shutdown (APSD). APSD shuts down the high output lasers in both directions when a fiber cut is detected.

The output WDM signal on the line port is automatically shut down, or disabled from turn-up, if either of the following conditions occurs:

- (*Cond. 1*) A Loss of Light fault is active against the input WDM and input OSC on the same line port. This triggers the port to undertake APSD measures. The line port turns off its output WDM signal and simultaneously sends a shutdown signal on the OSC to the far end.
- (*Cond. 2*) A shutdown signal is received from the far end OSC. The far end OSC sends a shutdown signal when APSD is triggered at the far end. In response to the shutdown signal, the near end line port turns off its output WDM signal, and keeps it turned off for as long as the shutdown signal persists.

Single Fiber-Cut Example

Starting with span fibers connected, and with the WDM and OSC operationally in-service, the following sequence of events occurs after the receive fiber is cut on the line port:

1. WDM and OSC Loss of Light Receive faults are raised on the near end line port. The near end therefore meets (*Cond. 1*).
2. The near end turns off its WDM output and sends an APSD shutdown signal on the OSC to the far end.
3. When the far end receives the shutdown signal, the far end meets (*Cond. 2*) and shuts down its WDM output.
4. Both fibers are no longer illuminated by the WDM, and the safety hazard is avoided.

When the fiber cut is repaired, or when the disconnected fiber is reconnected, the recovery proceeds as follows:

1. The OSC Loss of Light Receive fault on the near end line port is cleared. The near end no longer meets (*Cond. 1*).
2. The near end turns on its WDM output and stops transmitting the APSD shutdown signal to the far end.
3. Since the far end no longer receives the APSD shutdown signal, the far end no longer meets (*Cond. 2*) and reenables the WDM output.
4. Both the near end and the far end restore traffic onto the span.

Laser Safety: Automatic Power Reduction

To guard against accidental exposure to high power lasers, some ports support automatic power reduction (APR). APR reduces the output of the laser when a fiber cut is detected.



WARNING: APR is performed in software on the service module and is disabled whenever the service module undergoes a warm or cold reload. In a cold reload, the lasers are turned off and are in a safe state. In a warm reload, however, the lasers remain on while APR is disabled.

Without being limited to the foregoing, a service module might undergo a warm reload in the following situations:

- The user issues an operator command that warm reloads the service module.
 - The user issues an operator command that cold or warm reloads the Chassis Management Module (CMM) in a single CMM system.
 - The user performs a software upgrade of the chassis.
 - The user restores a configuration database to the chassis.
 - The user replaces the CMM in the chassis. See [“CMM Replacement” on page 41](#).
 - Any situation where a CMM fails in a single CMM system or where both CMMs fail in a dual CMM system. See [“CMM Failure or Removal” on page 41](#).
-
- [APR on 96-Channel Amplifier Modules on page 23](#)

APR on 96-Channel Amplifier Modules

The 96-Channel Amplifier client and DCM ports are capable of emitting high output powers. To guard against accidental exposure to high power lasers, these ports support APR, which reduces the output of the laser when a fiber cut is detected.

The 96-Channel Amplifier supports two APRs:

- Mid-stage between the DCM Out and DCM In ports. APR is triggered when a Loss of Light Receive (LoLightRx) fault is detected at the DCM IN port of the 96-Channel Amplifier module. Once APR is triggered, the output of the laser on the DCM Out port is automatically reduced to a safe level.
- Client Out port. APR is triggered when the optical back reflection (OBR) exceeds the threshold, and the output power is larger than 5 dBm. When APR is triggered, the output of the laser on the Client Out port is automatically reduced to a safe level.

Safety Rating and Label

All BT17800 Series products meet the FDA requirements for a class 1 laser product with a Class 1M hazard rating:

**LASER RADIATION DO NOT VIEW DIRECTLY WITH OPTICAL INSTRUMENTS CLASS 1M
LASER PRODUCT**

A caution label is located on each BT17800 Series laser circuit pack. Two different labels are used depending on the circuit pack.

Figure 1: Laser Safety Warning Label with Text



Figure 2: Laser Safety Warning Label Without Text



CAUTION: Read and understand all caution labels before working with the equipment.

BT17800 Series Laser Output Ports

The BT17800 Class 1M laser output ports are located on the following modules.

Table 4: Laser Output Ports

Module	Product Code (PEC)	Optical Wavelength	Port
96-Channel Amplifier	BT8A78AMP1	1528.77 nm to 1566.72 nm	DCM out
			Line Out
			C1 Out
96-Channel Fixed Mux/Demux	BT8A78MD03	1528.578 nm to 1566.928 nm	C1-C96 Out
			L1 Out
Wavelength Protection Switch	BT8A78WPS4	C-band: 1500 to 1570 nm	C1 Out A
		O-band: 1260 to 1350 nm	L1 Out B
		L-band: 1560 to 1620 nm	L1 Out A
			C2 Out A
			L2 Out B
			L2 Out A
			C3 Out A
			L3 Out B
			L3 Out A
			C4 Out A
			L4 Out B
			L4 Out A

Auto-Provisioning of BT17800 Equipment

When a hardware module is inserted into an unprovisioned slot, the BT17800 detects the insertion, and discovers and auto-provisions the module (if auto-provisioning is enabled). Auto-provisioning refers to the BT17800 automatically adding discovered equipment, including their locations and PECs, to the **equipment** branch of the component tree. In some cases, it might refer to automatic detection and provisioning of other hardware components. See the *BT17800 Command Line Reference Guide* for details.

If the slot that the module is inserted into has been pre-provisioned, then the module is not auto-provisioned. Instead, the inserted module is validated against the pre-provisioning, and if any differences are detected, the BT17800 raises an equipment mismatch alarm (eqptMism).

Auto-provisioning can be enabled or disabled. See [“Configuring Auto-Provisioning” on page 70](#) for details on how to change the auto-provisioning setting.

To see the list of hardware modules that are in the **equipment** branch of the component tree, use the **show equipment** command. For example (truncated for clarity):

```
bt17800# show equipment
```

Chassis	PEC	Admin State	Oper State	
chassis:1	BT8A78CH14	enabled	up	
Module	PEC	Admin State	Oper State	
cap:1/1	BT8A78CAP1	enabled	up	
cmm:1/A	BT8A78CMM1	enabled	up	
fan:1/1	BT8A78FAN3	enabled	up	
fan:1/2	BT8A78FAN3	enabled	up	
fan:1/3	BT8A78FAN3	enabled	up	
fan:1/4	BT8A78FAN3	enabled	up	
pem:1/1	BT8A78ACM1	enabled	up	
pem:1/3	BT8A78ACM1	enabled	up	
ufm:1/2	BT8A78UFM3	enabled	notPresent	
ufm:1/5	BT8A78UFM3	enabled	up	
ufm:1/7	BT8A78UFM4	enabled	notPresent	
ufm:1/8	BT8A78UFM4	enabled	up	
ufm:1/10	BT8A78UFM4	enabled	up	
BIC	PEC	Admin State	Oper State	
bic:1/2/1	BT8A78CFP1G	enabled	notPresent	
bic:1/5/1	BT8A78CFP1G	enabled	notPresent	
bic:1/5/2	BT8A78CFP1G	enabled	down	
bic:1/7/2	BT8A78CFP1G	enabled	notPresent	
bic:1/8/2	BT8A78SFP12G	enabled	up	
bic:1/10/2	BT8A78SFP12G	enabled	up	
Transceiver	PEC	Admin State	Oper State	Optical Format
cfp:1/5/1/1		enabled	notPresent	fixedX10
cfp:1/5/2/1		enabled	notPresent	tunableX1
msa:1/7/1/1		enabled	notPresent	tunableX1
cfp:1/7/2/1		enabled	notPresent	tunableX1
msa:1/8/1/1		enabled	up	tunableX1
sfpPlus:1/8/2/1		enabled	up	fixedX1
sfpPlus:1/8/2/4		enabled	up	fixedX1
sfpPlus:1/8/2/5		enabled	up	fixedX1
sfpPlus:1/8/2/6		enabled	up	fixedX1
sfpPlus:1/8/2/8	BP3AD6SS	enabled	up	fixedX1
sfpPlus:1/8/2/9	BP3AD6SS	enabled	up	fixedX1
msa:1/10/1/1		enabled	up	tunableX1
sfpPlus:1/10/2/1		enabled	up	fixedX1
sfpPlus:1/10/2/2		enabled	up	fixedX1
sfpPlus:1/10/2/3		enabled	up	fixedX1
sfpPlus:1/10/2/4	BP3AM6MS	enabled	up	fixedX1
sfpPlus:1/10/2/5		enabled	up	fixedX1
sfpPlus:1/10/2/6		enabled	up	fixedX1
sfpPlus:1/10/2/7	BP3AD6SS	enabled	up	fixedX1
sfpPlus:1/10/2/8	BP3AD6SS	enabled	up	fixedX1
sfpPlus:1/10/2/9	BP3AD6SS	enabled	up	fixedX1
sfpPlus:1/10/2/10	BP3AD6SS	enabled	up	fixedX1
sfpPlus:1/10/2/11	BP3AD6SS	enabled	up	fixedX1
sfpPlus:1/10/2/12	BP3AD6SS	enabled	up	fixedX1

Pre-Provisioning of BT17800 Components

The BT17800 supports pre-provisioning of components in its component tree. Pre-provisioning refers to the ability for an operator to provision components in advance of hardware installation, thereby allowing the decoupling of the hardware installation workflow from the provisioning workflow. Pre-provisioning is not just limited to equipment provisioning, but can include other provisioning such as the provisioning of services.

When pre-provisioning, it is normal to see an equipment missing alarm (eqptMiss) because the provisioned equipment is not physically present.

If a module is inserted into a slot that has been pre-provisioned, the inserted module is validated against the pre-provisioning, and if any differences are detected, the BT17800 raises an equipment mismatch alarm (eqptMism).

To see which modules have been pre-provisioned, use the **show equipment** command. For example (truncated for clarity):



NOTE: Modules that have an Oper State of `notPresent` are examples of pre-provisioning, where provisioning has been performed but the actual module has not been inserted. These modules do not appear in inventory.

```
bt17800# show equipment
```

Chassis	PEC	Admin State	Oper State
chassis:1	BT8A78CH14	enabled	up
Module	PEC	Admin State	Oper State
cap:1/1	BT8A78CAP1	enabled	up
cmm:1/A	BT8A78CMM1	enabled	up
fan:1/1	BT8A78FAN3	enabled	up
fan:1/2	BT8A78FAN3	enabled	up
fan:1/3	BT8A78FAN3	enabled	up
fan:1/4	BT8A78FAN3	enabled	up
pem:1/1	BT8A78ACM1	enabled	up
pem:1/3	BT8A78ACM1	enabled	up
ufm:1/2	BT8A78UFM3	enabled	notPresent
ufm:1/5	BT8A78UFM3	enabled	up
ufm:1/7	BT8A78UFM4	enabled	notPresent
ufm:1/8	BT8A78UFM4	enabled	up
ufm:1/10	BT8A78UFM4	enabled	up
BIC	PEC	Admin State	Oper State
bic:1/2/1	BT8A78CFP1G	enabled	notPresent
bic:1/5/1	BT8A78CFP1G	enabled	notPresent
bic:1/5/2	BT8A78CFP1G	enabled	down
bic:1/7/2	BT8A78CFP1G	enabled	notPresent
bic:1/8/2	BT8A78SFP12G	enabled	up
bic:1/10/2	BT8A78SFP12G	enabled	up

Transceiver	PEC	Admin State	Oper State	Optical Format
cfp:1/5/1/1		enabled	notPresent	fixedX10
cfp:1/5/2/1		enabled	notPresent	tunableX1
msa:1/7/1/1		enabled	notPresent	tunableX1
cfp:1/7/2/1		enabled	notPresent	tunableX1
msa:1/8/1/1		enabled	up	tunableX1
sfpPlus:1/8/2/1		enabled	up	fixedX1
sfpPlus:1/8/2/4		enabled	up	fixedX1
sfpPlus:1/8/2/5		enabled	up	fixedX1
sfpPlus:1/8/2/6		enabled	up	fixedX1
sfpPlus:1/8/2/8	BP3AD6SS	enabled	up	fixedX1
sfpPlus:1/8/2/9	BP3AD6SS	enabled	up	fixedX1
msa:1/10/1/1		enabled	up	tunableX1
sfpPlus:1/10/2/1		enabled	up	fixedX1
sfpPlus:1/10/2/2		enabled	up	fixedX1
sfpPlus:1/10/2/3		enabled	up	fixedX1
sfpPlus:1/10/2/4	BP3AM6MS	enabled	up	fixedX1
sfpPlus:1/10/2/5		enabled	up	fixedX1
sfpPlus:1/10/2/6		enabled	up	fixedX1
sfpPlus:1/10/2/7	BP3AD6SS	enabled	up	fixedX1
sfpPlus:1/10/2/8	BP3AD6SS	enabled	up	fixedX1
sfpPlus:1/10/2/9	BP3AD6SS	enabled	up	fixedX1
sfpPlus:1/10/2/10	BP3AD6SS	enabled	up	fixedX1
sfpPlus:1/10/2/11	BP3AD6SS	enabled	up	fixedX1
sfpPlus:1/10/2/12	BP3AD6SS	enabled	up	fixedX1

Turning Up the Software on the BTI7800

Use this procedure to turn up the software on a BTI7800 for the first time. This involves commissioning the system and installing the desired software load.

The BTI7800 Chassis Management Modules (CMMs) have non-volatile memory that stores software loads for all modules in the chassis. When a service module boots up, it retrieves its software image from the CMM.

Although each type of module has its own software image, the software that you install on the CMM comes in a single package. When you install the package onto the CMM, the CMM extracts the individual module images and makes them available to prospective service modules when they boot up.

The CMMs come preloaded with software from the factory, but the preloaded software version is not necessarily the software version that you ordered. The factory does not perform installation of the ordered software prior to shipping. You must install the requested software load yourself.

There are two ways to install software on a CMM:

- Using CLI commands to install an RPM file from a network download. This requires you to commission the BTI7800 first so that the BTI7800 has access to the network.
- Using a system repair drive to install software from local media. You can download the desired software load onto a USB drive and install the load onto the CMM from the USB drive. You do not need to commission the BTI7800 before you use this method. The USB software image is available as a gzipped file. You must gunzip the file before installing.

Prerequisites

- The BTI7800 chassis is installed, grounded, and powered. All common equipment with the exception of the Chassis Management Modules (CMMs) are installed and operational. See the *BTI7800 Series Hardware Overview and Installation Guide* for procedures on how to do this.
 - Ensure the CMMs and service modules are not yet inserted into the chassis.
1. Commission the system using the procedure described in [“Commissioning the BTI7800 for the First Time” on page 30](#).
 2. Retrieve the software image using the procedures described in [“Retrieving a BTI7800 Software Image” on page 267](#). The software is provided as an RPM file for use with CLI commands and as a gzipped USB image for use with a system repair drive.
Download the RPM or USB image as desired.
 3. Upgrade the software.
 - To upgrade using the CLI, see [“Upgrading the Software” on page 229](#).

- To upgrade using a USB drive, see [“Installing a Software Load on a CMM Using a System Repair Drive” on page 261](#).

You are now ready to install the service modules and provision the system and services.

Commissioning the BTI7800 for the First Time

Use this procedure to commission a BTI7800 Series chassis for the first time. Commissioning resets the configuration database to factory defaults and sets up basic system parameters that allow the system to be managed.



NOTE: Do not use this commissioning procedure if you are commissioning a replacement CMM on an in-service chassis. Follow the procedure in [“Restoring the Database from a Backup Without Affecting Service” on page 251](#) instead.



NOTE: This procedure resets the database to factory defaults and is service affecting. All existing provisioning is erased.

When you commission a chassis, you commission the CMM for that chassis. If you move a commissioned CMM to another chassis, you will need to commission the CMM for the new chassis.

You only need to commission a CMM for a dual CMM chassis if the chassis does not have an active CMM. If the chassis has an active CMM, the CMM that you insert will automatically become commissioned when it synchronizes with the active CMM. For this same reason, you only need to commission one CMM when turning up a dual CMM chassis. Once the commissioned CMM becomes active, the second CMM becomes commissioned when it synchronizes with the active CMM.

1. Seat the CMM into slot A. If your system has two CMMs, leave the other CMM unseated.
2. Log in locally to the CMM in slot A over the craft serial or craft Ethernet port.

For information on how to do this, see [“Logging In to the CMM Craft Ethernet or Craft Serial Ports” on page 45](#).

3. Enter setup mode. This is known as the commissioning shell.

```
localhost console
localhost login: admin
Password:

Shell Help: List of the commands you can use:
setup - Commission the CMM
cli    - Open CLI interface to the system
reboot - Reboot the CMM
exit   - Logout
```

```
scm1:~$ setup

Welcome to the BTI 7800 Series - CMM Commissioning Application!
Note: This process commissions one CMM at a time.
Type 'help' or '?' for the list of the commands. Press '<Ctrl> + C' at
any time to exit.
(cmm-setup)$
```

4. To see the list of available commands, type **help**.



NOTE: The commands in the commissioning shell should only be used on an uncommissioned system. Do not use the commissioning shell commands as a substitute for regular CLI commands.

5. Set the time zone.

For example:

```
(cmm-setup)$ settz

Please identify a location so that time zone rules can be set
correctly.
Please select a continent or ocean.
1) Africa
2) Americas
3) Antarctica
4) Arctic Ocean
5) Asia
6) Atlantic Ocean
7) Australia
8) Europe
9) Indian Ocean
10) Pacific Ocean
11) none - I want to specify the time zone using the Posix TZ format.
#?
```

Follow the series of menu-driven options to set the time zone.



NOTE: You must manually set the correct time zone, date, and time even if you use NTP servers. The BTI7800 requires a correct clock at all times, including the period prior to the establishment of NTP server connectivity. Use of NTP servers is recommended.

6. Set the date.

For example:

```
(cmm-setup)$ setdate

Set the system date and confirm setting.
```

```
The current date is 2015-01-01.
Enter the new date (in the format YYYY-MM-DD): 2015-06-12
System Date will be set to 2015-06-12
Confirm (yes/no/abort): yes

System Date is set to 2015-06-12
```

7. Set the time.

For example:

```
(cmm-setup)$ settime

Set the system time and confirm setting.

The current time is 00:02:48, Timezone is America/New_York.
Enter the new time (in 24-hour format-- HH:MM:SS): 12:13:00
System time will be set to 12:13:00
Confirm (yes/no/abort): yes

System time is set to 12:13:00
```

8. Set up the networking parameters.



NOTE: All parameters are required to be set for proper operation of the BTI7800.

For example:

```
(cmm-setup)$ commission

Set the parameters required for initial, basic CMM setup and system
management, and confirm the settings.

Controller Id: 1

Note: The System Management (Shared), Individual CMM, and Default
Gateway IP Addresses must be in the same network.

Enter System Management (Shared) Address (a.b.c.d): 10.10.1.22

Enter Management Netmask (/N or a.b.c.d): 255.255.255.0

Enter Default Gateway Address (a.b.c.d): 10.10.1.1

Enter NTP Server address (a.b.c.d): 192.168.35.251

Enter DNS Server address (a.b.c.d): 10.10.1.1

You have entered following values:
Controller ID                : 1
System Management (Shared) Address : 10.10.1.22
Management Netmask           : 255.255.255.0
Default Gateway Address       : 10.10.1.1
NTP servers                   : 192.168.35.251
DNS servers                   : 10.10.1.1
```

```
Confirm (yes/no/abort): yes
```

```
Do you wish to reset the database to factory defaults? This will impact traffic.
Confirm (yes/no):
```

9. Set the database to factory defaults.

This removes the existing configuration database and initializes a new database, but retains the commissioning parameters that you just set.

For example:

```
Do you wish to reset the database to factory defaults? This will impact traffic.
Confirm (yes/no): yes
```

The following values are set:

```
Controller ID           : 1
System Management (Shared) Address : 10.10.1.22
Management Netmask      : 255.255.255.0
Default Gateway Address : 10.10.1.1
NTP servers              : 192.168.35.251
DNS servers              : 10.10.1.1
```

If you are going to restore a database as part of commissioning, do that next - otherwise, reboot for IP settings to take effect.

10. Set the individual management IP address of the CMM. This is optional.

This address must be on the same subnet as the System Management (Shared) Address that you entered earlier.

```
(cmm-setup)$ setcmmip
```

```
Enter Individual (CMM) Management Address: 10.10.1.33
```

You have entered following value:

```
Individual CMM Address      : 10.10.1.33
```

```
Confirm (yes/no/abort): yes
```

11. Verify the settings.

For example:

```
(cmm-setup)$ show
```

```
Controller ID           : 1
Management Shared IP Address : 10.10.1.22
Management Netmask      : 255.255.255.0
Individual CMM IP       : 10.10.1.33
Default Gateway Address : 10.10.1.1
NTP Server Address      : 192.168.35.251
DNS Server Address      : 10.10.1.1
Current Time            : 12:40:59
Current Date            : 2015-06-12
Time Zone               : America/New_York
```

```
OS Version           : 1.0.0-16305
Application Version   : 3.0.0 17453
```

Proceed to step 12 if the settings are correct. Otherwise, go back and correct the settings as necessary by reissuing the respective command(s).

12. Reboot the CMM.

```
(cmm-setup)$ reboot

Do you want this CMM to reboot? (yes/no) : yes

Broadcast message from root@scm1 (pts/0) (Fri Jun 12 12:41:37 2015):

The system is going down for reboot NOW!
```

The CMM in slot A reboots and assumes the role of the active system controller module (SCM). This might take several minutes. Proceed to the next step after the CMM finishes rebooting.

13. If you have a dual CMM system, seat the other CMM into slot B. The CMM in slot B will now synchronize with the CMM in slot A. This might take several minutes. When this is finished, the Active LED on the CMM in slot B turns green.
14. Log in to the CLI using the shared management IP address and verify that the CMMs are synchronized if applicable. For information on how to log in to the CLI, see [“Logging In to the CLI” on page 44](#).

The examples below have been edited to show only the relevant output.

In a dual CMM system, the CMMs are synchronized when the HA Status is In Sync:

```
bti7800# show system

Active Controller      : cmm:1/A
Backup Controller     : cmm:1/B
HA Status              : In Sync
```

In a single CMM system, only the active controller is listed:

```
bti7800# show system

Active Controller      : cmm:1/A
HA Status              : Not Ready
```

15. Perform a cold reload of all modules in the system. This ensures the CMM and all service modules are properly synchronized.

```
bti7800# system reload all cold
```

The chassis is now commissioned.

Proceed to configure other system settings including administrative parameters (see [“Configuring General Administrative Parameters” on page 61](#)).

If you want to change the shared management IP address after commissioning, see [“Configuring the Shared Management IP Address and Subnet” on page 62](#).

If you want to restore the database from a backup, see [“Restoring the Database from a Backup from the CLI” on page 257](#).



NOTE: Before you remove a commissioned CMM from a chassis, always uncommission the CMM first. See [“Uncommissioning a CMM” on page 264](#). Uncommissioning ensures that the CMM behaves predictably when you later insert it into a chassis.

CHAPTER 2

Chassis Management

- [Management Overview on page 37](#)
- [Chassis Management Module \(CMM\) on page 39](#)
- [Logging In to the CLI on page 44](#)
- [Logging In to the CMM Craft Ethernet or Craft Serial Ports on page 45](#)

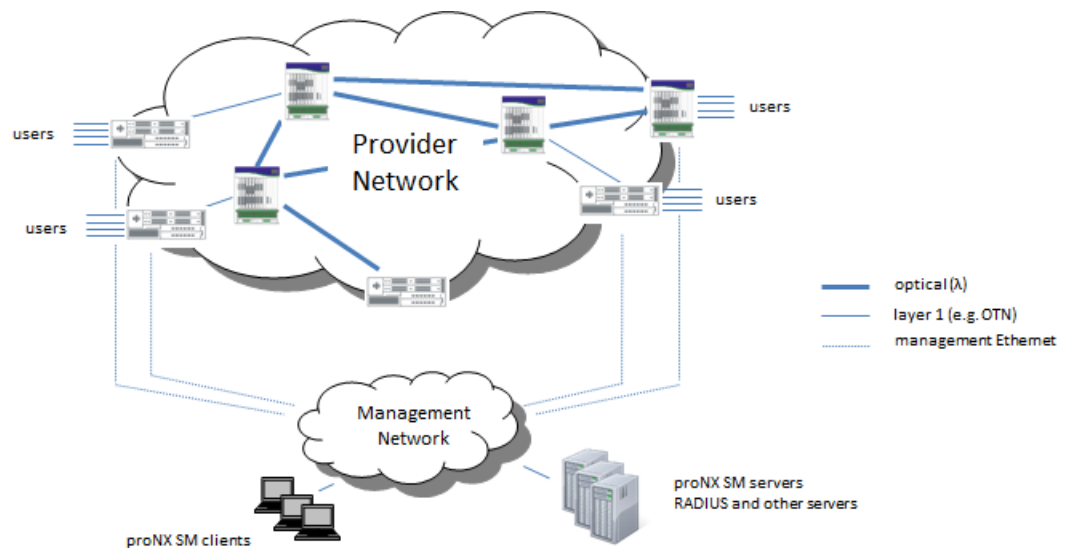
Management Overview

The BT17800 supports both inband management (releases 2.1.1 through release 4.4) and out-of-band management. The inband management network runs over the optical network infrastructure while the out-of-band management network connects to the BT17800 over a separate management Ethernet connection. A typical deployment uses both methods where inband management is used throughout except for those network elements (NEs) not part of the optical network.

This is shown in the following figure where the NEs that are part of the optical network infrastructure are managed inband while the NEs not part of the optical network infrastructure are managed over out-of-band management Ethernet connections. The NE on the far right acts as a gateway, routing management traffic between its out-of-band management Ethernet interface and the inband management network.



NOTE: Inband management is no longer supported starting in release 4.5.



Management functionality for the BT17800 resides within the Chassis Management Module (CMM). Each network element contains up to two CMMs (for redundancy), with each CMM connecting separately to the management Ethernet network if out-of-band management is required. If one connection goes down, the network element is still reachable through the other link. In the inband management network where management traffic is sent over optical links, redundancy is provided through proper optical network design.

You can get access to the NE's management software interface by connecting to a management IP address that is shared between the two CMMs. The IP address is the same regardless of whether the network element is being managed out-of-band or inband. Although both CMMs share this same IP address, only the currently active CMM owns (and responds to) the shared IP address. Additionally, each CMM can be assigned its own dedicated individual IP address. Use of this individual IP address is for advanced troubleshooting and is beyond the scope of this document.

You have the choice of connecting to the following management software interfaces on the CMM:

- CLI on the active CMM through the shared management IP address
- NETCONF on the active CMM through the shared management IP address
- SNMP on the active CMM through the shared management IP address
- Management OS shell:
 - on the active CMM, through the shared management IP address or through the active CMM's individual IP address
 - on the standby CMM, through the standby CMM's individual IP address

Working with the management OS shell is for advanced troubleshooting only and is beyond the scope of this document.

For the port numbers to use to connect to these management software interfaces, see [“BTI7800 Port Usage” on page 277](#).

Constraints

The following constraints apply to the management network:

- On any given network element, the shared IP address, the individual CMM IP addresses, and the default gateway must all reside on the same subnet.
- Each BTI7800 network element should be managed by at most two PSM servers (for performance reasons).
- The management network must support an MTU size of 1500 bytes.

Release History Table

Release	Description
4.5	Inband management is no longer supported starting in release 4.5.
2.1.1	inband management

Chassis Management Module (CMM)

- [CMM Overview on page 39](#)
- [CMM Failure or Removal on page 41](#)
- [CMM Replacement on page 41](#)

CMM Overview

The Chassis Management Module (CMM) provides management and control of the chassis, and is responsible for the following functions:

- Monitors, controls, and assures proper operation of the modules and other chassis components.
- Watches over the basic health of the system, reports anomalies, and takes corrective action when needed.
- Retrieves inventory information and sensor readings, as well as, receive event reports and failure notifications from the modules and field replaceable units (FRUs).
- Performs basic recovery operations, such as, power cycle or reset of managed entities.
- Provides low-level hardware management services to manage the power, cooling, and interconnect resources of a chassis.
- Provides non-volatile storage of configuration data and software loads.
- Enables operator control of all modules in the system.
- Supports an industry-standard CLI, NETCONF, and SNMP.

Figure 3: CMM Module



Table 5: CMM Ports

Port	Physical Interface	Description
Craft Serial (RS-232)	RJ-45	Provides local craft serial access for diagnostic and commissioning functions.
Expansion (EXP-1 to EXP-3)	RJ-45	Provides management plane connectivity in a multichassis configuration.
Management Ethernet (eth1)	RJ-45	Provides management network connectivity.
Craft Ethernet (eth0)	RJ-45	Provides local craft Ethernet access for diagnostic and commissioning functions.
USB-1	USB 2.0 Standard Type-A Receptacle	Provides the ability for the CMM to boot from a system repair drive.

CMMs are typically deployed in pairs in a network element in an active/standby configuration. The active CMM performs all of the management and control functions in the system. If the active CMM fails, the standby CMM takes over and becomes the active CMM.

A CMM can take on the following roles:

CMM Role	Description
Active system controller module (SCM)	The first CMM that comes up in a chassis is the active SCM. It performs all of the management and control functions in the system, and ensures that all modules (including the standby CMM) are loaded with the correct level of software. Therefore it is important that the first CMM in the chassis contain the software load that you want to run.
Standby SCM	The second CMM that comes up in a chassis becomes the standby SCM. The standby SCM automatically synchronizes with the active SCM so that the standby SCM can take over seamlessly if the active SCM fails. Configuration data, and operational data such as traffic module statistics, are mirrored on both SCMs.
Management relay module (MRM)	The role of the MRM applies to multichassis systems only. A multichassis system consists of a hub chassis and a satellite chassis. The CMMs in the hub chassis act as active and standby SCMs, similar to a single chassis system. The CMMs in the satellite chassis act as MRMs, relaying management commands and information between the active SCM in the hub chassis and the various modules in the satellite chassis. For more information on multichassis systems and MRMs, see “Multichassis System Configuration” on page 179 .

When using out-of-band management, both CMMs in a chassis should be physically connected to the management network. If the management Ethernet link to the active CMM fails, the standby CMM becomes the active CMM. In a multichassis system, only the SCMs (in the hub chassis) are connected to the management network.

CMM Failure or Removal

CMMs are typically deployed in pairs in a network element in an active/standby configuration. The active CMM performs the management and control functions in the system. If the active CMM fails or if the active CMM is removed or if the management Ethernet link to the active CMM goes down, the standby CMM takes over and becomes the active CMM. This is performed seamlessly without affecting traffic on the service modules.

If both CMMs fail or if both CMMs are removed in a dual CMM system, or if the sole CMM fails or if the sole CMM is removed in a single CMM system, the behavior is as follows:

- Management connectivity (CLI, SNMP, NETCONF) is lost.
- Alarms are no longer raised and PM collection stops.
- Chassis fans operate at full speed.
- Modules subsequently inserted into the chassis will not boot up. This includes modules that you remove and reinsert.
- Service is not affected.
 - In releases lower than 4.2, all service modules are warm reloaded and do not boot back up until the CMM recovers. Service modules continue to carry traffic but software-based features on the service modules (such as PM collection, APSD, APR, FPSD) are disabled until the service modules boot up.
 - Starting with release 4.2, service modules run normally and continue to carry traffic. Software-based features on the service modules (such as PM collection, APSD, APR, FPSD) continue to run normally.
- If the CMM that went down comes back up, it performs a warm reload of all service modules. This ensures that the CMM is synchronized with the service modules and that the service modules are in a known state. Service is not affected. Software-based features on the service modules (such as PM collection, APSD, APR, FPSD) are disabled temporarily while the service module reloads.

CMM Replacement

CMM replacement differs depending on whether you are replacing a CMM in a dual CMM system or in a single CMM system.



NOTE: You can always remove and reinsert a CMM with no impact to traffic as long as you reinsert the same CMM (that is, the same physical module with the same configuration).

Always uncommission a CMM before removing it from a chassis. This way, the CMM is in an uncommissioned state and cannot assume control of a chassis until it is recommissioned. This guards against situations where a CMM is placed into storage and then later reused in the same chassis in which it was originally commissioned. In that situation, the CMM might assume control and impose its old database onto the chassis.

- [Dual CMM System on page 42](#)
- [Single CMM System on page 42](#)

Dual CMM System

CMM replacement in a dual CMM system behaves as follows:

- You can remove and replace the standby CMM with no impact to traffic. When you insert the replacement CMM, the replacement CMM automatically synchronizes with the active CMM.
- You can remove and replace the active CMM with no impact to traffic. When you remove the active CMM, the standby CMM becomes the active CMM. When you subsequently insert the replacement CMM, the replacement CMM becomes the standby CMM and automatically synchronizes with the newly active CMM.

Single CMM System

When you replace the sole CMM in a chassis, the replacement CMM has no active CMM to synchronize with. Therefore, you will need to commission the replacement CMM.

- If you previously backed up the configuration database, you can commission the replacement CMM to use the backed-up database, resulting in no impact to traffic:
 - A configuration database is specific to a software version. In order to restore a backed-up database onto a replacement CMM, you must ensure that the replacement CMM is running the same software version as the software version running when the backup was created.
 - In releases lower than 4.2, a configuration database is also specific to a chassis. You can only restore a backed-up database to a replacement CMM on a chassis if the database was backed up from that chassis. You cannot restore a database to a CMM on a chassis if the database was backed up from another chassis.

Starting with release 4.2, this restriction is relaxed. You can restore a backed-up database to any chassis of the same chassis type (BT17801 to BT17801, BT17802 to BT17802, BT17814 to BT17814).

- If you did not back up the configuration database and cannot do so now, you will need to commission the replacement CMM to use the factory-default configuration, which results in traffic loss and which requires subsequent reconfiguration.



NOTE: On the BT17801, you do not need to reset the database to factory defaults if you neglected to back up the database explicitly. The database is automatically backed up to local chassis storage at regular intervals.

The existing configuration database residing on the replacement CMM is not used and does not take effect when you insert the replacement CMM into the chassis. The system checks to see if the CMM is commissioned for the chassis in which it is inserted. If it is not, you will need to commission the CMM before the replacement CMM can be used. During commissioning, the existing configuration database is erased. This prevents the CMM from changing configuration on all the modules and affecting services if you remove a CMM from one chassis and accidentally insert it into another chassis.

[Table 6 on page 43](#) shows the different CMM replacement scenarios in single CMM systems.

Table 6: CMM Replacement Scenarios in Single CMM Systems

Replacement Scenario	General Replacement Procedure
The replacement CMM is running the same software load as the CMM being replaced, and a backed-up configuration database of the original CMM exists.	<p>Commission the CMM for this chassis.</p> <p>As part of commissioning, restore the configuration database from the original CMM. Once the CMM has been commissioned, it performs a warm reload of all service modules.</p> <p>Service is not affected but software-based features on the service modules (such as PM collection, APSD, APR, FPSD) are disabled temporarily. See “CMM Failure or Removal” on page 41.</p>
The replacement CMM is running a software load that is different from the software currently running on the chassis, and a backed-up configuration database of the original CMM exists.	<p>Install the software version that was running on the original CMM onto the replacement CMM.</p> <p>Commission the CMM for this chassis.</p> <p>As part of commissioning, restore the configuration database from the original CMM. Once the CMM has been commissioned, it performs a warm reload of all service modules.</p> <p>Service is not affected but software-based features on the service modules (such as PM collection, APSD, APR, FPSD) are disabled temporarily. See “CMM Failure or Removal” on page 41.</p>
Any replacement situation where a backed-up configuration database of the original CMM does not exist.	<p>Since the configuration cannot be restored, all configuration is lost and service is affected.</p>

For the detailed CMM replacement procedure, see [“Replacing the CMM in a Single CMM System” on page 259](#).

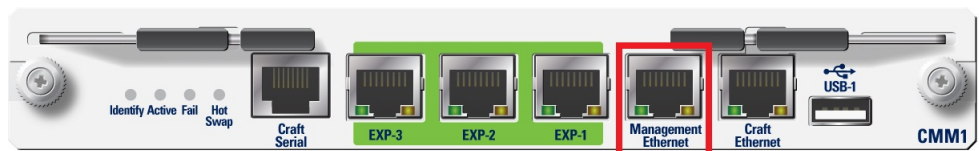
Release History Table

Release	Description
4.2	Starting with release 4.2, service modules run normally and continue to carry traffic. Software-based features on the service modules (such as PM collection, APSD, APR, FPSD) continue to run normally.
4.2	Starting with release 4.2, this restriction is relaxed. You can restore a backed-up database to any chassis of the same chassis type (BTI7801 to BTI7801, BTI7802 to BTI7802, BTI7814 to BTI7814).

Logging In to the CLI

Use this procedure to log in to the BTI7800 CLI. The BTI7800 CLI can be reached through SSH on port 22. The BTI7800 can support up to 20 simultaneous user CLI sessions.

1. Physically connect the Management Ethernet interface on the CMM to your management IP network.



2. Start an SSH session to the management interface from a computer on the management network. Use the shared management IP address you configured during commissioning and use port 22.



NOTE: The BTI7800 has multiple IP addresses. You should always use the shared management IP address to reach the CLI. See [“Management Overview” on page 37](#) for more information on the shared management IP address.

For Linux and MAC OS X, launch a terminal window and start an SSH session. For Windows, install and launch a terminal application (for example, PuTTY).

```
$ ssh -p22 user@10.228.220.104
```

```
*****
* WARNING! The use of this system is restricted to authorized users.      *
*                                                                           *
* All information and communications on this system are subject to review,*
* Monitoring and recording at any time, without notice or permission.    *
*                                                                           *
*****
user@10.228.220.104's password:
Welcome to BTI 7800 CLI admin connected from 192.168.0.157 using ssh on scm2
bti7800#
```

After you supply the correct login credentials, you will be logged in to the active SCM.

- When you log in, your CLI session is automatically placed in operational mode. To enter configuration mode type **config**. To return to operational mode, type **exit**.

```
bti7800# config
Entering configuration mode terminal
bti7800(config)#
bti7800(config)# exit
bti7800#
```

Operational mode commands do not change the stored configuration. An example of an operational mode command is the **show** command. To change the stored configuration, you must execute commands in configuration mode.

- If desired, use the **set** command to set user preferences for this session.

```
bti7800# set ?
Possible completions:
complete-on-space      Enable/disable completion on space
idle-timeout           Configure idle timeout
ignore-leading-space   Ignore leading whitespace (true/false)
paginate              Paginate output from CLI commands
prompt1               Set operational mode prompt
prompt2               Set configure mode prompt
screen-length          Configure screen length
screen-width           Configure screen width
terminal              Set terminal type
```

For example, to set the **idle-timeout** to 6000 seconds:

```
bti7800# set idle-timeout 6000
bti7800#
```



NOTE: If you want settings to persist across login sessions, use the **user-profile** command in configuration mode.

Logging In to the CMM Craft Ethernet or Craft Serial Ports

Use this procedure to log in to the craft Ethernet or craft serial ports on a CMM. You typically do this when commissioning a new system, performing a software installation from a system repair drive, setting the CMM software and configuration back to factory defaults, or resetting the admin user's password.

Table 7: Port Settings

Type of connection	Settings
Serial	<ul style="list-style-type: none"> Baud rate: 115200 bps (bits per second) Data bits: 8 Parity: None Stop bits: 1 bit
Ethernet	<ul style="list-style-type: none"> Management IP address / subnet of craft Ethernet port: 192.168.17.1/24 SSH port: 22

- Set the port parameters on your PC.
 - For the craft serial port, set the serial port parameters on your PC as specified in [Table 7 on page 46](#).
 - For the craft Ethernet port, set the IP address of the Ethernet port on your PC to be on the same subnet as the management IP address specified in [Table 7 on page 46](#).
- Connect an RS-232 or Ethernet UTP cable (CAT5 or better) from your PC to the respective CMM craft port.



- Establish communication with the management interface on the craft port.
 - For the craft serial port, press the Enter key to get the login prompt.
 - For the craft Ethernet port, start an SSH session to the management interface.

For Linux and MAC OS X, launch a terminal window and start an SSH session. For Windows, install and launch a terminal application (for example, PuTTY).

```
$ ssh -p22 192.168.17.1
```

Once connected, you will see the login prompt.
- Log in as the admin or admincraft user, as follows:
 - Most of the tasks require you to log in as the admin user. When logging in as the admin user, use the password that you configured for the admin user.
 - Log in as the admincraft user only if you want to reset the admin user's password (such as when you have lost the admin user's password and you have no access to any other administrator accounts). The admincraft user is a special user only authorized to log in locally on the craft interface. The admincraft password is hardcoded to **admincraft** and cannot be changed. For information on resetting the admin user's password, see ["Resetting the Password for the admin User" on page 52](#).



NOTE: The login credentials and the available commands are different if you are booting up from a system repair drive. For more information, see [“Installing a Software Load on a CMM Using a System Repair Drive” on page 261.](#)

If you are logging in on the craft serial port or if you are logging in to an uncommissioned chassis, you are placed in the commissioning shell. For example:

```
localhost login: admin
Password:
Shell Help:
List of the commands you can use:
setup - Commission the CMM
cli    - Open CLI interface to the system
reboot - Reboot the CMM
exit   - Logout

scm1:~$
```



NOTE: Only use the commissioning shell commands listed in the help output. Unlisted commands are not supported and should not be used.

If you are logging in on the craft Ethernet port on a commissioned chassis, you are placed in a CLI session.

5. Most tasks require you to be in the commissioning shell.

- To move from the initial CLI session to the commissioning shell:

```
bt17800# debug-utils shell
scm1:~$ setup

Welcome to the BTI 7800 Series - CMM Commissioning Application!
Note: This process commissions one CMM at a time.
Type 'help' or '?' for the list of the commands. Press '<Ctrl> + C' at any
time to exit.

(cmm-setup)$
```

To return to the CLI, type **exit**.

- To move from the shell to a CLI session:

```
scm1:~$ cli
*****
* WARNING! The use of this system is restricted to authorized users. *
*
* All information and communications on this system are subject to review,*
* Monitoring and recording at any time, without notice or permission. *
*****
```

```
*
*****
admin@10.91.0.5 password:
Welcome to BTI 7800 CLI
admin connected from 10.91.0.5 using ssh on scm1
bti7800#
```

To return to the shell, type **exit**.



NOTE: You can only enter a CLI session if the CMM is commissioned.

Release History Table

Release	Description
4.4	Log in as the admincraft user

CHAPTER 3

User Accounts and Authentication

- [Users and Access Privileges on page 49](#)
- [User Authentication and Authorization on page 52](#)

Users and Access Privileges

Access privileges to the BT17800 are managed by associating a user with an access group. The group defines the access privilege level for a user.

- [Users on page 49](#)
- [Access Privileges on page 49](#)
- [Adding a User Account on page 50](#)
- [Configuring User Session Parameters on page 51](#)
- [Resetting the Password for the admin User on page 52](#)

Users

The BT17800 creates a default user **admin** that has full system access privileges. The purpose of the default user is to allow first time access to the BT17800 for initial system connectivity and configuration tasks. The user **admin** cannot be deleted.



NOTE: For security purposes, once you complete initial configuration tasks, you should change the **admin** user password. It is also recommended that you create new users with full (superuser) access privileges instead of continuing to use the **admin** user to manage your system.



CAUTION: Do not forget the passwords to your superuser accounts. If you forget the passwords to all of your superuser accounts, you will need to recommission the system in order to regain superuser access.

Access Privileges

The BT17800 supports the following access privilege groups:

Table 8: BT17800 Access Privilege Groups

Group Name	Access Level
superuser	Full access to all system operations.
provisioning	Access to most network management configuration tasks. This level does not have access to some administrative tasks.
surveillance	Read-only access to monitor system operations.

Adding a User Account

Use this procedure to add a user account to the local configuration database.

The following restrictions apply:

- Only a user with superuser privileges can create, modify, and delete user accounts.



NOTE: To ensure there is at least one user with full system access, BT17800 prevents deleting and editing the name and access privilege of the admin user.

- Enter configuration mode.

```
bt17800# config
bt17800(config)#
```

- Create the user, including name, password, and access privilege group.

For example:

```
bt17800(config)# users JohnSmith group provisioning password "<password>"
bt17800(config)# commit
Commit complete.
```



NOTE: See the *BT17800 Series Command Line Reference Guide* for information on how passwords with non-alphanumeric characters are entered.

- Display the list of users.

```
bt17800(config)# do show running-config users
users user1 password $ABC123
users user1 group superuser
users user2 password $ABC123
users user2 group provisioning
```

```

users user3 password $ABC123
users user3 group provisioning
users admin password $ABC123

```

The passwords are displayed in an encrypted form.

Configuring User Session Parameters

Use this procedure to configure user session parameters.

User session parameters govern CLI behavior for the specified user. You can create command aliases, change the prompt, configure the idle timeout, and control many more session parameters. For a complete list of parameters, see the *BT17800 Series CLI Reference Guide*.

1. Enter configuration mode.

```

bti7800# config
bti7800(config)#

```

2. Enter user-profile mode for the user you want to manage.

For example:

```

bti7800(config)# user-profile user
bti7800(config-user-profile-user)#

```

If the profile does not exist, it is created.

3. Set the various parameters as desired.

For example, to disable the autowizard, enable pagination, and to set the idle timeout to 300 seconds:

```

bti7800(config-user-profile-user)# session autowizard false
bti7800(config-user-profile-user)# session paginate true
bti7800(config-user-profile-user)# session idle-timeout 300

```

4. Apply the changes.

For example:

```

bti7800(config-user-profile-user)# commit
Commit complete.

```



NOTE: Some changes take effect immediately. Others take effect when you reenter configuration mode. Yet others take effect the next time you log in.

Resetting the Password for the admin User

Use this procedure to reset the admin user's password to the factory default setting. This procedure requires you to log in to the craft interface. You cannot reset the admin password over the management network.



NOTE: This procedure is specific to resetting the password for the user called admin. It cannot be used to reset any other user's password.

1. Log in to the craft interface of the active CMM as the admincraft user. See [“Logging In to the CMM Craft Ethernet or Craft Serial Ports” on page 45](#).

If you do not know which CMM is active, try one CMM, and if the login attempt fails, try the other. The admincraft user is only allowed to log in to the active CMM. The system rejects any login attempts as the admincraft user on the standby CMM.

2. Start a CLI session.
 - If you log in on the craft serial port, you are placed into the commissioning shell. Type **cli** to start a CLI session.
 - If you log in on the craft Ethernet port, you are automatically placed into a CLI session.
3. Reset the admin password using the debug utilities command.

```
bt17800# debug-utils reset-admin-password
Commit complete.
bt17800#
```

The admin password is now reset to the factory default setting.

4. Type **exit** to exit the CLI session.

Release History Table

Release	Description
4.4	Use this procedure to reset the admin user's password to the factory default setting.

User Authentication and Authorization

The BT17800 supports local database and RADIUS/TACACS+ user authentication and authorization for CLI and NETCONF users.



NOTE: RADIUS is supported prior to release 2.1.1. TACACS+ is supported starting with release 4.1.

- [Local Authentication and Authorization on page 53](#)
- [RADIUS/TACACS+ Authentication and Authorization on page 53](#)
- [Authentication and Authorization Sequence on page 55](#)
- [Configuring the RADIUS/TACACS+ Server on page 56](#)
- [Provisioning RADIUS Authentication and Authorization on page 56](#)
- [Provisioning TACACS+ Authentication and Authorization on page 58](#)

Local Authentication and Authorization

The BT17800 maintains a local configuration database of users and their privilege levels. These users are managed with the **users** CLI command. When a user attempts to log in, the BT17800 checks the supplied username and password against the local configuration database. Local authentication (and authorization) is the default method used on the BT17800.

RADIUS/TACACS+ Authentication and Authorization

RADIUS and TACACS+ are two common client-server authentication, authorization, and accounting (AAA) protocols. The BT17800, acting as a RADIUS/TACACS+ client, communicates securely with the RADIUS/TACACS+ server to authenticate and authorize users. In response to a login request, the RADIUS/TACACS+ server authenticates the user and returns the access privilege level for that user.



NOTE: The BT17800 does not support accounting using RADIUS/TACACS+.

User credentials are encrypted using a shared secret that is known to both the BT17800 and the RADIUS/TACACS+ server. For RADIUS, the shared secret is used to encrypt the user password. For TACACS+, the shared secret is used to encrypt the entire contents of TACACS+ packets.

The BT17800 supports the following packet types and attributes according to *RFC 2865 Remote Authentication Dial In User Service* ([Table 9 on page 53](#)) and *draft-grant-tacacs-02.txt* ([Table 10 on page 54](#)).

Table 9: RADIUS Packets

Packet type	Attribute	Description
ACCESS-REQUEST - Sent from the BT17800 RADIUS client to the RADIUS server to request authentication and authorization	User-Name	The system login ID of the user
	User-Password	The user login password
	NAS-Identifier	The BT17800 management IP address

Table 9: RADIUS Packets (continued)

Packet type	Attribute	Description
ACCESS-ACCEPT - Sent from the RADIUS server to the BT17800 RADIUS client	Reply-Message	<p>Must be present</p> <p>Determines the group or privilege level of the user</p> <p>Contains one of superuser, provisioning, surveillance, or btiuser (deprecated)</p> <p>NOTE: If this user is configured in the local configuration database as well, then you must ensure that the group assignment for this user is identical between the RADIUS and the local configuration database.</p>
	Idle-Timeout	<p>Must be present</p> <p>Determines the inactivity timeout of the user</p> <p>Valid ranges are the following:</p> <ul style="list-style-type: none"> • 0: Disabled • 5 through 60 minutes

Table 10: TACACS+ Packets

Packet type	Attribute	Description
START - Sent from the BT17800 TACACS+ client to the TACACS+ server to request authentication	user	The system login ID of the user
REPLY (GETPASS) - Sent from the TACACS+ server to the BT17800 TACACS+ client asking for the user password		
CONTINUE - Sent from the BT17800 TACACS+ client to the TACACS+ server specifying the user password	password	The user login password
REPLY (PASS or FAIL) - Sent from the TACACS+ server to the BT17800 TACACS+ client allowing or rejecting the user		
REQUEST (authorization) - Sent from the BT17800 TACACS+ client to the TACACS+ server requesting the authorization level	user	The system login ID of the user

Table 10: TACACS+ Packets (continued)

Packet type	Attribute	Description
REPLY (authorization) - Sent from the TACACS+ server to the BT17800 TACACS+ client indicating the authorization level	priv-lvl or priv_lvl	<p>Must be present</p> <p>The privilege level for the user</p> <ul style="list-style-type: none"> • 0: surveillance • 1: btiuser (deprecated) • 2 through 14: provisioning • 15: superuser <p>NOTE: If this user is configured in the local configuration database as well, then you must ensure that the group assignment for this user is identical between the TACACS+ and the local configuration database.</p>

The RADIUS/TACACS+ authentication and authorization exchange occurs only at user login. TACACS+ command authorization is not supported.

Changes to user authentication or authorization settings on the external server (or the availability of the external server itself) do not affect the current login session.

RADIUS/TACACS+ authentication and authorization are not enabled by default.



NOTE: RADIUS and TACACS+ are mutually exclusive on the BT17800. If you configure a BT17800 to use RADIUS servers, you cannot also configure the same BT17800 to use TACACS+ servers, and vice versa.

Authentication and Authorization Sequence

If the BT17800 is configured to use one or more RADIUS/TACACS+ servers, RADIUS/TACACS+ authentication and authorization take precedence over local authentication and authorization. The BT17800 can be configured to use up to four RADIUS/TACACS+ servers.

Software Version	Authentication and Authorization Sequence
Releases lower than 4.1	<p>When a user tries to log in, the BT17800 attempts to authenticate the user with the first configured RADIUS server. If authentication is successful, the user is allowed to log in. If authentication is not successful for any reason (including bad credentials), the BT17800 times out and tries the same server again until the maximum number of allowed attempts with one server is reached. The BT17800 then attempts authentication with the next configured server in the list. If all configured RADIUS servers are exhausted, the BT17800 attempts to authenticate the user against the local configuration database.</p> <p>NOTE: Local authentication takes place if RADIUS authentication fails for any reason. It is therefore important that you properly maintain the local database even if you intend to use RADIUS authentication. If you fail to do so, you may run into situations where the RADIUS server rejects a user's credentials while local authentication accepts those same credentials.</p>

Software Version	Authentication and Authorization Sequence
Releases 4.1 and higher	<p>When a user tries to log in, the BTI7800 attempts to authenticate and authorize the user using the first configured RADIUS/TACACS+ server. If the first server does not respond within the timeout period:</p> <ul style="list-style-type: none"> • RADIUS: The BTI7800 tries the same server again until the maximum number of allowed attempts with one server is reached, at which time the BTI7800 attempts to connect with the next configured server in the list. • TACACS+: The BTI7800 attempts to connect with the next configured server in the list. <p>For both protocols, if authentication is successful, the user is allowed to log in. If authentication is not successful due to bad credentials, the user is denied access.</p> <p>If all configured RADIUS/TACACS+ servers are unreachable, the BTI7800 attempts to authenticate and authorize the user against the local configuration database.</p>

Configuring the RADIUS/TACACS+ Server

In order for the RADIUS/TACACS+ server to accept requests from each BTI7800 in the network, the RADIUS/TACACS+ server administrator must perform the following tasks:

Tasks	Required Configuration
Configure the RADIUS/TACACS+ server to accept requests from each BTI7800 implementing RADIUS/TACACS+ as a client.	<p>Specify the IP address (management IP address) of each BTI7800 using RADIUS/TACACS+.</p> <p>Specify the shared secret for each BTI7800. This must match the shared secret configured on the BTI7800 itself.</p>
Configure the RADIUS/TACACS+ server with the user accounts of all users requiring access to the BTI7800 network.	Specify the username, password, and group (privilege level) for all users on every BTI7800 using RADIUS/TACACS+.

The RADIUS/TACACS+ server can reside on the same server as the proNX Service Manager or on any other server. If you are using the RADIUS server that is prepackaged with the proNX Service Manager, you have the added benefit of being able to use the proNX Service Manager to add and remove users to and from the RADIUS database. For details, see the *proNX Service Manager Installation and Administration Guide* and the *proNX Service Manager User Guide*.

Refer to the applicable RADIUS/TACACS+ server user guide for any additional operating, configuration, or provisioning requirements.

Provisioning RADIUS Authentication and Authorization

Use this procedure to configure the BTI7800 to use RADIUS authentication and authorization.



NOTE: In releases lower than release 4.3, you must have **superuser** privileges to provision RADIUS authentication and authorization. In releases 4.3 and higher, you can provision RADIUS authentication and authorization with the **provisioning** privilege.

1. Specify the IP address of the RADIUS server.

For example:

```
bti7800(config)# system radius server 10.1.1.1 bti7800(config-server-10.1.1.1)#
```



NOTE: The default port is 1812. This must not be changed.

2. Specify the shared secret to use.

For example:

```
bti7800(config-server-10.1.1.1)# shared-secret <password>
bti7800(config-server-1.1.1.1)# exit
bti7800(config-system)#
```

3. Repeat 1 to 2 for each RADIUS server you want to use.

4. Optionally, configure the RADIUS system parameters.

- a. Specify the number of attempts that the BTI7800 makes to contact the same RADIUS server before the BTI7800 attempts to contact the next RADIUS server.

For example, to specify 5 attempts:

```
bti7800(config-system)# radius options attempts 5
```

- b. Specify the timeout value for the access request.

For example, to specify 10 seconds:

```
bti7800(config-system)# radius options timeout 10
```

5. Apply the provisioning.

```
bti7800(config-system)# commit
Commit complete.
```

The BTI7800 is now configured to use the configured RADIUS servers. Ensure any firewalls in the path are configured to allow RADIUS packets. Use the **ping** and **traceroute** commands to test the connectivity to each RADIUS server.

Provisioning TACACS+ Authentication and Authorization

Use this procedure to configure the BTI7800 to use TACACS+ authentication and authorization.



NOTE: In releases lower than release 4.3, you must have **superuser** privileges to provision TACACS+ authentication and authorization. In releases 4.3 and higher, you can provision TACACS+ authentication and authorization with the **provisioning** privilege.

1. Specify the IP address of the TACACS+ server.

For example:

```
bti7800(config)# system tacacs-plus server 10.1.1.1
bti7800(config-server-10.1.1.1)#
```

2. Specify the shared secret to use.

For example:

```
bti7800(config-server-10.1.1.1)# shared-secret <password>
```

3. Optionally, specify the authentication port to use.

For example:

```
bti7800(config-server-10.1.1.1)# authentication-port 49
bti7800(config-server-10.1.1.1)# exit
bti7800(config-system)#
```

4. Repeat 1 to 3 for each TACACS+ server you want to use.

5. Optionally, configure the TACACS+ system parameters.

For example, to set the timeout:

```
bti7800(config-system)# tacacs-plus options timeout 5
```

6. Apply the provisioning.

```
bti7800(config-system)# commit
Commit complete.
```

The BTI7800 is now configured to use the configured TACACS+ servers. Ensure any firewalls in the path are configured to allow TACACS+ packets. Use the **ping** and **traceroute** commands to test the connectivity to each TACACS+ server.

Release History Table

Release	Description
4.3	In releases 4.3 and higher, you can provision RADIUS authentication and authorization with the provisioning privilege.
4.3	In releases 4.3 and higher, you can provision TACACS+ authentication and authorization with the provisioning privilege.
4.1	TACACS+ is supported starting with release 4.1.
4.1	If authentication is not successful due to bad credentials, the user is denied access.

CHAPTER 4

System Provisioning

- [Configuring General Administrative Parameters on page 61](#)
- [Configuring the Shared Management IP Address and Subnet on page 62](#)
- [Configuring the Default Gateway on page 64](#)
- [Configuring the Individual Management IP Addresses on page 65](#)
- [Configuring DNS Servers on page 66](#)
- [Configuring NTP Servers and Time Zones on page 67](#)
- [Configuring Management Sources on page 69](#)
- [Configuring Auto-Provisioning on page 70](#)
- [Configuring Auto-Reprovisioning on page 71](#)
- [Configuring Auto-Warm-Boot on page 72](#)
- [Configuring AINS on page 73](#)
- [Setting the Autowizard on page 76](#)
- [Setting the Date and Time on page 77](#)
- [Configuring SNMP on page 78](#)

Configuring General Administrative Parameters

A BTI7800 system is a collection of one or more BTI7800 chassis managed by the same CMM active/standby pair. System provisioning refers to configuring system-level parameters on a BTI7800 system.

Use this procedure to configure general administrative parameters for the system. These parameters include the name and location of the system, and the contact information for the person administering the system. Set these parameters to descriptive strings that help identify the system to other operators.

1. Enter system configuration mode.

For example:

```
bti7800# config
Entering configuration mode terminal
bti7800(config)# system
bti7800(config-system)#
```

2. Specify the name of the system.

For example:

```
bti7800(config-system)# name NYC-47
bti7800(config-system)#
```

3. Specify the location of the system.

For example:

```
bti7800(config-system)# location manhattan
bti7800(config-system)#
```

4. Specify the contact information for the system.

For example:

```
bti7800(config-system)# contact "John Administrator 555-1234"
bti7800(config-system)#
```

5. Commit your changes.

```
bti7800(config-system)# commit
bti7800(config-system)#
```

6. Verify your changes by displaying the new settings.

For example (partial output only):

```
bti7800(config-system)# do show system

Name           : NYC-47
Contact        : John Administrator 555-1234
Location       : manhattan
```

Configuring the Shared Management IP Address and Subnet

Use this procedure to change the shared management IP address and subnet on the BTI7800. The shared management IP address and subnet are typically set up during commissioning.

Management of the BTI7800 is performed on the Chassis Management Modules, which run in an active/standby redundancy scheme. Both CMMs have management Ethernet interfaces for connecting to the management IP network, but only the active CMM performs management functions. You connect to the system through a virtual, shared management IP address, which is owned by the active CMM. If the active CMM goes down, the standby CMM becomes active and takes over ownership of the shared management IP address.

Additionally, each CMM has its own individual IP address that you can explicitly connect to if required. All three management IP addresses and the default gateway must reside on the same subnet.



NOTE: Changing the shared management IP address might cause your current management session to terminate.

1. Enter system configuration mode.

For example:

```
bti7800# config
Entering configuration mode terminal
bti7800(config)# system
bti7800(config-system)#
```

2. Delete the individual management IP addresses if configured.

If an individual management IP address has been configured, then you should delete it. This ensures that there is no conflict between the individual management IP addresses and the new subnet. For example:

```
bti7800(config-system)# no controller-1 static-address
bti7800(config-system)# no controller-2 static-address
```

3. Delete the default gateway if configured.

If a default gateway has been configured, then you should delete it. This ensures that there is no conflict between the default gateway and the new subnet. For example:

```
bti7800(config-system)# no gateway-address
```

4. Set the shared management IP address and subnet.

The subnet is specified in CIDR format.

For example:

```
bti7800(config-system)# mgmt-address 10.1.220.104/10
```

5. Commit your changes.

```
bti7800(config-system)# commit
```

Commit complete.



NOTE: If you change the IP address that you are using for the current management session, the current session will terminate, and you will need to reconnect using the new IP address. If you change the IP subnet as well, then you might need to reconfigure your management network before you can reconnect.

6. Verify your settings by displaying the new settings.

For example:

```
bti7800# show system mgmt-interface | inc MgmtAddress
MgmtAddress: 10.1.220.104/10
```

To configure the default gateway, see [“Configuring the Default Gateway” on page 64](#). To configure the optional individual management IP addresses, see [“Configuring the Individual Management IP Addresses” on page 65](#).

Configuring the Default Gateway

Use this procedure to configure the default gateway on the BTI7800.

Prerequisites:

- The shared management IP address (and subnet) must be set up.

The default gateway is typically set up during commissioning.



NOTE: The default gateway, the shared management IP address, and the individual management IP addresses must all reside on the same subnet.



NOTE: Changing the default gateway will affect the routing of packets. Setting the default gateway incorrectly might cause originating packets (such as SNMP traps) to be dropped.

1. Enter system configuration mode.

For example:

```
bti7800# config
Entering configuration mode terminal
bti7800(config)# system
bti7800(config-system)#
```

2. Set the default gateway.

For example:

```
bti7800(config-system)# gateway-address 10.1.220.1
```

3. Commit your changes.

```
bti7800(config-system)# commit
Commit complete.
```

Configuring the Individual Management IP Addresses

Use this procedure to configure the individual management IP address on a CMM. This is optional. You do not normally need to connect to the individual management IP address. Use of the individual management IP address is beyond the scope of this document.

Prerequisites:

- The shared management IP address (and subnet) and the default gateway must be set up.

Each CMM has its own IP address that you can explicitly connect to if required. These individual management IP addresses are typically set up during commissioning.



NOTE: The individual management IP addresses, the shared management IP address, and the default gateway must all reside on the same subnet.

1. Enter system configuration mode.

For example:

```
bti7800# config
Entering configuration mode terminal
bti7800(config)# system
bti7800(config-system)#
```

2. Set the individual management IP address for the CMM in slot A.

All management IP addresses must reside on the same subnet.

For example:

```
bti7800(config-system)# controller-1 static-address 10.1.220.189
```

3. Set the individual management IP address for the CMM in slot B.

All management IP addresses must reside on the same subnet.

For example:

```
bti7800(config-system)# controller-2 static-address 10.1.220.190
```

4. Commit your changes.

```
bti7800(config-system)# commit
Commit complete.
bti7800(config-system)# end
bti7800#
```

5. Verify your settings by displaying the new settings.

For example:

```
bti7800# show system mgmt-interface
```

```
MgmtAddress: 10.1.220.104/10
```

Name	IP	Netmask	MAC Address	Duplex	Speed
eth0-cmm:1/A	192.168.17.1	255.255.255.0	00:14:d0:00:69:04	Unknown	Unkn
eth1-cmm:1/A	10.1.220.189	255.192.0.0	00:14:d0:00:69:05	Full	100
eth0-cmm:1/B	192.168.17.1	255.255.255.0	00:14:d0:50:5a:b3	Unknown	Unkn
eth1-cmm:1/B	10.1.220.190	255.192.0.0	00:14:d0:50:5a:b4	Full	100

Name	Baud rate	Parity	Stop Bits	Flow Control
ttyS0-cmm:1/A	115200	no	1	no hardware
ttyS0-cmm:1/B	115200	no	1	no hardware

Configuring DNS Servers

Use this procedure to specify the DNS servers that this system will use. By specifying a valid DNS server, you will be able to enter hostnames in commands that accept hostnames as input.

1. Enter system configuration mode.

For example:

```
bti7800# config
Entering configuration mode terminal
bti7800(config)# system
bti7800(config-system)#
```

2. Add the list of DNS servers that you want the system to use.

For example:

```
bti7800(config-system)# dns server 172.25.0.61 10.10.1.2
bti7800(config-system)#
```

3. Commit your changes.

```
bti7800(config-system)# commit
bti7800(config-system)#
```

4. Verify your settings by displaying the new settings.

For example (partial output only):

```
bti7800(config-system)# do show system
DNS                        : 172.25.0.61, 10.10.1.2
```

Configuring NTP Servers and Time Zones

Use this procedure to specify the NTP servers that the system will use and to set the time zone.



NOTE: We recommend that you always use NTP servers for the system time. If you are unable to use NTP servers, you can set the time manually using the procedure in [“Setting the Date and Time” on page 77](#).



NOTE: If the NTP server provides a reference time that is different from the local system time, the local system clock is changed gradually to match the reference clock. For larger time differences, the local system clock might take an hour or more to finish synchronizing with the reference clock. For even larger time differences, the local system clock might not synchronize at all. This is standard NTP behavior.



NOTE: Changing the time affects PMs. For more information, see [“Effect of a Time Change on PMs” on page 216](#).

1. Enter system configuration mode.

For example:

```
bti7800# config
Entering configuration mode terminal
bti7800(config)# system
bti7800(config-system)#
```

2. Add the list of NTP servers that you want the system to use.

For example:

```
bti7800(config-system)# ntp server 10.1.1.1 10.2.2.2
```

```
bti7800(config-system)#
```

The NTP servers are placed on the server list in the order that you add them.

3. Set the time zone.

For example:

```
bti7800(config-system)# clock timezone-location America/New_York
bti7800(config-system)#
```

4. Commit your changes.

```
bti7800(config-system)# commit
bti7800(config-system)# exit
bti7800#
```

5. Warm reload the CMMs for the time change to take effect.

- a. Determine which CMM is active and which CMM is standby.

For example:

```
bti7800# show system | include Controller
Active Controller      : cmm:1/A
Backup Controller     : cmm:1/B
```

- b. Warm reload the standby/backup CMM.

For example:

```
bti7800# system reload warm cmm:1/B
```

Wait until the standby CMM finishes reloading before proceeding to the next step. The standby CMM is finished reloading when the HA Status is In Sync, for example:

```
bti7800# show system | include HA
HA Status              : In Sync
```

- c. Warm reload the active CMM.

For example:

```
bti7800# system reload warm cmm:1/A
```

Your CLI session terminates as the active CMM reloads.

- d. Once the CMM finishes reloading, log back in to the CLI and verify your settings by displaying the new settings. This might take several minutes.

For example:

```
bti7800# show system ntp
```

```

remote      refid      st t when poll reach  delay  offset  jitter
=====
10.1.1.1    10.1.1.3    2 u  16   64   1  57.721  2.958  0.000
10.2.2.2    10.2.2.5    2 u  15   64   1  38.271 -4.293  0.000

bti7800# show system clock
current-datetime      : 2015-01-23T16:44:18-05:00
boot-datetime         : 2015-01-22T23:58:05-05:00
uptime               : 0 days,16:46:13
timezone              : America/New_York

```



NOTE: The T delineates the date from the time. The time shown is the local time in the specified timezone. The timezone is indicated by the UTC offset, which in the above example is UTC-05:00.

Configuring Management Sources

Use this procedure to specify the IP addresses that are allowed to gain management access to the system.



NOTE: This feature is supported starting with release 2.1.1.



NOTE: If no management sources are configured, all management sources are allowed.

If a connection request arrives on the CMM management Ethernet port (eth1) or inband on the optical network, and if the request is destined for any of the protocol ports in the following list, the system validates the source IP address in the connection request with the list of allowed management sources. If the source IP address in the connection request is not in the allowed management source list, the connection is rejected.

- SSH (port 22)
- CLI (port 2024)
- NETCONF (port 2022)
- SNMP (port 161)



NOTE: Management source verification does not take place if the connection request is destined for a protocol port not in the above list.

This command only governs new connection requests. Existing established management connections are not affected. Connection requests on the craft Ethernet port (eth0) are also not affected. Any source can connect to the craft Ethernet port.

1. Enter system configuration mode.

For example:

```
bti7800# config Entering configuration mode terminal
bti7800(config)# system
bti7800(config-system)#
```

2. Add the list of management sources that you want to allow.

For example:

```
bti7800(config-system)# mgmt-sources 10.1.1.5/32 192.168.10.0/24
bti7800(config-system)#
```

3. Commit your changes.

```
bti7800(config-system)# commit
bti7800(config-system)#
```

4. Verify your settings by displaying the new settings.

For example (partial output only):

```
bti7800(config-system)# do show system
Management Sources      : 10.1.1.5/32, 192.168.10.0/24
```

Release History Table

Release	Description
2.1.1	Use this procedure to specify the IP addresses that are allowed to gain management access to the system.

Configuring Auto-Provisioning

Use this procedure to configure auto-provisioning.

If auto-provisioning is enabled, the system automatically discovers and provisions newly inserted equipment. For more information, see [“Auto-Provisioning of BTI7800 Equipment” on page 25](#).

1. Enter configuration mode.

For example:

```
bti7800# config
```

```
bti7800(config)#
```

2. Specify whether auto-provisioning is enabled or disabled.

If auto-provisioning is enabled, the system automatically provisions newly inserted equipment for you. If auto-provisioning is disabled, you must manually provision newly inserted equipment.

For example, to enable auto-provisioning:

```
bti7800(config-system)# auto-prov true
bti7800(config-system)#
```

3. Commit your changes.

```
bti7800(config-system)# commit
bti7800(config-system)#
```

Configuring Auto-Reprovisioning

Use this procedure to configure auto-reprovisioning.

Auto-reprovisioning enables you to replace one module with a different module without requiring you to perform manual reconfiguration. This is currently supported for certain UFM modules. See [“Replacing a UFM3 or a UFM4” on page 91](#).

1. Enter configuration mode.

For example:

```
bti7800# config
bti7800(config)#
```

2. Specify whether auto-reprovisioning is enabled or disabled.

If auto-reprovisioning is enabled, the system automatically unprovisions the module being replaced, and provisions the newly inserted module. If auto-reprovisioning is disabled, you must manually unprovision the module being replaced, and manually provision the newly inserted module.

For example, to enable auto-reprovisioning:

```
bti7800(config-system)# auto-reprov true
bti7800(config-system)#
```

3. Commit your changes.

```
bti7800(config-system)# commit
bti7800(config-system)#
```

Configuring Auto-Warm-Boot

Use this procedure to configure auto-warm-boot. It is recommended that you leave this setting at its default value.

When auto-warm-boot is enabled, the active CMM automatically warm reloads a service module and/or a standby CMM up to 3 times if the service module and/or standby CMM is unresponsive.

Warm reloading modules does not affect traffic.

1. Enter configuration mode for the system parameters.

```
bt17800# config
bt17800(config)# system
bt17800(config-system)#
```

2. Specify whether auto-warm-boot is enabled or disabled.

- a. To enable auto-warm-boot for all modules (service modules and standby CMM):

```
bt17800(config-system)# no auto-warm-boot disabled
```

- b. To disable auto-warm-boot for all modules (service modules and standby CMM):

```
bt17800(config-system)# auto-warm-boot disabled ALL
```

- c. To disable auto-warm-boot for service modules:

```
bt17800(config-system)# auto-warm-boot disabled PLD
```

- d. To disable auto-warm-boot for CMMs:

```
bt17800(config-system)# auto-warm-boot disabled CMM
```

- e. Use a combination of commands to achieve other outcomes.

For example, to enable auto-warm-boot for service modules only:

```
bt17800(config-system)# no auto-warm-boot disabled
bt17800(config-system)# auto-warm-boot disabled CMM
```

3. Commit your changes.

```
bt17800(config-system)# commit
Commit complete.
```

Configuring AINS

Auto-In-Service (AINS) temporarily suppresses alarm reporting against a managed entity for first-time provisioning or during a maintenance interval, which eliminates managing transitory faults that occur while a service or system component is being set up.

You can configure system-wide and interface level AINS support.

System-wide AINS Support

If you do not configure AINS settings when provisioning a new interface, the system-wide AINS default values are applied to that interface. The following table lists the system-wide AINS commands:

Parameter	Description	Range	Default Value
default-ains	Enables or disables AINS on new interfaces.	true: Enable AINS false: Disable AINS	false
default-ains-timer	Sets the AINS countdown duration on new interfaces, in hours and minutes, in the format: HH:MM.	00:00 to 99:59	08:00

Interface-level AINS Support

Interface-level AINS values are configured on a specified interface. The following table lists the interface-level AINS commands:

Parameter	Description	Range	Default Value
ains	Enables or disables AINS on a specified interface.	true: Enable AINS false: Disable AINS	false
ains-timer	Sets the AINS countdown duration on the interface, in hours and minutes, in the format: HH:MM.	00:00 to 99:59	08:00

For more information about configuring interfaces, refer to the *BT17800 Series Command Line Reference Guide*.

Guidelines

AINS can be set to true for any interface regardless of the setting of any other attribute, including the administrative status of the interface.

AINS settings persist in the database and survive system restarts.

When an interface operational state changes to "down", the current countdown timer is cancelled and the countdown timer reinitializes to the AINS timer setting when the operational status of the interface returns to "up".

When AINS is enabled for an interface, there is no alarm reporting for that interface. Raise or clear traps are not generated for faults on the interface, and there are no entries in the interface alarm list—**show alarms**, in addition, no threshold crossing alerts are generated. All faults raised against the interface can be viewed in the condition list—**show conditions**.

AINS enabled on an interface automatically transitions to disabled when the following occurs:

- No fault is raised against the interface.
- The operational status of the interface is "up".
- The interface remains fault free, with operational status "up" for a duration equal to the AINS countdown duration setting.

Once AINS automatically transitions to disabled, any fault subsequently raised against the interface is reported as an alarm. To satisfy the conditions for automatically transitioning from enabled to disabled, a fault-free, operationally up condition must persist for the duration equal to the interface AINS timer setting. When an interface with AINS enabled enters this state, the persistence interval begins and the remaining duration in the persistence interval is tracked with a countdown timer for the interface. If a fault is raised or the operational status changes to any value other than "up", the current countdown timer is cancelled and reinitializes to the AINS timer setting when the interface returns to fault-free, operationally up status.

Since the automatic transition to disabled depends on the operational status of the interface being "up", the transition out of AINS does not occur if:

- The interface is administratively disabled.
- Supporting equipment or other supporting interface is not operationally "up".

AINS can be configured on an interface at any time. If a countdown timer is active for an interface, setting the AINS timer on that interface reinitializes the current active timer to the new timer setting.

AINS Status Monitoring

Each interface supports a new read-only attribute named **Ains Countdown Timer**, which is displayed in the **show interface** output. This attribute displays only if the AINS countdown timer is active. If an interface with AINS enabled is fault free and operationally up, **Ains Countdown Timer** displays the remaining time in the persistence interval in hours and minutes, for example 07:48 for 7 hours, 48 minutes.

Configuration Examples

Following are examples of AINS system-wide and interface configuration and monitoring:

Enabling AINS System-wide

```
bti7800(config)# show running-configuration system
```

```
system
 location UNKNOWN
 ains
  default-ains      false
  default-ains-timer 08:00
!
```

```
bti7800(config)# system ains default-ains true
bti7800(config)# system ains default-ains-timer 04:00
bti7800(config-system)# commit
Commit complete.
bti7800(config-system)#
```

Enabling AINS on an Interface

```
bti7800(config)# interface 10ge:1/3/1/1 type ethernetCsmacd
bti7800(config-interface-10ge:1/3/1/1)# commit
Commit complete.
bti7800(config-interface-10ge:1/3/1/1)# show full-configuration
interface 10ge:1/3/1/1
 type      ethernetCsmacd
 enabled
 ains      true
 ains-timer 04:00
 laser-enabled true
 fpsd      true
 loopback-mode noLoopback
!
bti7800(config-interface-10ge:1/3/1/1)#
```

Provisioning the AINS timer on an Interface

This example configures the timer for 2 hours, 30 minutes:

```
bti7800(config)# interface 10ge:1/3/1/2 type ethernetCsmacd ains-timer 02:30
bti7800(config-interface-10ge:1/3/1/2)# commit
Commit complete.
bti7800(config-interface-10ge:1/3/1/2)# show full-configuration
interface 10ge:1/3/1/2
 type      ethernetCsmacd
 enabled
 ains      true
 ains-timer 02:30
 laser-enabled true
 fpsd      true
 loopback-mode noLoopback
!
bti7800(config-interface-10ge:1/3/1/2)#
```

Checking the Interface Status: Operationally Down

Note: Only a portion of the whole interface status is displayed.

```
bt17800(config)# do show interface 10ge:1/3/1/2
```

```
Name                : 10ge:1/3/1/2
Description          :
Type                 : ethernet
Interface Index      : 2
Admin State          : enabled
Operational State    : LowerLayerDown
AINS                 : enabled
AINS Timer           : 02:30
Laser Enabled        : enabled
Laser Status         :
--More--
```

Checking the Interface Status: Operationally Up

```
bt17800(config)# do show interface 10ge:1/3/1/2
```

```
Name                : 10ge:1/3/1/2
Description          :
Type                 : ethernet
Interface Index      : 2
Admin State          : enabled
Operational State    : up
AINS                 : enabled
AINS Timer           : 02:30
AINS Countdown       : 01:47
Laser Enabled        : enabled
Laser Status         :
--More--
```

Setting the Autowizard

Use this procedure to override the configured autowizard setting for the system. If you enable autowizard, the CLI prompts you to enter mandatory parameters when configuring a component. This procedure is executed in operational mode.

When you reboot the system, the autowizard setting changes back to the configured setting. See [“Configuring User Session Parameters” on page 51](#).



NOTE: If you intend to use the running-config output as input to the CLI, you should disable autowizard.

1. Configure the autowizard setting.

- a. To enable autowizard:

```
bti7800# autowizard true
```

- b. To disable autowizard:

```
bti7800# autowizard false
```

Setting the Date and Time

Use this procedure to set the system date and time when NTP servers are not available. This procedure is executed in operational mode.



NOTE: Changing the time affects PMs. For more information, see [“Effect of a Time Change on PMs” on page 216](#).

1. Set the date and time.

For example:

```
bti7800# system clock set-date-time 2017-07-26T13:49:46
```

NOTE: If the system is using NTP, date and time would be overridden by NTP. Proceed? [no,yes] yes
bti7800#

2. Warm reload the CMMs for the time change to take effect.

- a. Determine which CMM is active and which CMM is standby.

For example:

```
bti7800# show system | include Controller
```

```
Active Controller      : cmm:1/A
Backup Controller     : cmm:1/B
```

- b. Warm reload the standby/backup CMM.

For example:

```
bti7800# system reload warm cmm:1/B
```

Wait until the standby CMM finishes reloading before proceeding to the next step. The standby CMM is finished reloading when the HA Status is In Sync, for example:

```
bti7800# show system | include HA
```

```
HA Status              : In Sync
```

- c. Warm reload the active CMM.

For example:

```
bti7800# system reload warm cmm:1/A
```

Your CLI session terminates as the active CMM reloads.

- d. Once the CMM finishes reloading, log back in to the CLI and verify your settings by displaying the new settings. This might take several minutes.

For example:

```
bti7800# show system clock | include current
current-datetime      : 2017-07-26T13:53:50-04:00
```



NOTE: The T delineates the date from the time. The time shown is the local time in the specified timezone. The timezone is indicated by the UTC offset, which in the above example is UTC-04:00.

Configuring SNMP

Use this procedure to configure SNMP community strings and trap receivers.

1. Configure the community strings.



NOTE: In releases lower than release 4.3, you must have superuser privileges to provision SNMP community strings. In releases 4.3 and higher, you can provision SNMP community strings with the provisioning privilege.

- a. Configure the read-only community string.

For example:

```
bti7800(config)# snmp-server community R0 password
bti7800(config-community-R0)# commit
Commit complete.
bti7800(config-community-R0)# exit
bti7800(config)#
```

- b. Configure the read-write community string.

For example:

```
bti7800(config)# snmp-server community RW password
bti7800(config-community-RW)# commit
Commit complete.
bti7800(config-community-RW)# exit
bti7800(config)#
```

- c. Display the new configuration.

For example:

```
bti7800(config)# do show running-config snmp-server community

snmp-server community RW
password
!
snmp-server community RO
password
!
```

2. Configure the trap receiver.

- a. Specify the IP address of the trap receiver.

For example:

```
bti7800(config)# snmp-server host 10.1.1.1
bti7800(config-host-10.1.1.1)# commit
Commit complete.
bti7800(config-host-10.1.1.1)# exit
bti7800(config)#
```

- b. Repeat until you have configured all trap receivers.

- c. Display the trap receivers.

For example:

```
bti7800(config)# do show snmp host
```

Target-Name	IP-Address	Port	TimeOut-Value	Retry-Count	Tag-List
10.1.1.1 v2	10.1.1.1	162	1500	3	std_v2_t
10.2.2.2 v2	10.2.2.2	162	1500	3	std_v2_t

Release History Table

Release	Description
4.3	In releases 4.3 and higher, you can provision SNMP community strings with the provisioning privilege.

CHAPTER 5

Module Provisioning

- [Overview on page 81](#)
- [Universal Forwarding Modules on page 81](#)
- [Optical Modules on page 96](#)
- [Enabling and Disabling Modules on page 98](#)
- [Module Reload Times on page 99](#)

Overview

This section provides information about module provisioning that is not specific to any application. In general, this is the provisioning that is related to the equipment branch of the provisioning tree, but it can include other parts of the tree as well.

If you enable auto-provisioning (see [“Auto-Provisioning of BT17800 Equipment” on page 25](#)), you will not need to use many of the procedures in this chapter because the system auto-provisions the equipment for you when you insert the module into the chassis.

However, if you want to pre-provision equipment (see [“Pre-Provisioning of BT17800 Components” on page 27](#)) or if you do not enable auto-provisioning, then follow the procedures contained in this section.



NOTE: If auto-provisioning can replace a procedure, then it is clearly indicated at the beginning of the procedure.

Universal Forwarding Modules

The Universal Forwarding Module (UFM) is a service module that can be configured for transport services such as transponding and muxponding. It is available in different types with different capabilities, as follows:



NOTE: The UFM6 is supported starting with release 4.1.

Table 11: UFM Types

	UFM3	UFM4	UFM6
Name	Universal Forwarding Module	Universal Forwarding Module with Integrated 100G Coherent MSA XCVR	Universal Forwarding Module with Integrated 400G Coherent MSA XCVR
PEC	BT8A78UFM3	BT8A78UFM4	BT8A78UFM6-I02
Integrated 100G Coherent MSA XCVR	N	Y	N
Integrated 400G Coherent MSA XCVR	N	N	Y
Number of BIC slots	2	1	0
Transport services	Y	Y	Y
BT17801	Y	Y	Y
BT17802	Y	Y	Y
BT17814	Y	Y	Y

A UFM contains zero, one, or two slots for BTI Interface Cards. BTI Interface Cards (BICs) are modules that hold pluggable transceivers. Pluggable transceivers are inserted into a BIC, which in turn is inserted into a BIC slot of a supporting UFM. There are different types of BICs depending on the pluggables required. By housing different BICs, the same UFM can hold different combinations of 10-Gbps and 100-Gbps interfaces.

- [UFM Location Identifiers on page 82](#)
- [Provisioning UFM Equipment on page 87](#)
- [Replacing a UFM3 or a UFM4 on page 91](#)
- [Configuring a Loopback on a UFM Interface on page 95](#)

UFM Location Identifiers

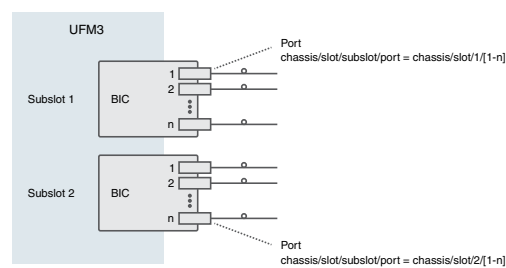
Each addressable component in a BT17800 system consists of a component name and a location identifier. Together, they uniquely identify components in a system. All location identifiers begin with a chassis/slot combination, which specifies the chassis and slot that the component resides in. The location can then be further qualified depending on the type of component and module being specified.

For UFM3s, the location identifiers differ depending on the UFM type. All UFM types have two subslots or groups. A subslot can represent a physical subslot or a fixed grouping of ports.

- [UFM3 Location Identifiers on page 83](#)
- [UFM4 Location Identifiers on page 84](#)
- [UFM6 Location Identifiers on page 85](#)

UFM3 Location Identifiers

The UFM3 consists of two subslots for BICs.



Each BIC is addressed using the **chassis/slot/subslot** location identifier format. For example:

- **bic:1/5/1** represents the BIC in subslot 1 of the UFM in chassis 1 slot 5.

Different BICs hold different types and numbers of transceivers. Each transceiver is addressed using the **chassis/slot/subslot/port** location identifier format. For example:



NOTE: The figure above is for illustration only and is not intended to depict any particular BIC type.

- **sfpPlus:1/5/1/8** represents an SFP+ transceiver on port 8 of the first BIC.
- **cfp:1/5/2/1** represents a CFP transceiver on port 1 of the second BIC.

Associated with each transceiver port is an interface. This interface is addressed using the **chassis/slot/subslot/port** location identifier format. For example:

- **otu2:1/5/1/8** (**otu2e:1/5/1/8**) represents an OTU2 (OTU2e) interface on the above SFP+ transceiver.
- **otu4:1/5/2/1** represents an OTU4 interface on the above CFP transceiver.

Within each OTU2 (OTU2e) is an ODU2 (ODU2e), which is addressed using the **chassis/slot/subslot/port** location identifier format. For example:

- **odu2:1/5/1/8 (odu2e:1/5/1/8)** represents the ODU2 (ODU2e) interface contained within the above OTU2 (OTU2e).

Similarly, within each OTU4 is an ODU4, which is addressed using the **chassis/slot/subslot/port** location identifier format. For example:

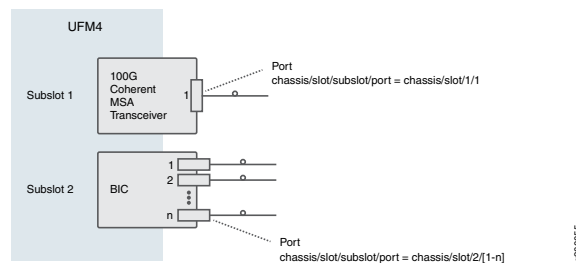
- **odu4:1/5/2/1** represents the ODU4 interface contained within the above OTU4.

If the ODU4 is configured for multiplexing, the multiplexed ODU2 (ODU2e) subinterfaces are addressed using the **chassis/slot/subslot/port.subinterface** location identifier format. For example:

- **odu2:1/5/2/1.5 (odu2e:1/5/2/1.5)** represents the fifth ODU2 (ODU2e) subinterface multiplexed into the above ODU4/OTU4.

UFM4 Location Identifiers

The UFM4 consists of an integrated 100G Coherent MSA XCVR and a subslot for a single BIC. The 100G Coherent MSA XCVR is conceptually located in subslot 1 and the BIC is located in subslot 2.



The 100G Coherent MSA XCVR is addressed using the **chassis/slot/subslot/port** location identifier format. For example:

- **msa:1/5/1/1** represents the 100G Coherent MSA XCVR on a UFM in chassis 1 slot 5 subslot 1 port 1. This transceiver is always in subslot 1 port 1. It consists of a single 100-Gbps port.

Associated with the 100G Coherent MSA XCVR port is a single 100-Gbps interface. This interface is addressed using the **chassis/slot/subslot/port** location identifier format. For example:

- **otu4:1/5/1/1** represents the OTU4 interface for the above transceiver.

Within the OTU4 is an ODU4, which is addressed using the **chassis/slot/subslot/port** location identifier format. For example:

- **odu4:1/5/1/1** represents the ODU4 interface contained within the above OTU4.

If the ODU4 is configured for multiplexing, the multiplexed ODU2 subinterfaces are addressed using the **chassis/slot/subslot/port.subinterface** location identifier format. For example:

- **odu2:1/5/1/1.5** represents the fifth ODU2 subinterface multiplexed into the above ODU4/OTU4.

The BIC in this UFM is addressed using the **chassis/slot/subslot** location identifier format. For example:

- **bic:1/5/2** represents the BIC in the above UFM. The BIC in this UFM is always in subslot 2.

Different BICs hold different types and numbers of transceivers. Each transceiver is addressed using the **chassis/slot/subslot/port** location identifier format. For example:

- **sfpPlus:1/5/2/8** represents an SFP+ transceiver on port 8 of the above BIC.

Associated with each transceiver port is an interface. This interface is addressed using the **chassis/slot/subslot/port** location identifier format. For example:

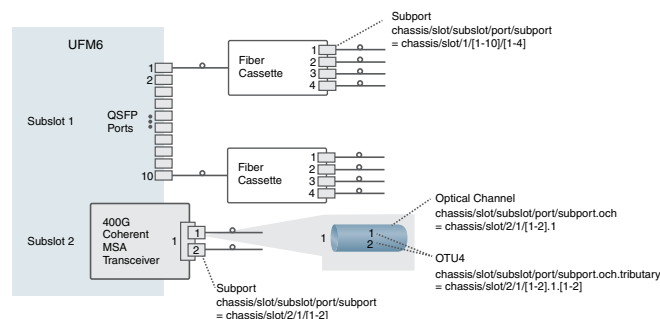
- **10ge:1/5/2/8** represents a 10-Gigabit Ethernet interface on the above SFP+ transceiver.

UFM6 Location Identifiers

The UFM6 consists of ten QSFP (six QSFP+ ports and four dual-mode QSFP+/QSFP28) ports and one integrated 400G Coherent MSA XCVR. The ten QSFP ports are located conceptually in subslot 1, and the 400G Coherent MSA XCVR is located conceptually in subslot 2. These are labeled **Port Group 1** and **Port Group 2** on the UFM faceplate.



NOTE: The six QSFP+ ports are client ports 3, 4, 5, 8, 9, and 10. The four dual-mode QSFP+/QSFP28 ports are client ports 1, 2, 6, and 7.



Each QSFP+ or QSFP28 transceiver is addressed using the **chassis/slot/subslot/port** location identifier format. For example:

- **qsfp:1/5/1/8** represents a QSFP+ transceiver in a UFM6 in chassis 1 slot 5 subslot 1 port 8.
- **qsfp28:1/5/1/1** represents a QSFP28 transceiver in a UFM6 in chassis 1 slot 5 subslot 1 port 1.

The QSFP+ transceivers supported for UFM6 are available in two different types. The first type carries four individual fiber pairs, with each fiber pair attached to a separate internal 10-Gbps interface. Each 10-Gbps interface is addressed using the **chassis/slot/subslot/port/subport** location identifier format. For example:

- **10ge:1/5/1/8/3** represents a 10-Gigabit Ethernet interface attached to the third fiber pair of the above QSFP+ transceiver.

The second type, QSFP+ 40GE, also carries four individual fiber pairs, but the signals on the fibers are combined to terminate on a single internal 40-Gbps interface. Each 40-Gbps interface is addressed using the **chassis/slot/subslot/port** location identifier format. For example:

- **40ge:1/5/1/2** represents a 40-Gigabit Ethernet interface on the above QSFP+ 40GE transceiver.

The QSFP28 transceiver supports one 100-Gbps interface, which is addressed using the **chassis/slot/subslot/port** location identifier format. For example:

- **100ge:1/5/1/1** represents a 100-Gigabit Ethernet interface on the above QSFP28 transceiver.

The 400G Coherent MSA XCVR is addressed using the **chassis/slot/subslot/port** location identifier format. For example:

- **msa400:1/5/2/1** represents the 400G Coherent MSA XCVR in a UFM6 in chassis 1 slot 5 subslot 2 port 1. This transceiver consists of a single internal 400-Gbps port.

The internal 400-Gbps port in the 400G Coherent MSA XCVR is divided into the two 200-Gbps ports that are visible on the faceplate, with each 200-Gbps port carrying a single optical channel. The optical channel represents the optical signal and contains the settings and attributes that govern the constituent 100-Gbps signals. The optical channel is represented as an interface. It is addressed using the **chassis/slot/subslot/port/subport.och** location identifier format. For example:

- **och:1/5/2/1/2.1** represents the optical channel interface on the second 200-Gbps subport of the above transceiver.

Depending on the modulation chosen, each optical channel can contain one or two 100-Gbps signals. Each 100-Gbps signal is attached to a logical 100-Gbps (OTU4) interface. The 100-Gbps interface is addressed using the **chassis/slot/subslot/port/subport.och.tributary** location identifier format. For example:

- **otu4:1/5/2/1/2.1.2** represents the second 100-Gbps interface in the above optical channel.



NOTE: If the optical channel modulation is configured to allow only one 100-Gbps signal, that signal must be on the first 100-Gbps interface (for example, **otu4:1/5/2/1/2.1.1**). If the modulation is configured to allow two 100-Gbps signals, then you can use either of the two 100-Gbps interfaces (for example, **otu4:1/5/2/1/2.1.1** or **otu4:1/5/2/1/2.1.2**) even if you are only configuring one 100-Gbps interface.

Within the OTU4 is an ODU4, which is addressed using the **chassis/slot/subslot/port/subport.och.tributary** location identifier format. For example:

- **odu4:1/5/2/1/2.1.2** represents the ODU4 interface contained within the above OTU4.

If the ODU4 is configured for multiplexing 10-Gbps subinterfaces, the multiplexed ODU2 (ODU2e) subinterfaces are addressed using the **chassis/slot/subslot/port/subport.och.tributary.subinterface** location identifier format. For example:

- **odu2:1/5/2/1/2.1.2.5** (**odu2e:1/5/2/1/2.1.2.5**) represents the fifth ODU2 (ODU2e) subinterface multiplexed into the above ODU4/OTU4.

If the ODU4 is configured for multiplexing 40-Gbps subinterfaces, the multiplexed ODU3 subinterfaces are addressed using the **chassis/slot/subslot/port/subport.och.tributary.subinterface** location identifier format. For example:

- **odu3:1/5/2/1/2.1.2.2** represents the second ODU3 subinterface multiplexed into the above ODU4/OTU4.

Provisioning UFM Equipment

Provisioning UFM equipment consists of provisioning the UFM itself, the BTI Interface Cards (BICs) if applicable, and the transceivers.

- [Provisioning a UFM on page 87](#)
- [Provisioning a BTI Interface Card \(BIC\) on page 88](#)
- [Provisioning a Transceiver on page 89](#)

Provisioning a UFM

Use this procedure to add a UFM to a chassis.

If auto-provisioning is enabled and you do not want to pre-provision, then you can skip this procedure because the system automatically provisions the UFM when you insert the UFM into the chassis.

The type of UFM you are adding is specified by the **ufm-type** attribute, as shown in the following table:

UFM	ufm-type
UFM3	dual-bic-non-switching
UFM4	msa-non-switching
UFM6	msa400-10g-100g-client



NOTE: UFM types not listed above have been deprecated.

1. Enter configuration mode.

```
bt17800# config
bt17800(config)#
```

2. Add the UFM and specify the type of UFM you are adding.

For example, the following adds a UFM4 to chassis 1 slot 2:

```
bt17800(config)# equipment chassis:1 module ufm:1/2
Value for 'ufm-type'
[dual-bic-non-switching,dual-bic-switching,msa-non-switching,msa-switching,msa400-10g-100g-client]:
msa-non-switching
bt17800(config-module-ufm:1/2)#
```

3. Apply the changes.

```
bt17800(config-module-ufm:1/2)# commit
Commit complete.
```

Provisioning a BTI Interface Card (BIC)

Use this procedure to add a BIC.

If auto-provisioning is enabled and you do not want to pre-provision, then you can skip this procedure because the system automatically provisions the BIC when the system detects the presence of the BIC. The system detects the presence of the BIC in these situations:

- The BIC is inserted into a UFM that is already installed in the chassis.
- The BIC is inserted into an uninstalled UFM that is then installed into the chassis.

The type of BIC you are adding is specified by the **bic-type** attribute, as shown in the following table:

BIC	bic-type
12x SFP+ BIC	sfp-bic
1x CFP BIC	cfp-bic

1. Enter configuration mode.

```
bti7800# config
bti7800(config)#
```

2. Add the BIC to the desired BIC slot in the UFM.

The following example adds a 1x CFP BIC to BIC slot 2 in the UFM in slot 7:

```
bti7800(config)# equipment chassis:1 module ufm:1/7 bic bic:1/7/2
Value for 'bic-type' [cfp-bic,qsfp-bic,sfp-bic]: cfp-bic
bti7800(config-bic-bic:1/7/2)#
```

3. Apply the configuration changes.

For example:

```
bti7800(config-bic-bic:1/7/2)# commit
Commit complete.
```

Provisioning a Transceiver

Use this procedure to add a transceiver. A transceiver component can be added to a BIC or to a UFM with fixed ports or to a UFM with an integrated transceiver.

If auto-provisioning is enabled and you do not want to pre-provision, then you can skip this procedure because the system automatically provisions the transceiver when the system detects the presence of the transceiver. The system detects the presence of the transceiver in these situations:

- The transceiver is inserted into a BIC that is already installed in the chassis.
- The transceiver is inserted into an uninstalled BIC that is then installed into a UFM in the chassis.
- The transceiver is inserted into an uninstalled BIC that is then inserted into an uninstalled UFM that is then installed in the chassis.
- The transceiver is inserted into a UFM that is already installed in the chassis.

- The transceiver is inserted into an uninstalled UFM that is then installed in the chassis.
- For a UFM with an integrated transceiver, the system detects the integrated transceiver when the UFM is inserted into the chassis.

1. Enter configuration mode.

```
bti7800# config
bti7800(config)#
```

2. Add a transceiver.

You can add a transceiver to a BIC or you can add a transceiver directly to a UFM. The type of transceiver you are adding is specified by the **optical-format** attribute. For more details on the **optical-format** attribute, see the *BTI7800 Series Command Line Reference Guide*.

- a. To add a transceiver to an existing BIC on a UFM3 or UFM4:

The following example adds a fixed-wavelength single-channel SFP+ transceiver to port 3 of an existing BIC in subslot 2 of the UFM in slot 2.

```
bti7800(config)# equipment chassis:1 module ufm:1/2 bic bic:1/2/2 transceiver
sfpPlus:1/2/2/3
Value for 'optical-format' [fixedX1,fixedX4,fixedX10,tunableX1,...]: fixedX1
bti7800#(config-transceiver-sfpPlus:1/2/2/3)#
```

- b. To add a transceiver component to the 100G Coherent MSA XCVR in an existing UFM4:

The following example adds a tunable single-channel CFP transceiver to an existing UFM in slot 2.

```
bti7800(config)# equipment chassis:1 module ufm:1/2 transceiver msa:1/2/1/1
Value for 'optical-format' [fixedX1,fixedX4,fixedX10,tunableX1,...]:
tunableX1
bti7800#(config-transceiver-msa:1/2/1/1)#
```



NOTE: The integrated transceiver in a UFM4 is a tunable CFP transceiver that is always addressed using subslot 1 port 1.

- c. To add a client-side transceiver to an existing UFM6:

The following example adds a QSFP+ transceiver to an existing UFM in slot 5.

```
bti7800(config)# equipment chassis:1 module ufm:1/5 transceiver qsfp:1/5/1/3
Value for 'optical-format' [fixedX1,fixedX4,fixedX10,none,...]: fixedX4
bti7800(config-transceiver-qsfp:1/5/1/3)#
```



NOTE: The client-side transceivers in UFM6 are always addressed using subslot 1.

- d. To add a transceiver component to the 400G Coherent MSA XCVR in an existing UFM6:

The following example adds a 400-Gbps transceiver to an existing UFM6 in slot 5.

```
bti7800(config)# equipment chassis:1 module ufm:1/5 transceiver
msa400:1/5/2/1
Value for 'optical-format' [fixedX1,fixedX4,fixedX10,none,...]: tunableX2
bti7800(config-transceiver-msa400:1/5/2/1)#
```



NOTE: The integrated transceiver in UFM6 is always addressed using subslot 2 port 1.

3. Optionally, configure the PEC.

You do not normally need to configure the PEC. If you do configure the PEC, ensure that the PEC matches the PEC of the transceiver that you install. You cannot configure PECs for integrated transceivers.

- a. For transceivers that do not have a 740-xxxxxx code assigned, enter the PEC.

For example:

```
bti7800#(config-transceiver-sfpPlus:1/2/2/3)# pec BP3AM6MS
```

- b. For transceivers that do have a 740-xxxxxx code assigned, enter the 740-xxxxxx code.

For example:

```
bti7800(config-transceiver-qsfp:1/5/1/3)# pec 740-058730
```

4. Apply the configuration changes.

For example:

```
bti7800(config)# commit
Commit complete.
```

Replacing a UFM3 or a UFM4

When replacing a UFM4 with a similarly equipped UFM3, or replacing a UFM3 with a similarly equipped UFM4, the system can automatically unprovision the old UFM and provision the new UFM. This is called auto-reprovisioning, and includes the unprovisioning

of the old equipment, interfaces, and cross-connects, and the reprovisioning of the new equipment, interfaces, and cross-connects.

Auto-reprovisioning automatically removes configuration for the old UFM, adds configuration for the new UFM, and modifies any parameters that are not compatible with the new UFM.

When auto-reprovisioning is performed successfully, the new UFM boots seamlessly into the new configuration, preserving all provisioned interfaces and cross-connects. No manual reconfiguration is necessary.

This section describes the software configuration changes that automatically result from this replacement procedure. For the replacement procedure itself, see the *BT17800 Series Hardware Overview and Installation Guide*.

- [Qualifying Criteria on page 92](#)
- [Provisioning Changes on page 93](#)
- [Alarm Behavior on page 95](#)
- [Post-Upgrade Verification on page 95](#)

Qualifying Criteria

The system automatically reprovisions a UFM when the following criteria are met:

UFM Replacement	Criteria	Notes
UFM4 to UFM3	<ul style="list-style-type: none"> • Auto-reprovisioning is enabled. See “Configuring Auto-Reprovisioning” on page 71. • A UFM3 is inserted into a slot that is provisioned for a UFM4. • An MSA transceiver is configured on the UFM4 being replaced. 	<p>The inserted UFM3 should have a 1x CFP BIC installed in BIC slot 1, and a 100G Coherent CFP installed in that BIC. The UFM3 should also have the same equipment installed in BIC slot 2 as the UFM4 being replaced.</p> <p>If the inserted UFM3 is not equipped as described, auto-reprovisioning still takes place but alarms might be raised indicating missing or mismatched equipment.</p>
UFM3 to UFM4	<ul style="list-style-type: none"> • Auto-reprovisioning is enabled. See “Configuring Auto-Reprovisioning” on page 71. • A UFM4 is inserted into a slot that is provisioned for a UFM3. • A 1x CFP BIC is configured in BIC slot 1 of the UFM3 being replaced. • A 100G Coherent CFP is configured on the 1x CFP BIC. 	<p>The inserted UFM4 should have the same equipment installed in BIC slot 2 as the UFM3 being replaced.</p> <p>If the inserted UFM4 is not equipped as described, auto-reprovisioning still takes place but alarms might be raised indicating missing or mismatched equipment.</p>



NOTE: Auto-reprovisioning does not apply to any other UFM replacement procedure.

Provisioning Changes

When the qualifying criteria are met, the system performs the following provisioning changes:

Table 12: Reprovisioning When Replacing a UFM4 with a UFM3

Parameter	Old Value (UFM4)	New Value (UFM3)
<code>equipment chassis module ufm ufm-type</code>	msa-non-switching	dual-bic-non-switching
<code>equipment chassis module ufm pec</code>	BT8A78UFM4	BT8A78UFM3
<code>equipment chassis module ufm transceiver msa</code>	Exists.	Removed.
<code>equipment chassis module ufm bic in BIC slot 1</code>	Does not exist.	Created.
<code>equipment chassis module ufm bic bic-type</code> for the BIC in BIC slot 1	--	cfp-bic
<code>equipment chassis module ufm bic admin-status</code> for the BIC in BIC slot 1	--	up
<code>equipment chassis module ufm bic transceiver cfp</code> for the BIC in BIC slot 1	Does not exist.	Created.
<code>equipment chassis module ufm bic transceiver cfp optical-format</code> for the CFP in the BIC in BIC slot 1	--	tunableX1
<code>equipment chassis module ufm bic transceiver cfp admin-status</code> for the CFP in the BIC in BIC slot 1	--	Set to the same value as the original <code>equipment chassis module ufm transceiver msa admin-status</code> .
<code>equipment chassis module ufm bic transceiver cfp custom</code> for the CFP in the BIC in BIC slot 1	--	Set to the same values as the original <code>equipment chassis module ufm transceiver msa custom</code> fields.
<code>interface</code>	Might exist.	Unchanged. If an interface for the MSA transceiver exists, then the same interface is now implicitly associated with the new CFP transceiver. If an interface for the MSA transceiver does not exist, then an interface for the new CFP transceiver also does not exist.
<code>interface otu4 cprws</code>	32-symbols	48-symbols
	8-symbols	6-symbols
	4-symbols	3-symbols
<code>cross-connect</code>	Might exist.	Unchanged.

Table 13: Reprovisioning When Replacing a UFM3 with a UFM4

Parameter	Old Value (UFM3)	New Value (UFM4)
equipment chassis module ufm ufm-type	dual-bic-non-switching	msa-non-switching
equipment chassis module ufm pec	BT8A78UFM3	BT8A78UFM4
equipment chassis module ufm transceiver msa	Does not exist.	Created.
equipment chassis module ufm transceiver msa optical-format	--	tunableX1
equipment chassis module ufm transceiver msa admin-status	--	Set to the same value as the original equipment chassis module ufm bic transceiver cfp admin-status .
equipment chassis module ufm transceiver msa custom	--	Set to the same values as the original equipment chassis module ufm bic transceiver cfp custom fields.
equipment chassis module ufm bic in BIC slot 1	Exists.	Removed.
equipment chassis module ufm bic transceiver cfp	Exists.	Removed.
interface	Might exist.	Unchanged. If an interface for the CFP transceiver exists, then the same interface is now implicitly associated with the new MSA transceiver. If an interface for the CFP transceiver does not exist, then an interface for the new MSA transceiver also does not exist.
interface otu4 cprws	48-symbols	32-symbols
	6-symbols	8-symbols
	3-symbols	4-symbols
interface otu4 tx-power	-15dBm to -5dBm	-5dBm
	-5dBm to 1dBm	Unchanged.
cross-connect	Might exist.	Unchanged.



NOTE: Auto-reprovisioning does not change any parameters for the equipment or interfaces in BIC slot 2.

Alarm Behavior

Under normal situations, when you insert a UFM into a slot provisioned for a UFM of another type, an Equipment Mismatch (eqptMism) alarm is raised against the inserted UFM.

In situations where auto-reprovisioning takes place, this alarm is suppressed.

Post-Upgrade Verification

After you replace the UFM, use the following commands to verify that the new UFM has been configured correctly:

- **show inventory** to verify that the new UFM and BICs are in inventory
- **show equipment** to verify that the new UFM and BICs are operationally up
- **show running-config equipment chassis:1 module ufm** to verify that the module configuration is correct
- **show running-config interface** to verify that the previous interface configuration has been properly propagated
- **show running-config cross-connect** to verify that the previous cross-connect configuration has been properly propagated
- **show conditions** to ensure that no unexpected condition or alarm exists

Configuring a Loopback on a UFM Interface

Use this procedure to place a UFM interface into loopback mode.

Both facility and terminal loopbacks are supported, as follows:

Loopback type	Supported interfaces	Description
Facility loopback	OTU, SONET/SDH, Ethernet interfaces	<p>Traffic arriving on the facility (link) is both looped back and allowed to pass straight through. Traffic in the opposite direction is dropped.</p> <p>For the looped-back traffic on OTU interfaces, the OTU overhead is regenerated and the FEC bytes are recalculated.</p>
Terminal loopback	OTU, SONET/SDH, Ethernet interfaces NOTE: Terminal loopback is not supported on an OTU interface that contains an ODU configured for multiplexing.	<p>Traffic arriving from a remote source (from the direction of the backplane) is both looped back and allowed to pass straight through to the local link. Traffic in the opposite direction is dropped.</p>

1. Enter configuration mode.

```
bti7800# config
bti7800(config)#
```

2. Disable the interface that is to be placed into loopback mode.

For example:

```
bti7800(config)# interface otu4:1/7/1/1
bti7800(config-interface-otu4:1/7/1/1)# disabled
```

The interface no longer passes traffic in either direction.

3. Place the interface into loopback mode.

- a. To configure a facility loopback:

```
bti7800(config-interface-otu4:1/7/1/1)# loopback-mode facility
```

- b. To configure a terminal loopback:

```
bti7800(config-interface-otu4:1/7/1/1)# loopback-mode terminal
```

4. Apply the configuration changes.

For example:

```
bti7800(config-interface-otu4:1/7/1/1)# commit
Commit complete.
```

The interface starts to pass traffic through and loop traffic back in accordance with the loopback type.

Release History Table

Release	Description
4.4	QSFP+ 40GE
4.4	multiplexed ODU3 subinterfaces
4.1	The UFM6 is supported starting with release 4.1.

Optical Modules

- [Terminal Amplifier Module on page 97](#)
- [Wavelength Protection Switch Module on page 97](#)

Terminal Amplifier Module

The 96-Channel Amplifier (AMP1) is a terminal amplifier module that integrates two erbium-doped optical amplifiers to provide bidirectional amplification of the composite DWDM signal in a point-to-point bookended configuration. The amplifier is optimized for 10-Gbps, 25-Gbps, and 100-Gbps signals, and includes an embedded optical supervisory channel (OSC) used for span loss control.

- [Provisioning a Terminal Amplifier Module on page 97](#)

Provisioning a Terminal Amplifier Module

Use this procedure to add a terminal amplifier module to a chassis. An example of a terminal amplifier is the 96-Channel Amplifier.

If auto-provisioning is enabled and you do not want to pre-provision, then you can skip this procedure because the system automatically provisions the terminal amplifier module when you insert the terminal amplifier module into the chassis.

1. Enter configuration mode.

```
bti7800# config
bti7800(config)#
```

2. Add the amplifier module.

For example, the following adds an amplifier module to chassis 1 slot 11:

```
bti7800(config)# equipment chassis:1 module amp:1/11
bti7800(config-module-amp:1/11)#
```

3. Specify the PEC.

For example, to specify the 96-Channel Amplifier:

```
bti7800(config-module-amp:1/11)# pec BT8A78AMP1
```

4. Apply the provisioning.

```
bti7800(config-module-amp:1/11)# commit
Commit complete.
```

Wavelength Protection Switch Module

The Wavelength Protection Switch (WPS4) provides four independent 1+1 revertive and non-revertive optical protection switches. It can be deployed with a variety of equipment including ROADM elements and non-equalizing terminal amplifiers.

- [Provisioning a WPS Module on page 98](#)

Provisioning a WPS Module

Use this procedure to add a WPS module to a chassis.

If auto-provisioning is enabled and you do not want to pre-provision, then you can skip this procedure because the system automatically provisions the WPS module when you insert the WPS module into the chassis.

1. Enter configuration mode.

```
bti7800# config
bti7800(config)#
```

2. Add the WPS module.

For example, to provision a WPS module in chassis 1 slot 12:

```
bti7800(config)# equipment chassis:1 module wps:1/12
bti7800(config-module-wps:1/12)#
```

3. Specify the PEC.

For example, to specify a WPS4 module:

```
bti7800(config-module-wps:1/12)# pec BT8A78WPS4
```

4. Apply the provisioning.

```
bti7800(config-module-wps:1/12)# commit
Commit complete.
```

Enabling and Disabling Modules

Use this procedure to administratively enable or disable modules.

Most modules can be administratively enabled or disabled. Modules should be administratively disabled prior to removal.

This procedure applies to all modules.

1. Enter configuration mode.

```
bti7800# config
bti7800(config)#
```

2. Enter configuration mode for the module you want to enable or disable.

For example, to enter configuration mode for the ROADM module in chassis 1 slot 8:

```
bti7800(config)# equipment chassis:1 module roadm:1/8
```

```
bti7800(config-module-roadm:1/8)#
```

3. Enable or disable the module.

- a. To enable the module:

For example:

```
bti7800(config-module-roadm:1/8)# admin-status up
```

- b. To disable the module:

For example:

```
bti7800(config-module-roadm:1/8)# admin-status down
```

4. Apply the provisioning.

```
bti7800(config-module-roadm:1/8)# commit
```

Commit complete.

Module Reload Times

A fully configured module might take several minutes to start up. [Table 14 on page 99](#) shows the expected worst-case module reload times for the different modules. The reload time is measured from the time that the reload command is issued to the time when the equipment state is operationally up and all the services on the module are up.

Table 14: Module Reload Times

Module	PEC	Warm Reload Startup Time	Cold Reload Startup Time
UFM3	BT8A78UFM3	7 minutes	7 minutes
UFM4	BT8A78UFM4	7 minutes	7 minutes
UFM6	BT8A78UFM6-I02	9 minutes	12 minutes
WPS4	BT8A78WPS4	8 minutes	6 minutes
AMP1	BT8A78AMP1	8 minutes	5 minutes



NOTE: These measurements were taken in release 4.1 and release 4.2. The reload times might be different in other releases.

CHAPTER 6

Transport Solutions

- UFM Interfaces on page 101
- Provisioning a Transport Interface on page 116
- Provisioning an Optical Channel Interface on page 120
- Provisioning Transponding and Muxponding Cross-Connects on page 122
- Link Layer Discovery Protocol (LLDP) Snooping on page 144
- Transport (UFM) Performance Monitoring on page 148

UFM Interfaces

- Overview on page 101
- UFM6 Interface and Protocol Restrictions on page 107
- Multiplexed Interfaces on page 111
- Forward Error Correction (FEC) Types on page 115

Overview

Interfaces on the UFM are defined by their names and types and are addressed in the following format: *interface_name:location_id*, as shown in [Table 15 on page 102](#):



NOTE: The UFM6 and the QSFP-4X10GE-LR (740-054050) and QSFP-100G-LR4-2 (740-074685) transceivers are supported starting with release 4.1.



NOTE: The QSFP-4X10GD-LR (740-058730) transceiver is supported starting with release 4.2.



NOTE: The QSFP-4X10GE-SR (740-054053), QSFP-100G-LR4-D (740-073859), and QSFP-100GBASE-SR4 (740-058734) transceivers are supported starting with release 4.3.



NOTE: The QSFP-40GBASE-SR4 (740-067443), QSFP-40GBASE-LR4 (740-073093 740-043308), and JNP-100G-AOC-xx (740-06xxxx) transceivers are supported starting with release 4.4.

Table 15: UFM Interfaces

Interface Name (Protocol)	Interface Type	Supported UFM	Supported Transceivers	Interface Identifier	Introduced in Release
otu2 ¹	otnOtu	UFM3	BP3AD6SS	otu2:chassis/slot/subslot/port	Before 2.1.1
		UFM4	BP3AM6MS BP3AM6DL-xx BP3AM6TL	For example: otu2:1/5/2/3	
		UFM6	QSFP-4X10GD-LR (740-058730)	otu2:chassis/slot/subslot/port/subport For example: otu2:1/5/1/10/4	
otu2e ¹	otnOtu	UFM3	BP3AD6SS BP3AM6MS BP3AM6DL-xx BP3AM6TL	otu2e:chassis/slot/subslot/port For example: otu2e:1/5/2/4	4.1
		UFM6	QSFP-4X10GD-LR (740-058730)	otu2e:chassis/slot/subslot/port/subport For example: otu2e:1/5/1/10/4	
otu4	otnOtu	UFM3	BP3AMASS	otu4:chassis/slot/subslot/port	Before 2.1.1
		UFM4	BP3AMDLI BP3AMCTL CFP-100GBASE-CHRT 100G Coherent MSA XCVR	For example: otu4:1/5/2/1	
		UFM6	400G Coherent MSA XCVR	otu4:chassis/slot/subslot/port/ subport.channel.tributary for OTU4 interfaces within an optical channel For example: otu4:1/5/2/1/2.1.2	
			QSFP-100G-LR4-D (740-073859)	otu4:chassis/slot/subslot/port For example: otu4:1/5/1/1	

Table 15: UFM Interfaces (continued)

Interface Name (Protocol)	Interface Type	Supported UFM	Supported Transceivers	Interface Identifier	Introduced in Release
odu2 ^{1,2}	otnOdu	UFM3	BP3AD6SS	odu2:chassis/slot/subslot/port	Before 2.1.1
		UFM4	BP3AM6MS	For example: odu2:1/5/2/3	
			BP3AM6DL-xx		
			BP3AM6TL		
		UFM6	QSFP-4X10GD-LR (740-058730)	odu2:chassis/slot/subslot/port/subport For example: odu2:1/5/1/10/4	4.2
odu2 ³	otnOdu	UFM3	BP3AMASS	odu2:chassis/slot/subslot/port.subinterface for ODU2 subinterfaces within an ODU4	Before 2.1.1
		UFM4	BP3AMDLI	For example: odu2:1/5/2/1.1	
			BP3AMCTL		
			CFP-100GBASE-CHRT		
			100G Coherent MSA XCVR		
		UFM6	400G Coherent MSA XCVR	odu2:chassis/slot/subslot/port/subport.channel.tributary.subinterface for ODU2 subinterfaces within an ODU4 For example: odu2:1/5/2/1/2.1.2.8	
odu2e ^{1,4}	otnOdu	UFM3	BP3AD6SS	odu2e:chassis/slot/subslot/port	4.1
			BP3AM6MS	For example: odu2e:1/5/2/3	
			BP3AM6DL-xx		
			BP3AM6TL		
		UFM6	QSFP-4X10GD-LR (740-058730)	odu2e:chassis/slot/subslot/port/subport For example: odu2e:1/5/1/10/4	4.2

Table 15: UFM Interfaces (continued)

Interface Name (Protocol)	Interface Type	Supported UFM	Supported Transceivers	Interface Identifier	Introduced in Release
odu2e ⁵	otnOdu	UFM3	BP3AMASS BP3AMDLI BP3AMCTL CFP-100GBASE-CHRT	odu2e:chassis/slot/subslot/port.subinterface for ODU2e subinterfaces within an ODU4 For example: odu2e:1/5/2/1.1	Before 2.1.1
		UFM6	400G Coherent MSA XCVR	odu2e:chassis/slot/subslot/port/subport.channel.tributary.subinterface for ODU2e subinterfaces within an ODU4 For example: odu2e:1/5/2/1/2.1.2.8	4.1
odu3	otnOdu	UFM6	400G Coherent MSA XCVR	odu3:chassis/slot/subslot/port/subport.channel.tributary.subinterface for ODU3 subinterfaces within an ODU4 For example: odu3:1/5/2/1/2.1.2.1	4.4
odu4 ⁶	otnOdu	UFM3	BP3AMASS	odu4:chassis/slot/subslot/port	Before 2.1.1
		UFM4	BP3AMDLI BP3AMCTL CFP-100GBASE-CHRT 100G Coherent MSA XCVR	For example: odu4:1/5/2/1	
		UFM6	400G Coherent MSA XCVR	odu4:chassis/slot/subslot/port/subport.channel.tributary for ODU4 interfaces within an optical channel. For example: odu4:1/5/2/1/2.1.2	4.1
			QSFP-100G-LR4-D (740-073859)	odu4:chassis/slot/subslot/port For example: odu4:1/5/1/1	4.3

Table 15: UFM Interfaces (continued)

Interface Name (Protocol)	Interface Type	Supported UFM3	Supported Transceivers	Interface Identifier	Introduced in Release
10ge ¹⁰	ethernetCsmacd	UFM3	BP3AD6SS	10ge:chassis/slot/subslot/port	Before 2.1.1
		UFM4	BP3AM6MS	For example: 10ge:1/5/2/3	
			BP3AM6DL-xx		
			BP3AM6TL		
		UFM6	QSFP-4X10GE-LR (740-054050)	10ge:chassis/slot/subslot/port/subport For example: 10ge:1/5/1/10/4	4.1
			QSFP-4X10GD-LR (740-058730)	Same as above.	4.2
			QSFP-4X10GE-SR (740-054053)	Same as above.	4.3
40ge ⁷¹⁰	ethernetCsmacd	UFM6	QSFP-4X10GE-SR (740-054053)	40ge:chassis/slot/subslot/port For example: 40ge:1/5/1/1	4.4
			QSFP-40GBASE-SR4 (740-067443)		
			QSFP-40GBASE-LR4 (740-073093) 740-043308)		
100ge ¹⁰	ethernetCsmacd	UFM3	BP3AMASS	100ge:chassis/slot/subslot/port	Before 2.1.1
		UFM4	BP3AMDLI	For example: 100ge:1/5/2/1	
		UFM6	QSFP-100G-LR4-2 (740-074685)	100ge:chassis/slot/subslot/port For example: 100ge:1/5/1/1	4.1
			QSFP-100G-LR4-D (740-073859)	Same as above.	4.3
			QSFP-100GBASE-SR4 (740-058734)	Same as above.	4.3
			JNP-100G-AOC-xx (740-06xxxx)	Same as above.	4.4

Table 15: UFM Interfaces (continued)

Interface Name (Protocol)	Interface Type	Supported UFM	Supported Transceivers	Interface Identifier	Introduced in Release
oc192 ¹	sonet	UFM3	BP3AM6MS	oc192:chassis/slot/subslot/port	Before 2.1.1
		UFM4	BP3AM6DL-xx BP3AM6TL	For example: oc192:1/5/2/3	
		UFM6	QSFP-4X10GD-LR (740-058730)	oc192:chassis/slot/subslot/port/subport For example: oc192:1/5/1/10/3	
stm64 ¹	sonet	UFM3	BP3AM6MS	stm64:chassis/slot/subslot/port	Before 2.1.1
		UFM4	BP3AM6DL-xx BP3AM6TL	For example: stm64:1/5/2/3	
		UFM6	QSFP-4X10GD-LR (740-058730)	stm64:chassis/slot/subslot/port/subport For example: stm64:1/5/1/10/3	
wanoc192 ⁸	sonet	UFM3	BP3AM6MS	wanoc192:chassis/slot/subslot/port	Before 2.1.1
		UFM4	BP3AM6DL-xx BP3AM6TL	For example: wanoc192:1/5/2/3	
wanstm64 ⁹	sonet	UFM3	BP3AM6MS	wanstm64:chassis/slot/subslot/port	Before 2.1.1
		UFM4	BP3AM6DL-xx BP3AM6TL	For example: wanstm64:1/5/2/3	
och	opticalChannel	UFM6	400G Coherent MSA XCVR	och:chassis/slot/subslot/port/subport.channel For example: och:1/5/2/1/2.1	4.1
8gfc	fibreChannel	UFM6	QSFP-4X10GE-SR (740-054053) QSFP-4X10GD-LR (740-058730)	8gfc:chassis/slot/subslot/port/subport For example: 8gfc:1/5/1/10/3	4.3
10gfc	fibreChannel	UFM6	QSFP-4X10GE-SR (740-054053) QSFP-4X10GD-LR (740-058730)	10gfc:chassis/slot/subslot/port/subport For example: 10gfc:1/5/1/10/3	4.3

Table 15: UFM Interfaces (continued)

Interface Name (Protocol)	Interface Type	Supported UFM3	Supported Transceivers	Interface Identifier	Introduced in Release
---------------------------	----------------	----------------	------------------------	----------------------	-----------------------

¹ The UFM3 and UFM4 are compatible with most OTN/SONET/SDH transport applications. Contact your Juniper Networks representative for more information.

² Created automatically when an otu2 interface is created on a 10-Gbps port.

³ Created automatically on a UFM3 and UFM4 when a gmp-capable odu4 interface is created. Must be manually created on a UFM6.

⁴ Created automatically when an otu2e interface is created on a 10-Gbps port.

⁵ Created automatically on UFM6 when a gmp-capable odu4 line interface is created. Must be manually created on a UFM3 and UFM4.

⁶ Created automatically when an otu4 interface is created.

⁷ 40ge interfaces can only be created on a UFM6 if the UFM6 has the correct SERDES configuration applied. See [“Provisioning a Transport Interface” on page 116](#) for details.

⁸ 10-Gigabit Ethernet WAN PHY over OC-192.

⁹ 10-Gigabit Ethernet WAN PHY over STM-64.

¹⁰ Ethernet interfaces on all UFM3 support fixed rate, full-duplex only. Do not enable auto-negotiation in equipment attached to these interfaces.

UFM6 Interface and Protocol Restrictions

Figure 4: UFM6 Client Ports

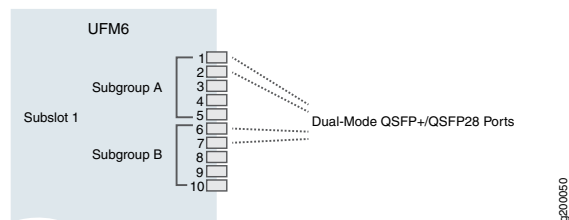


Figure 4 on page 107 shows the UFM6 client ports (port group 1). The client ports are divided into two subgroups: A for ports 1 through 5, and B for ports 6 through 10. Ports within a subgroup must be provisioned for the same rate group; however, ports in different subgroups can be provisioned for a different rate group. There are two protocol rate groups, as follows:

- 10-Gbps, 40-Gbps
- 100-Gbps

For example, ports in subgroup A can be provisioned as QSFP+ (10-Gbps) and QSFP+ 40GE (40-Gbps) ports, while ports in subgroup B can be provisioned as QSFP28 (100-Gbps) ports, or vice versa.

Additionally, the QSFP+ 40GE and QSFP28 transceivers can only be installed in specific client ports, as follows:

- The QSFP+ 40 GE transceiver can only be installed in client ports 1, 2, 4, 5, 6, 7, 9, and 10. Installing a QSFP+ 40GE transceiver in client ports 3 or 8 will cause an Inventory Unsupported (InventoryUnsupp) alarm to be raised against the transceiver.
- The QSFP28 transceiver can only be installed in the dual-mode client ports 1, 2, 6, and 7. Installing a QSFP28 transceiver in client ports 3, 4, 5, 8, 9, or 10 will cause an Inventory Unsupported (InventoryUnsupp) alarm to be raised against the transceiver.

[Table 16 on page 108](#) lists the possible client port configurations for the supported transceivers.

Table 16: UFM6 Client Port Configurations

Description	Subgroup	Transceiver	Ports
4 x 10-Gbps and 40-Gbps transceivers in both subgroup A and subgroup B	A	QSFPP-4X10GE-LR (740-054050)	1 to 5
		QSFPP-4X10GD-LR (740-058730)	
		QSFPP-4X10GE-SR (740-054053)	
	B	QSFPP-40GBASE-SR4 (740-067443)	1, 2, 4, 5
		QSFPP-40GBASE-LR4 (740-073093 740-043308)	
		QSFPP-40GBASE-LR4 (740-073093 740-043308)	
	A	QSFPP-4X10GE-LR (740-054050)	6 to 10
		QSFPP-4X10GD-LR (740-058730)	
		QSFPP-4X10GE-SR (740-054053)	
	B	QSFPP-40GBASE-SR4 (740-067443)	6, 7, 9, 10
		QSFPP-40GBASE-LR4 (740-073093 740-043308)	
		QSFPP-40GBASE-LR4 (740-073093 740-043308)	

Table 16: UFM6 Client Port Configurations (continued)

Description	Subgroup	Transceiver	Ports
4 x 10-Gbps and 40-Gbps transceivers in subgroup A and 100-Gbps transceivers in subgroup B	A	QSFP-4X10GE-LR (740-054050)	1 to 5
		QSFP-4X10GD-LR (740-058730)	
		QSFP-4X10GE-SR (740-054053)	
		QSFP-40GBASE-SR4 (740-067443)	1, 2, 4, 5
		QSFP-40GBASE-LR4 (740-073093 740-043308)	
	B	QSFP-100G-LR4-2 (740-074685)	6, 7
		QSFP-100G-LR4-D (740-073859)	
		QSFP-100GBASE-SR4 (740-058734)	
		JNP-100G-AOC-xx (740-06xxxx)	8 to 10
		Unused	
100-Gbps transceivers in subgroup A and 4 x 10-Gbps and 40-Gbps transceivers in subgroup B	A	QSFP-100G-LR4-2 (740-074685)	1, 2
		QSFP-100G-LR4-D (740-073859)	
		QSFP-100GBASE-SR4 (740-058734)	
		Unused	3 to 5
	B	QSFP-4X10GE-LR (740-054050)	6 to 10
		QSFP-4X10GD-LR (740-058730)	
		QSFP-4X10GE-SR (740-054053)	
		QSFP-40GBASE-SR4 (740-067443)	6, 7, 9, 10
		QSFP-40GBASE-LR4 (740-073093 740-043308)	

Table 16: UFM6 Client Port Configurations (continued)

Description	Subgroup	Transceiver	Ports
100-Gbps transceivers in both subgroup A and subgroup B	A	QSFP-100G-LR4-2 (740-074685)	1, 2
		QSFP-100G-LR4-D (740-073859)	
		QSFP-100GBASE-SR4 (740-058734)	
		JNP-100G-AOC-xx (740-06xxxx)	
	B	Unused	3 to 5
		Unused	
	B	QSFP-100G-LR4-2 (740-074685)	6, 7
		QSFP-100G-LR4-D (740-073859)	
		QSFP-100GBASE-SR4 (740-058734)	
		JNP-100G-AOC-xx (740-06xxxx)	
		Unused	8 to 10
		Unused	

The client dual-mode ports on the UFM6 have restrictions on what protocol combinations can be configured on its subports when using QSFP+ 4 x 10-Gbps transceivers. This is shown in [Table 17 on page 110](#). This table does not apply to QSFP+ 40GE transceivers.

Table 17: UFM6 Client QSFP+ Dual-Mode Subport Protocol Restrictions

Client Port	10-Gbps Subports	Protocol Restrictions
1	1 to 4	<p>All subports must be configured for the same protocol family:</p> <ul style="list-style-type: none"> all 10ge all otu2/odu2 all otu2e/odu2e all oc192/stm64 all 8gfc all 10gfc
2	1 to 4	<p>All subports must be configured for the same protocol family:</p> <ul style="list-style-type: none"> all 10ge all otu2/odu2 all otu2e/odu2e all oc192/stm64 all 8gfc all 10gfc
3	1 to 4	No restriction

Table 17: UFM6 Client QSFP+ Dual-Mode Subport Protocol Restrictions (continued)

Client Port	10-Gbps Subports	Protocol Restrictions
4	1 to 4	No restriction
5	1 to 4	No restriction
6	1 to 4	All subports must be configured for the same protocol family: <ul style="list-style-type: none"> • all 10ge • all otu2/odu2 • all otu2e/odu2e • all oc192/stm64 • all 8gfc • all 10gfc
7	1 to 4	All subports must be configured for the same protocol family: <ul style="list-style-type: none"> • all 10ge • all otu2/odu2 • all otu2e/odu2e • all oc192/stm64 • all 8gfc • all 10gfc
8	1 to 4	No restriction
9	1 to 4	No restriction
10	1 to 4	No restriction

Multiplexed Interfaces

An ODU4 interface on a UFM3, UFM4, or on the integrated transceiver on a UFM6 can be configured as a multiplexed (**gmp-capable**) interface that maps lower-order ODUs into the ODU4 using the generic mapping procedure (GMP). The same ODU4 can contain a mix of ODU2, ODU2e, and ODU3 signals (where supported).

Table 18 on page 112 shows the multiplexing that is supported on the various UFM6s:

Table 18: UFM Multiplexed Interfaces

Subinterface	Containing interface	Description	UFM	Example identifiers
ODU2 or ODU2e	ODU4	Ten lower-order ODU subinterfaces within an ODU4.	UFM3	odu2:1/7/1/1.x or odu2e:1/7/1/1.x , where x is a value from 1 to 10.
		Each ODU subinterface consists of eight 1.25 Gbps tributary slots.	UFM4	odu2:1/7/1/1.x , where x is a value from 1 to 10. NOTE: The UFM4 does not support ODU2e.
			UFM6	odu2:1/5/2/1/2.1.2.x or odu2e:1/5/2/1/2.1.2.x , where x is a value from 1 to 10.
ODU3	ODU4	Two lower-order ODU subinterfaces within an ODU4. Each ODU subinterface consists of thirty-one 1.25 Gbps tributary slots.	UFM6	odu3:1/5/2/1/x.1.y.Z where x, y, Z are values from 1 to 2.

The mapping of the subinterfaces to the containing ODU4 interface is specified by the optical data tributary group (**odtg**) and the tributary slot list (**tributary-slot-list**) attributes on the ODU4 interface. These attributes are automatically configured and cannot be changed.

The mappings for ODU2 and ODU2e interfaces into an ODU4 are shown in [Table 19 on page 112](#). Each ODU4 contains up to 10 ODU2 and ODU2e subinterfaces.

Table 19: ODU2 (ODU2e) Subinterface Mapping Into an ODU4

Subinterface	Default ODTG	Default tributary slots
ODU2 1.1 ODU2e 1.1	1	1 to 8
ODU2 1.2 ODU2e 1.2	2	9 to 16
ODU2 1.3 ODU2e 1.3	3	17 to 24
ODU2 1.4 ODU2e 1.4	4	25 to 32
ODU2 1.5 ODU2e 1.5	5	33 to 40

Table 19: ODU2 (ODU2e) Subinterface Mapping Into an ODU4 (continued)

Subinterface	Default ODTG	Default tributary slots
ODU2 1.6 ODU2e 1.6	6	41 to 48
ODU2 1.7 ODU2e 1.7	7	49 to 56
ODU2 1.8 ODU2e 1.8	8	57 to 64
ODU2 1.9 ODU2e 1.9	9	65 to 72
ODU2 1.10 ODU2e 1.10	10	73 to 80

The mappings for ODU3 subinterfaces into an ODU4 on an optical channel on the UFM6 are shown in [Table 20 on page 113](#). Each ODU4 contains up to two ODU3 subinterfaces, but the mapping is different depending on whether the ODU3 is mapped to the first or to the second ODU4 in the optical channel. In the first ODU4, the ODU3 subinterfaces are mapped to the lower order tributary slots, leaving 16 unmapped higher order tributary slots for ODU2 and ODU2e mappings. In the second ODU4, the ODU3 subinterfaces are mapped to the higher order tributary slots, leaving 16 unmapped lower order tributary slots for ODU2 and ODU2e mappings.

Table 20: ODU3 Subinterface Mapping Into an ODU4

Subinterface	Default ODTG	Default tributary slots
First ODU4		
ODU3 1.1	1	1 to 31
ODU3 1.2	5	33 to 63
Available for ODU2 or ODU2e	9	65 to 72
Available for ODU2 or ODU2e	10	73 to 80
Second ODU4		
Available for ODU2 or ODU2e	1	1 to 8
Available for ODU2 or ODU2e	2	9 to 16

Table 20: ODU3 Subinterface Mapping Into an ODU4 (continued)

Subinterface	Default ODTG	Default tributary slots
ODU3 2.1	3	17 to 47
ODU3 2.2	7	49 to 79

If you are configuring a mix of ODU2, ODU2e, and ODU3 subinterfaces on an ODU4 on a UFM6, ensure that the subinterfaces do not use conflicting tributary slots. For example, if you configure ODU3 2.1, which uses tributary slots 17 to 47 on the second ODU4, you cannot also configure ODU2 or ODU2e subinterfaces 1.3 through 1.6 on the same ODU4 because those ODU2 or ODU2e subinterfaces use tributary slots 17 through 48.

- [Multiplexed Interfaces on UFM3 and UFM4 on page 114](#)
- [Multiplexed Interfaces on UFM6 on page 114](#)

Multiplexed Interfaces on UFM3 and UFM4

The ODU2 subinterfaces are automatically created on UFM3 and UFM4 as follows:

- When you configure an ODU4 interface for multiplexing, the system automatically creates 10 ODU2 subinterfaces .1 through .10. For example (truncated for clarity):

```
bt17800(config)# do show interface table | include 1/7
```

```

odu2:1/7/1/1.1      n/a          no-multiplex  n/a
odu2:1/7/1/1.2      n/a          no-multiplex  n/a
odu2:1/7/1/1.3      n/a          no-multiplex  n/a
odu2:1/7/1/1.4      n/a          no-multiplex  n/a
odu2:1/7/1/1.5      n/a          no-multiplex  n/a
odu2:1/7/1/1.6      n/a          no-multiplex  n/a
odu2:1/7/1/1.7      n/a          no-multiplex  n/a
odu2:1/7/1/1.8      n/a          no-multiplex  n/a
odu2:1/7/1/1.9      n/a          no-multiplex  n/a

odu2:1/7/1/1.10     n/a          no-multiplex  n/a
odu4:1/7/1/1        lowerLayerDown gmp-capable   n/a
otu4:1/7/1/1        enabled      lowerLayerDown 192.100 THz 1560.61 nm enabled

```

If you want ODU2e subinterfaces instead, delete the corresponding ODU2 subinterface and manually create the desired ODU2e subinterface. You can have a mix of ODU2 and ODU2e subinterfaces within the same ODU4. For information on changing between ODU2 and ODU2e subinterfaces, see [“Provisioning a Transport Interface” on page 116](#).

Multiplexed Interfaces on UFM6

The ODU2e subinterfaces are automatically created on UFM6 as follows:

- When you create an ODU4 line interface, the system automatically configures it for multiplexing and creates ten ODU2e subinterfaces .1 through .10. For example (truncated for clarity):

```
bti7800(config)# do show interface table | include 1/5/2/1/2.1.2
```

odu2e:1/5/2/1/2.1.2.1	n/a	no-multiplex	n/a
odu2e:1/5/2/1/2.1.2.2	n/a	no-multiplex	n/a
odu2e:1/5/2/1/2.1.2.3	n/a	no-multiplex	n/a
odu2e:1/5/2/1/2.1.2.4	n/a	no-multiplex	n/a
odu2e:1/5/2/1/2.1.2.5	n/a	no-multiplex	n/a
odu2e:1/5/2/1/2.1.2.6	n/a	no-multiplex	n/a
odu2e:1/5/2/1/2.1.2.7	n/a	no-multiplex	n/a
odu2e:1/5/2/1/2.1.2.8	n/a	no-multiplex	n/a
odu2e:1/5/2/1/2.1.2.9	n/a	no-multiplex	n/a
odu2e:1/5/2/1/2.1.2.10	n/a	no-multiplex	n/a
odu4:1/5/2/1/2.1.2	lowerLayerDown	gmp-capable	n/a
otu4:1/5/2/1/2.1.2	enabled	lowerLayerDown	n/a

If you want a different type of subinterface, delete the corresponding ODU2e subinterface and manually create the desired ODU subinterface. You can have a mix of ODU2, ODU2e, and ODU3 subinterfaces within the same ODU4. If you are creating an ODU3 subinterface, you will need to delete all the ODU2 and ODU2e subinterfaces that use the same tributary slots as the new ODU3 subinterface. See [Table 19 on page 112](#) and [Table 20 on page 113](#) for the tributary slots that the different ODU subinterfaces use.

For information on changing between ODU2, ODU2e, and ODU3 subinterfaces, see [“Provisioning a Transport Interface” on page 116](#).

Forward Error Correction (FEC) Types

Forward error correction can be provisioned on OTU and optical channel interfaces. The following are the supported configurations:

Table 21: FEC Types

Interface	Supported FEC Types
OTU2 or OTU2e	<ul style="list-style-type: none"> No FEC (no-fec) Generic FEC (g-fec) G.975.1 i.4 Super FEC (s-fec-i4) G.975.1 i.7 Super FEC (s-fec-i7) <p>NOTE: The ports on the 12x SFP+ BIC are divided into three port groups (ports 1 to 4, ports 5 to 8, ports 9 to 12). Within each port group, you cannot configure one port for G.975.1 i.4 Super FEC and another port for G.975.1 i.7 Super FEC. The Super FEC settings are mutually exclusive within a port group.</p> <p>On a UFM6, all 10-Gbps client ports within the same QSFP+ transceiver have a similar restriction. You cannot configure one 10-Gbps port for G.975.1 i.4 Super FEC and another 10-Gbps port on the same transceiver for G.975.1 i.7 Super FEC. The Super FEC settings are mutually exclusive within a transceiver.</p>
OTU4 on 100G Coherent MSA XCVR	<ul style="list-style-type: none"> Soft-Decision FEC (soft-fec)
OTU4 on 100G Coherent CFP	<ul style="list-style-type: none"> Soft-Decision FEC (soft-fec)

Table 21: FEC Types (continued)

Interface	Supported FEC Types
OTU4 on all other CFPs	<ul style="list-style-type: none"> Swizzle FEC (swiz-fec)
OTU4 on the QSFP28 100GE Ethernet/OTN LR4 (QSFP-100G-LR4-D (740-073859))	<ul style="list-style-type: none"> No FEC (no-fec) Generic FEC (g-fec)
Optical channel on 400G Coherent MSA XCVR	<ul style="list-style-type: none"> Soft-Decision FEC with 25% overhead (sd-fec-25pc) for 16-QAM modulation Soft-Decision FEC with 25% overhead (sd-fec-25pc) for QPSK modulation - Releases 4.2 and higher Soft-Decision FEC (soft-fec) for QPSK modulation - Releases 4.2 and higher <p>NOTE: This FEC is applied to the optical channel, which can include one or two OTU4 signals.</p>

Release History Table

Release	Description
4.4	The QSFP-40GBASE-SR4 (740-067443), QSFP-40GBASE-LR4 (740-073093 740-043308), and JNP-100G-AOC-xx (740-06xxxx) transceivers are supported starting with release 4.4.
4.4	QSFP+ 40GE
4.4	ODU3
4.3	The QSFP-4X10GE-SR (740-054053), QSFP-100G-LR4-D (740-073859), and QSFP-100GBASE-SR4 (740-058734) transceivers are supported starting with release 4.3.
4.3	OTU4 on the QSFP28 100GE Ethernet/OTN LR4 (QSFP-100G-LR4-D (740-073859))
4.2	The QSFP-4X10GD-LR (740-058730) transceiver is supported starting with release 4.2.
4.2	Soft-Decision FEC with 25% overhead (sd-fec-25pc) for QPSK modulation
4.2	Soft-Decision FEC (soft-fec) for QPSK modulation
4.1	The UFM6 and the QSFP-4X10GE-LR (740-054050) and QSFP-100G-LR4-2 (740-074685) transceivers are supported starting with release 4.1.

Provisioning a Transport Interface

Use this procedure to provision a transport interface on a UFM.

Prerequisites

- The corresponding transceiver is provisioned.
- The correct SERDES configuration must be applied on the UFM6 if you are configuring a 40Ge interface on the UFM6. Otherwise, the configuration will fail and you will see a `cfgFail` alarm. The correct SERDES configuration is automatically applied if the UFM6 is inserted, reseated, or cold reloaded when the chassis is running software release 4.4 or higher.

1. Enter configuration mode.

```
bti7800# config
bti7800(config)#
```

2. Add the interface.

The following example adds an OTU4 interface. See [“UFM Interfaces” on page 101](#) for information on setting the interface **type**.

```
bti7800(config)# interface otu4:1/7/1/1
Value for 'type' [ethernetCsmacd,otn0du,otn0tu,sonet]: otn0tu
bti7800(config-interface-otu4:1/7/1/1)#
```



NOTE: This automatically creates a corresponding `odu4:1/7/1/1` interface.

3. Specify the frequency of the interface. This is required for interfaces with tunable transceivers.

For example:

```
bti7800(config-interface-otu4:1/7/1/1)# frequency 192.1
```

4. Specify the type of FEC to use. The FEC type can only be changed when the interface is disabled.

For example:

```
bti7800(config-interface-otu4:1/7/1/1)# disabled
bti7800(config-interface-otu4:1/7/1/1)# fec-type soft-fec
bti7800(config-interface-otu4:1/7/1/1)# commit
Commit complete.
bti7800(config-interface-otu4:1/7/1/1)# enabled
bti7800(config-interface-otu4:1/7/1/1)# commit
Commit complete.
```

See [“Forward error correction \(FEC\) types” on page 115](#) for information on supported values for the **fec-type**.

5. Specify whether the corresponding ODU interface is a multiplexed (muxponding) or non-multiplexed (transponding) interface.



NOTE: Muxponding is only supported when multiplexing onto ODU4 interfaces.

- a. To configure a non-multiplexed interface:

```
bti7800(config-interface-odu4:1/7/1/1)# multiplex-mode no-multiplex
bti7800(config-interface-odu4:1/7/1/1)# commit
Commit complete.
```

- b. To configure a multiplexed interface:

```
bti7800(config-interface-odu4:1/7/1/1)# multiplex-mode gmp-capable
bti7800(config-interface-odu4:1/7/1/1)# commit
Commit complete.
```

After you configure a multiplexed ODU4 interface and commit the changes, the lower-order subinterfaces are automatically created. Depending on the UFM, the system creates either ODU2 or ODU2e subinterfaces.

Here is an example of the lower-order ODU2 subinterfaces within an ODU4 (truncated for clarity):

```
bti7800(config)# do show interface table | include odu2:1/7/1/1
```

odu2:1/7/1/1.1	n/a	no-multiplex	n/a
odu2:1/7/1/1.2	n/a	no-multiplex	n/a
odu2:1/7/1/1.3	n/a	no-multiplex	n/a
odu2:1/7/1/1.4	n/a	no-multiplex	n/a
odu2:1/7/1/1.5	n/a	no-multiplex	n/a
odu2:1/7/1/1.6	n/a	no-multiplex	n/a
odu2:1/7/1/1.7	n/a	no-multiplex	n/a
odu2:1/7/1/1.8	n/a	no-multiplex	n/a
odu2:1/7/1/1.9	n/a	no-multiplex	n/a
odu2:1/7/1/1.10	n/a	no-multiplex	n/a

Here is an example of the lower-order ODU2e subinterfaces within an ODU4 (truncated for clarity):

```
bti7800(config)# do show interface table | include odu2e:1/5/2/1/2.1.2
```

odu2e:1/5/2/1/2.1.2.1	n/a	no-multiplex	n/a
odu2e:1/5/2/1/2.1.2.2	n/a	no-multiplex	n/a
odu2e:1/5/2/1/2.1.2.3	n/a	no-multiplex	n/a
odu2e:1/5/2/1/2.1.2.4	n/a	no-multiplex	n/a
odu2e:1/5/2/1/2.1.2.5	n/a	no-multiplex	n/a
odu2e:1/5/2/1/2.1.2.6	n/a	no-multiplex	n/a
odu2e:1/5/2/1/2.1.2.7	n/a	no-multiplex	n/a
odu2e:1/5/2/1/2.1.2.8	n/a	no-multiplex	n/a
odu2e:1/5/2/1/2.1.2.9	n/a	no-multiplex	n/a
odu2e:1/5/2/1/2.1.2.10	n/a	no-multiplex	n/a

Here is an example of the lower-order ODU3 subinterfaces within an ODU4 (truncated for clarity):

```
bti7800# show interface table | include odu3
```

odu3:1/14/2/1/1.1.1.1	n/a	no-multiplex	n/a
odu3:1/14/2/1/1.1.1.2	n/a	no-multiplex	n/a

- c. To change a subinterface between different ODU types::

In some situations, you might want to change an ODU2 subinterface to an ODU2e subinterface and vice-versa. To do this, delete the subinterface you want to replace and create the desired subinterface.

For example, the following deletes an ODU2e subinterface and creates a new ODU2 subinterface at that same location.

```
bti7800(config)# no interface odu2e:1/5/2/1/2.1.2.5
```

```
bti7800(config)# interface odu2:1/5/2/1/2.1.2.5
```

Value for 'type' [ethernetCsmacd,opticalChannel,otnOdu,otnOtu,...]: otnOdu

```
bti7800(config-interface-odu2:1/5/2/1/2.1.2.5)# commit
```

Commit complete.

For example, the following deletes a set of ODU2e subinterfaces and creates a new ODU3 subinterface that uses the same tributary slots.

```
bti7800(config)# no interface odu2e:1/14/2/1/1.1.1.1
```

```
bti7800(config)# no interface odu2e:1/14/2/1/1.1.1.2
```

```
bti7800(config)# no interface odu2e:1/14/2/1/1.1.1.3
```

```
bti7800(config)# no interface odu2e:1/14/2/1/1.1.1.4
```

```
bti7800(config)# interface odu3:1/14/2/1/1.1.1.1
```

Value for 'type' [ethernetCsmacd,opticalChannel,otnOdu,otnOtu,...]: otnOdu

```
bti7800(config-interface-odu3:1/14/2/1/1.1.1.1)# commit
```

Commit complete.



NOTE: You must delete and create the subinterface before committing. If you commit in between the deletion and creation, you will get an error.

For information on multiplexed interfaces, see [“Multiplexed Interfaces” on page 111](#).

Release History Table

Release	Description
4.4	The correct SERDES configuration must be applied on the UFM6 if you are configuring a 40ge interface on the UFM6.
4.4	ODU3 subinterfaces within an ODU4

Provisioning an Optical Channel Interface

Use this procedure to create an optical channel interface on the 400G Coherent MSA XCVR on a UFM6.

The 400G Coherent MSA XCVR contains two 200-Gbps line ports that are visible on the faceplate, with each 200-Gbps port carrying a single optical channel. The optical channel represents the optical signal and contains the settings and attributes that govern the constituent 100-Gbps signals.

Depending on the modulation chosen, each optical channel can contain one or two 100-Gbps signals.

The optical channel is represented as an interface. It must be created before the constituent OTU4 interfaces are created.

1. Enter configuration mode.

```
bt17800# config
bt17800(config)#
```

2. Create the optical channel interface. For example:

```
bt17800(config)# interface och:1/5/2/1/1.1
Value for 'type' [ethernetCsmacd,opticalChannel,otn0du,otn0tu,...]:
opticalChannel
bt17800(config-interface-och:1/5/2/1/1.1)#
```

Do not commit the provisioning until the very end of this procedure. Certain attributes can only be set during interface creation (before committing).

3. Specify the frequency of the optical signal.

For example:

```
bt17800(config-interface-och:1/5/2/1/1.1)# frequency 192.1
```

4. Specify the modulation.

You can set the modulation to 16-QAM or QPSK. If you set the modulation to 16-QAM, the optical channel can contain up to two OTU4 signals (at the expense of reach). If

you set the modulation to QPSK, the optical channel can contain only one OTU4 signal but with longer reach.

For example:

```
bti7800(config-interface-och:1/5/2/1/1.1)# modulation qpsk
```



NOTE: In releases lower than release 4.3, the modulation setting must be the same on both optical channels on the UFM6. In releases 4.3 and higher, this restriction does not apply and the modulation setting can be different on both optical channels.

5. Specify the type of FEC to use.

For example:

```
bti7800(config-interface-och:1/5/2/1/1.1)# fec-type sd-fec-25pc
```

See [“Forward error correction \(FEC\) types” on page 115](#) for information on supported values for the **fec-type**.



NOTE: In releases lower than release 4.3, the FEC type must be the same on both optical channels on the UFM6. In releases 4.3 and higher, this restriction does not apply and the FEC type can be different on both optical channels.

6. Apply the provisioning.

```
bti7800(config-interface-och:1/5/2/1/1.1)# commit
Commit complete.
```

Release History Table

Release	Description
4.3	In releases 4.3 and higher, this restriction does not apply and the modulation setting can be different on both optical channels.
4.3	In releases 4.3 and higher, this restriction does not apply and the FEC type can be different on both optical channels.

Provisioning Transponding and Muxponding Cross-Connects

- [Supported Cross-Connects on page 122](#)
- [Provisioning a Transponding Cross-Connect on a UFM3 or UFM4 on page 136](#)
- [Provisioning a Transponding Cross-Connect on a UFM6 on page 138](#)
- [Provisioning a Muxponding Cross-Connect on a UFM3 or UFM4 on page 139](#)
- [Provisioning a Muxponding Cross-Connect on a UFM6 on page 141](#)

Supported Cross-Connects

Cross-connects can be created between interfaces within the same UFM. Cross-connects cannot be created across UFM. Depending on what you are cross-connecting, you can be regenerating, transponding, or muxponding.

[Table 22 on page 122](#) lists the cross-connects that are supported. The **A** and **B** designations in the table are used only to distinguish between the two cross-connect endpoints. They are assigned arbitrarily and are interchangeable.



NOTE: Not all interfaces are supported on all transceivers. To see which transceivers support which interfaces, see [“UFM Interfaces” on page 101](#).



NOTE: The UFM6 is supported starting with release 4.1.



NOTE: When cross-connecting two 10-Gbps interfaces on a UFM3 equipped with 12x SFP+ BICs, both interfaces must reside on the same BIC.

Table 22: UFM Cross-Connects

Description	Supported UFM	Interface A	Interface B	Rate	Introduced in Release
Regenerating					
10GbE to/from 10GbE	UFM3 UFM4	10ge on an SFP+ transceiver	10ge on an SFP+ transceiver	10GbE	Before 2.1.1

Table 22: UFM Cross-Connects (continued)

Description	Supported UFM3 UFM4	Interface A	Interface B	Rate	Introduced in Release
SONET/SDH (OC-192/STM-64/10GbE WAN PHY) to/from SONET/SDH (OC-192/STM-64/10GbE WAN PHY)	UFM3 UFM4	oc192/stm64/wanoc192/wanstm64 on an SFP+ transceiver	oc192/stm64/wanoc192/wanstm64 on an SFP+ transceiver	OC-192 or STM-64	Before 2.1.1
OTU2 to/from OTU2	UFM3 UFM4	odu2 on an SFP+ transceiver	odu2 on an SFP+ transceiver	ODU2	Before 2.1.1
OTU2e to/from OTU2e	UFM3	odu2e on an SFP+ transceiver	odu2e on an SFP+ transceiver	ODU2e	4.1
100GbE to/from 100GbE	UFM3	100ge on a CFP transceiver	100ge on a CFP transceiver	100GbE	4.2
OTU4 to/from OTU4	UFM3 UFM4	odu4 on a CFP or on the integrated transceiver	odu4 on a CFP or on the integrated transceiver	ODU4	Before 2.1.1
	UFM6 ¹	odu4 on a QSFP28 transceiver	odu4 on the integrated transceiver	ODU4	4.3
Transponding					
10GbE to/from OTU2	UFM3 UFM4	10ge on an SFP+ transceiver	odu2 on an SFP+ transceiver	ODU2	Before 2.1.1
10GbE to/from OTU2e	UFM3	10ge on an SFP+ transceiver	odu2e on an SFP+ transceiver	ODU2e	4.5
SONET/SDH (OC-192/STM-64/10GbE WAN PHY) to/from OTU2	UFM3 UFM4	oc192/stm64/wanoc192/wanstm64 on an SFP+ transceiver	odu2 on an SFP+ transceiver	ODU2	Before 2.1.1
100GbE to/from OTU4	UFM3 UFM4	100ge on a CFP transceiver	odu4 on a CFP or on the integrated transceiver	ODU4	Before 2.1.1
	UFM6 ¹	100ge on a QSFP28 transceiver	odu4 on the integrated transceiver	ODU4	4.1
Muxponding					

Table 22: UFM Cross-Connects (continued)

Description	Supported UFM	Interface A	Interface B	Rate	Introduced in Release
10GbE to/from OTU4	UFM3 UFM4	10ge on an SFP+ transceiver	odu2 within an odu4 on a CFP or on the integrated transceiver	ODU2	Before 2.1.1
	UFM3	10ge on an SFP+ transceiver	odu2e within an odu4 on a CFP	ODU2e	4.5
	UFM6 ¹	10ge on a QSFP+ transceiver	odu2e within an odu4 on the integrated transceiver	ODU2e	4.1
OTU2 to/from OTU4	UFM3 UFM4	odu2 on an SFP+ transceiver	odu2 within an odu4 on a CFP or on the integrated transceiver	ODU2	Before 2.1.1
	UFM6 ¹	odu2 on a QSFP+ transceiver	odu2 within an odu4 on the integrated transceiver	ODU2	4.2
OTU2e to/from OTU4	UFM3	odu2e on an SFP+ transceiver	odu2e within an odu4 on a CFP or on the integrated transceiver	ODU2e	4.1
	UFM6 ¹	odu2e on a QSFP+ transceiver	odu2e within an odu4 on the integrated transceiver	ODU2e	4.2
SONET/SDH (OC-192/STM-64) to/from OTU4	UFM3 UFM4	oc192/stm64 on an SFP+ transceiver	odu2 within an odu4 on a CFP or on the integrated transceiver	ODU2	Before 2.1.1
	UFM6 ¹	oc192/stm64 on a QSFP+ transceiver	odu2 within an odu4 on the integrated transceiver	ODU2	4.2
SONET/SDH (10GbE WAN PHY) to/from OTU4	UFM3 UFM4	wanoc192/wanstm64 on an SFP+ transceiver	odu2 within an odu4 on a CFP or on the integrated transceiver	ODU2	Before 2.1.1
Fibre Channel to/from OTU4	UFM6 ¹	8gfc on a QSFP+ transceiver	odu2 within an odu4 on the integrated transceiver	ODU2	4.3
		10gfc on a QSFP+ transceiver	odu2e within an odu4 on the integrated transceiver	ODU2e	4.3
40GbE to/from OTU4	UFM6 ¹	40ge on a QSFP+ 40GE transceiver	odu3 within an odu4 on the integrated transceiver	ODU3	4.4

¹ UFM6 modules have fixed cross-connect mappings. See [Table 23 on page 125](#).

Table 23: UFM6 Fixed Cross-Connect Mappings

Description	Client Interface	Line Interface	Introduced in Release
100GbE to/from OTU4	100ge:chassis/slot/1/1	odu4:chassis/slot/2/1/1.1.1	4.1
	100ge:chassis/slot/1/2	odu4:chassis/slot/2/1/1.1.2	4.1
	100ge:chassis/slot/1/6	odu4:chassis/slot/2/1/2.1.1	4.1
	100ge:chassis/slot/1/7	odu4:chassis/slot/2/1/2.1.2	4.1
OTU4 to/from OTU4	odu4:chassis/slot/1/1	odu4:chassis/slot/2/1/1.1.1	4.3
	odu4:chassis/slot/1/2	odu4:chassis/slot/2/1/1.1.2	4.3
	odu4:chassis/slot/1/6	odu4:chassis/slot/2/1/2.1.1	4.3
	odu4:chassis/slot/1/7	odu4:chassis/slot/2/1/2.1.2	4.3

Table 23: UFM6 Fixed Cross-Connect Mappings (continued)

Description	Client Interface	Line Interface	Introduced in Release
10GbE/SONET/SDH/OTU2 to/from subinterface within OTU4	10ge:chassis/slot/1/1/1	odu2e:chassis/slot/2/1/1.1.1.1	4.1
	oc192:chassis/slot/1/1/1	odu2:chassis/slot/2/1/1.1.1.1	4.2
	stm64:chassis/slot/1/1/1	odu2:chassis/slot/2/1/1.1.1.1	4.2
	odu2:chassis/slot/1/1/1	odu2:chassis/slot/2/1/1.1.1.1	4.2
	odu2e:chassis/slot/1/1/1	odu2e:chassis/slot/2/1/1.1.1.1	4.2
	8gfc:chassis/slot/1/1/1	odu2:chassis/slot/2/1/1.1.1.1	4.3
	10gfc:chassis/slot/1/1/1	odu2e:chassis/slot/2/1/1.1.1.1	4.3
	10ge:chassis/slot/1/1/2	odu2e:chassis/slot/2/1/1.1.1.2	4.1
	oc192:chassis/slot/1/1/2	odu2:chassis/slot/2/1/1.1.1.2	4.2
	stm64:chassis/slot/1/1/2	odu2:chassis/slot/2/1/1.1.1.2	4.2
	odu2:chassis/slot/1/1/2	odu2:chassis/slot/2/1/1.1.1.2	4.2
	odu2e:chassis/slot/1/1/2	odu2e:chassis/slot/2/1/1.1.1.2	4.2
	8gfc:chassis/slot/1/1/2	odu2:chassis/slot/2/1/1.1.1.2	4.3
	10gfc:chassis/slot/1/1/2	odu2e:chassis/slot/2/1/1.1.1.2	4.3
	10ge:chassis/slot/1/1/3	odu2e:chassis/slot/2/1/1.1.1.3	4.1
	oc192:chassis/slot/1/1/3	odu2:chassis/slot/2/1/1.1.1.3	4.2
	stm64:chassis/slot/1/1/3	odu2:chassis/slot/2/1/1.1.1.3	4.2
	odu2:chassis/slot/1/1/3	odu2:chassis/slot/2/1/1.1.1.3	4.2
	odu2e:chassis/slot/1/1/3	odu2e:chassis/slot/2/1/1.1.1.3	4.2
	8gfc:chassis/slot/1/1/3	odu2:chassis/slot/2/1/1.1.1.3	4.3
	10gfc:chassis/slot/1/1/3	odu2e:chassis/slot/2/1/1.1.1.3	4.3
	10ge:chassis/slot/1/1/4	odu2e:chassis/slot/2/1/1.1.1.4	4.1
	oc192:chassis/slot/1/1/4	odu2:chassis/slot/2/1/1.1.1.4	4.2
	stm64:chassis/slot/1/1/4	odu2:chassis/slot/2/1/1.1.1.4	4.2
	odu2:chassis/slot/1/1/4	odu2:chassis/slot/2/1/1.1.1.4	4.2
	odu2e:chassis/slot/1/1/4	odu2e:chassis/slot/2/1/1.1.1.4	4.2
	8gfc:chassis/slot/1/1/4	odu2:chassis/slot/2/1/1.1.1.4	4.3
	10gfc:chassis/slot/1/1/4	odu2e:chassis/slot/2/1/1.1.1.4	4.3

Table 23: UFM6 Fixed Cross-Connect Mappings (continued)

Description	Client Interface	Line Interface	Introduced in Release
	10ge:chassis/slot/1/2/1	odu2e:chassis/slot/2/1/1.1.5	4.1
	oc192:chassis/slot/1/2/1	odu2:chassis/slot/2/1/1.1.5	4.2
	stm64:chassis/slot/1/2/1	odu2:chassis/slot/2/1/1.1.5	4.2
	odu2:chassis/slot/1/2/1	odu2:chassis/slot/2/1/1.1.5	4.2
	odu2e:chassis/slot/1/2/1	odu2e:chassis/slot/2/1/1.1.5	4.2
	8gfc:chassis/slot/1/2/1	odu2:chassis/slot/2/1/1.1.5	4.3
	10gfc:chassis/slot/1/2/1	odu2e:chassis/slot/2/1/1.1.5	4.3
	10ge:chassis/slot/1/2/2	odu2e:chassis/slot/2/1/1.1.6	4.1
	oc192:chassis/slot/1/2/2	odu2:chassis/slot/2/1/1.1.6	4.2
	stm64:chassis/slot/1/2/2	odu2:chassis/slot/2/1/1.1.6	4.2
	odu2:chassis/slot/1/2/2	odu2:chassis/slot/2/1/1.1.6	4.2
	odu2e:chassis/slot/1/2/2	odu2e:chassis/slot/2/1/1.1.6	4.2
	8gfc:chassis/slot/1/2/2	odu2:chassis/slot/2/1/1.1.6	4.3
	10gfc:chassis/slot/1/2/2	odu2e:chassis/slot/2/1/1.1.6	4.3
	10ge:chassis/slot/1/2/3	odu2e:chassis/slot/2/1/1.1.7	4.1
	oc192:chassis/slot/1/2/3	odu2:chassis/slot/2/1/1.1.7	4.2
	stm64:chassis/slot/1/2/3	odu2:chassis/slot/2/1/1.1.7	4.2
	odu2:chassis/slot/1/2/3	odu2:chassis/slot/2/1/1.1.7	4.2
	odu2e:chassis/slot/1/2/3	odu2e:chassis/slot/2/1/1.1.7	4.2
	8gfc:chassis/slot/1/2/3	odu2:chassis/slot/2/1/1.1.7	4.3
	10gfc:chassis/slot/1/2/3	odu2e:chassis/slot/2/1/1.1.7	4.3
	10ge:chassis/slot/1/2/4	odu2e:chassis/slot/2/1/1.1.8	4.1
	oc192:chassis/slot/1/2/4	odu2:chassis/slot/2/1/1.1.8	4.2
	stm64:chassis/slot/1/2/4	odu2:chassis/slot/2/1/1.1.8	4.2
	odu2:chassis/slot/1/2/4	odu2:chassis/slot/2/1/1.1.8	4.2
	odu2e:chassis/slot/1/2/4	odu2e:chassis/slot/2/1/1.1.8	4.2
	8gfc:chassis/slot/1/2/4	odu2:chassis/slot/2/1/1.1.8	4.3
	10gfc:chassis/slot/1/2/4	odu2e:chassis/slot/2/1/1.1.8	4.3

Table 23: UFM6 Fixed Cross-Connect Mappings (continued)

Description	Client Interface	Line Interface	Introduced in Release
	10ge:chassis/slot/1/3/1	odu2e:chassis/slot/2/1/1.1.1.9	4.1
	oc192:chassis/slot/1/3/1	odu2:chassis/slot/2/1/1.1.1.9	4.2
	stm64:chassis/slot/1/3/1	odu2:chassis/slot/2/1/1.1.1.9	4.2
	odu2:chassis/slot/1/3/1	odu2:chassis/slot/2/1/1.1.1.9	4.2
	odu2e:chassis/slot/1/3/1	odu2e:chassis/slot/2/1/1.1.1.9	4.2
	8gfc:chassis/slot/1/3/1	odu2:chassis/slot/2/1/1.1.1.9	4.3
	10gfc:chassis/slot/1/3/1	odu2e:chassis/slot/2/1/1.1.1.9	4.3
	10ge:chassis/slot/1/3/2	odu2e:chassis/slot/2/1/1.1.1.10	4.1
	oc192:chassis/slot/1/3/2	odu2:chassis/slot/2/1/1.1.1.10	4.2
	stm64:chassis/slot/1/3/2	odu2:chassis/slot/2/1/1.1.1.10	4.2
	odu2:chassis/slot/1/3/2	odu2:chassis/slot/2/1/1.1.1.10	4.2
	odu2e:chassis/slot/1/3/2	odu2e:chassis/slot/2/1/1.1.1.10	4.2
	8gfc:chassis/slot/1/3/2	odu2:chassis/slot/2/1/1.1.1.10	4.3
	10gfc:chassis/slot/1/3/2	odu2e:chassis/slot/2/1/1.1.1.10	4.3
	10ge:chassis/slot/1/3/3	odu2e:chassis/slot/2/1/1.1.2.1	4.1
	oc192:chassis/slot/1/3/3	odu2:chassis/slot/2/1/1.1.2.1	4.2
	stm64:chassis/slot/1/3/3	odu2:chassis/slot/2/1/1.1.2.1	4.2
	odu2:chassis/slot/1/3/3	odu2:chassis/slot/2/1/1.1.2.1	4.2
	odu2e:chassis/slot/1/3/3	odu2e:chassis/slot/2/1/1.1.2.1	4.2
	8gfc:chassis/slot/1/3/3	odu2:chassis/slot/2/1/1.1.2.1	4.3
	10gfc:chassis/slot/1/3/3	odu2e:chassis/slot/2/1/1.1.2.1	4.3
	10ge:chassis/slot/1/3/4	odu2e:chassis/slot/2/1/1.1.2.2	4.1
	oc192:chassis/slot/1/3/4	odu2:chassis/slot/2/1/1.1.2.2	4.2
	stm64:chassis/slot/1/3/4	odu2:chassis/slot/2/1/1.1.2.2	4.2
	odu2:chassis/slot/1/3/4	odu2:chassis/slot/2/1/1.1.2.2	4.2
	odu2e:chassis/slot/1/3/4	odu2e:chassis/slot/2/1/1.1.2.2	4.2
	8gfc:chassis/slot/1/3/4	odu2:chassis/slot/2/1/1.1.2.2	4.3
	10gfc:chassis/slot/1/3/4	odu2e:chassis/slot/2/1/1.1.2.2	4.3

Table 23: UFM6 Fixed Cross-Connect Mappings (continued)

Description	Client Interface	Line Interface	Introduced in Release
	10ge:chassis/slot/1/4/1	odu2e:chassis/slot/2/1/1.1.2.3	4.1
	oc192:chassis/slot/1/4/1	odu2:chassis/slot/2/1/1.1.2.3	4.2
	stm64:chassis/slot/1/4/1	odu2:chassis/slot/2/1/1.1.2.3	4.2
	odu2:chassis/slot/1/4/1	odu2:chassis/slot/2/1/1.1.2.3	4.2
	odu2e:chassis/slot/1/4/1	odu2e:chassis/slot/2/1/1.1.2.3	4.2
	8gfc:chassis/slot/1/4/1	odu2:chassis/slot/2/1/1.1.2.3	4.3
	10gfc:chassis/slot/1/4/1	odu2e:chassis/slot/2/1/1.1.2.3	4.3
	10ge:chassis/slot/1/4/2	odu2e:chassis/slot/2/1/1.1.2.4	4.1
	oc192:chassis/slot/1/4/2	odu2:chassis/slot/2/1/1.1.2.4	4.2
	stm64:chassis/slot/1/4/2	odu2:chassis/slot/2/1/1.1.2.4	4.2
	odu2:chassis/slot/1/4/2	odu2:chassis/slot/2/1/1.1.2.4	4.2
	odu2e:chassis/slot/1/4/2	odu2e:chassis/slot/2/1/1.1.2.4	4.2
	8gfc:chassis/slot/1/4/2	odu2:chassis/slot/2/1/1.1.2.4	4.3
	10gfc:chassis/slot/1/4/2	odu2e:chassis/slot/2/1/1.1.2.4	4.3
	10ge:chassis/slot/1/4/3	odu2e:chassis/slot/2/1/1.1.2.5	4.1
	oc192:chassis/slot/1/4/3	odu2:chassis/slot/2/1/1.1.2.5	4.2
	stm64:chassis/slot/1/4/3	odu2:chassis/slot/2/1/1.1.2.5	4.2
	odu2:chassis/slot/1/4/3	odu2:chassis/slot/2/1/1.1.2.5	4.2
	odu2e:chassis/slot/1/4/3	odu2e:chassis/slot/2/1/1.1.2.5	4.2
	8gfc:chassis/slot/1/4/3	odu2:chassis/slot/2/1/1.1.2.5	4.3
	10gfc:chassis/slot/1/4/3	odu2e:chassis/slot/2/1/1.1.2.5	4.3
	10ge:chassis/slot/1/4/4	odu2e:chassis/slot/2/1/1.1.2.6	4.1
	oc192:chassis/slot/1/4/4	odu2:chassis/slot/2/1/1.1.2.6	4.2
	stm64:chassis/slot/1/4/4	odu2:chassis/slot/2/1/1.1.2.6	4.2
	odu2:chassis/slot/1/4/4	odu2:chassis/slot/2/1/1.1.2.6	4.2
	odu2e:chassis/slot/1/4/4	odu2e:chassis/slot/2/1/1.1.2.6	4.2
	8gfc:chassis/slot/1/4/4	odu2:chassis/slot/2/1/1.1.2.6	4.3
	10gfc:chassis/slot/1/4/4	odu2e:chassis/slot/2/1/1.1.2.6	4.3

Table 23: UFM6 Fixed Cross-Connect Mappings (continued)

Description	Client Interface	Line Interface	Introduced in Release
	10ge:chassis/slot/1/5/1	odu2e:chassis/slot/2/1/1.1.2.7	4.1
	oc192:chassis/slot/1/5/1	odu2:chassis/slot/2/1/1.1.2.7	4.2
	stm64:chassis/slot/1/5/1	odu2:chassis/slot/2/1/1.1.2.7	4.2
	odu2:chassis/slot/1/5/1	odu2:chassis/slot/2/1/1.1.2.7	4.2
	odu2e:chassis/slot/1/5/1	odu2e:chassis/slot/2/1/1.1.2.7	4.2
	8gfc:chassis/slot/1/5/1	odu2:chassis/slot/2/1/1.1.2.7	4.3
	10gfc:chassis/slot/1/5/1	odu2e:chassis/slot/2/1/1.1.2.7	4.3
	10ge:chassis/slot/1/5/2	odu2e:chassis/slot/2/1/1.1.2.8	4.1
	oc192:chassis/slot/1/5/2	odu2:chassis/slot/2/1/1.1.2.8	4.2
	stm64:chassis/slot/1/5/2	odu2:chassis/slot/2/1/1.1.2.8	4.2
	odu2:chassis/slot/1/5/2	odu2:chassis/slot/2/1/1.1.2.8	4.2
	odu2e:chassis/slot/1/5/2	odu2e:chassis/slot/2/1/1.1.2.8	4.2
	8gfc:chassis/slot/1/5/2	odu2:chassis/slot/2/1/1.1.2.8	4.3
	10gfc:chassis/slot/1/5/2	odu2e:chassis/slot/2/1/1.1.2.8	4.3
	10ge:chassis/slot/1/5/3	odu2e:chassis/slot/2/1/1.1.2.9	4.1
	oc192:chassis/slot/1/5/3	odu2:chassis/slot/2/1/1.1.2.9	4.2
	stm64:chassis/slot/1/5/3	odu2:chassis/slot/2/1/1.1.2.9	4.2
	odu2:chassis/slot/1/5/3	odu2:chassis/slot/2/1/1.1.2.9	4.2
	odu2e:chassis/slot/1/5/3	odu2e:chassis/slot/2/1/1.1.2.9	4.2
	8gfc:chassis/slot/1/5/3	odu2:chassis/slot/2/1/1.1.2.9	4.3
	10gfc:chassis/slot/1/5/3	odu2e:chassis/slot/2/1/1.1.2.9	4.3
	10ge:chassis/slot/1/5/4	odu2e:chassis/slot/2/1/1.1.2.10	4.1
	oc192:chassis/slot/1/5/4	odu2:chassis/slot/2/1/1.1.2.10	4.2
	stm64:chassis/slot/1/5/4	odu2:chassis/slot/2/1/1.1.2.10	4.2
	odu2:chassis/slot/1/5/4	odu2:chassis/slot/2/1/1.1.2.10	4.2
	odu2e:chassis/slot/1/5/4	odu2e:chassis/slot/2/1/1.1.2.10	4.2
	8gfc:chassis/slot/1/5/4	odu2:chassis/slot/2/1/1.1.2.10	4.3
	10gfc:chassis/slot/1/5/4	odu2e:chassis/slot/2/1/1.1.2.10	4.3

Table 23: UFM6 Fixed Cross-Connect Mappings (continued)

Description	Client Interface	Line Interface	Introduced in Release
	10ge:chassis/slot/1/6/1	odu2e:chassis/slot/2/1/2.1.1.1	4.1
	oc192:chassis/slot/1/6/1	odu2:chassis/slot/2/1/2.1.1.1	4.2
	stm64:chassis/slot/1/6/1	odu2:chassis/slot/2/1/2.1.1.1	4.2
	odu2:chassis/slot/1/6/1	odu2:chassis/slot/2/1/2.1.1.1	4.2
	odu2e:chassis/slot/1/6/1	odu2e:chassis/slot/2/1/2.1.1.1	4.2
	8gfc:chassis/slot/1/6/1	odu2:chassis/slot/2/1/2.1.1.1	4.3
	10gfc:chassis/slot/1/6/1	odu2e:chassis/slot/2/1/2.1.1.1	4.3
	10ge:chassis/slot/1/6/2	odu2e:chassis/slot/2/1/2.1.1.2	4.1
	oc192:chassis/slot/1/6/2	odu2:chassis/slot/2/1/2.1.1.2	4.2
	stm64:chassis/slot/1/6/2	odu2:chassis/slot/2/1/2.1.1.2	4.2
	odu2:chassis/slot/1/6/2	odu2:chassis/slot/2/1/2.1.1.2	4.2
	odu2e:chassis/slot/1/6/2	odu2e:chassis/slot/2/1/2.1.1.2	4.2
	8gfc:chassis/slot/1/6/2	odu2:chassis/slot/2/1/2.1.1.2	4.3
	10gfc:chassis/slot/1/6/2	odu2e:chassis/slot/2/1/2.1.1.2	4.3
	10ge:chassis/slot/1/6/3	odu2e:chassis/slot/2/1/2.1.1.3	4.1
	oc192:chassis/slot/1/6/3	odu2:chassis/slot/2/1/2.1.1.3	4.2
	stm64:chassis/slot/1/6/3	odu2:chassis/slot/2/1/2.1.1.3	4.2
	odu2:chassis/slot/1/6/3	odu2:chassis/slot/2/1/2.1.1.3	4.2
	odu2e:chassis/slot/1/6/3	odu2e:chassis/slot/2/1/2.1.1.3	4.2
	8gfc:chassis/slot/1/6/3	odu2:chassis/slot/2/1/2.1.1.3	4.3
	10gfc:chassis/slot/1/6/3	odu2e:chassis/slot/2/1/2.1.1.3	4.3
	10ge:chassis/slot/1/6/4	odu2e:chassis/slot/2/1/2.1.1.4	4.1
	oc192:chassis/slot/1/6/4	odu2:chassis/slot/2/1/2.1.1.4	4.2
	stm64:chassis/slot/1/6/4	odu2:chassis/slot/2/1/2.1.1.4	4.2
	odu2:chassis/slot/1/6/4	odu2:chassis/slot/2/1/2.1.1.4	4.2
	odu2e:chassis/slot/1/6/4	odu2e:chassis/slot/2/1/2.1.1.4	4.2
	8gfc:chassis/slot/1/6/4	odu2:chassis/slot/2/1/2.1.1.4	4.3
	10gfc:chassis/slot/1/6/4	odu2e:chassis/slot/2/1/2.1.1.4	4.3

Table 23: UFM6 Fixed Cross-Connect Mappings (continued)

Description	Client Interface	Line Interface	Introduced in Release
	10ge:chassis/slot/1/7/1	odu2e:chassis/slot/2/1/2.1.1.5	4.1
	oc192:chassis/slot/1/7/1	odu2:chassis/slot/2/1/2.1.1.5	4.2
	stm64:chassis/slot/1/7/1	odu2:chassis/slot/2/1/2.1.1.5	4.2
	odu2:chassis/slot/1/7/1	odu2:chassis/slot/2/1/2.1.1.5	4.2
	odu2e:chassis/slot/1/7/1	odu2e:chassis/slot/2/1/2.1.1.5	4.2
	8gfc:chassis/slot/1/7/1	odu2:chassis/slot/2/1/2.1.1.5	4.3
	10gfc:chassis/slot/1/7/1	odu2e:chassis/slot/2/1/2.1.1.5	4.3
	10ge:chassis/slot/1/7/2	odu2e:chassis/slot/2/1/2.1.1.6	4.1
	oc192:chassis/slot/1/7/2	odu2:chassis/slot/2/1/2.1.1.6	4.2
	stm64:chassis/slot/1/7/2	odu2:chassis/slot/2/1/2.1.1.6	4.2
	odu2:chassis/slot/1/7/2	odu2:chassis/slot/2/1/2.1.1.6	4.2
	odu2e:chassis/slot/1/7/2	odu2e:chassis/slot/2/1/2.1.1.6	4.2
	8gfc:chassis/slot/1/7/2	odu2:chassis/slot/2/1/2.1.1.6	4.3
	10gfc:chassis/slot/1/7/2	odu2e:chassis/slot/2/1/2.1.1.6	4.3
	10ge:chassis/slot/1/7/3	odu2e:chassis/slot/2/1/2.1.1.7	4.1
	oc192:chassis/slot/1/7/3	odu2:chassis/slot/2/1/2.1.1.7	4.2
	stm64:chassis/slot/1/7/3	odu2:chassis/slot/2/1/2.1.1.7	4.2
	odu2:chassis/slot/1/7/3	odu2:chassis/slot/2/1/2.1.1.7	4.2
	odu2e:chassis/slot/1/7/3	odu2e:chassis/slot/2/1/2.1.1.7	4.2
	8gfc:chassis/slot/1/7/3	odu2:chassis/slot/2/1/2.1.1.7	4.3
	10gfc:chassis/slot/1/7/3	odu2e:chassis/slot/2/1/2.1.1.7	4.3
	10ge:chassis/slot/1/7/4	odu2e:chassis/slot/2/1/2.1.1.8	4.1
	oc192:chassis/slot/1/7/4	odu2:chassis/slot/2/1/2.1.1.8	4.2
	stm64:chassis/slot/1/7/4	odu2:chassis/slot/2/1/2.1.1.8	4.2
	odu2:chassis/slot/1/7/4	odu2:chassis/slot/2/1/2.1.1.8	4.2
	odu2e:chassis/slot/1/7/4	odu2e:chassis/slot/2/1/2.1.1.8	4.2
	8gfc:chassis/slot/1/7/4	odu2:chassis/slot/2/1/2.1.1.8	4.3
	10gfc:chassis/slot/1/7/4	odu2e:chassis/slot/2/1/2.1.1.8	4.3

Table 23: UFM6 Fixed Cross-Connect Mappings (continued)

Description	Client Interface	Line Interface	Introduced in Release
	10ge:chassis/slot/1/8/1	odu2e:chassis/slot/2/1/2.1.1.9	4.1
	oc192:chassis/slot/1/8/1	odu2:chassis/slot/2/1/2.1.1.9	4.2
	stm64:chassis/slot/1/8/1	odu2:chassis/slot/2/1/2.1.1.9	4.2
	odu2:chassis/slot/1/8/1	odu2:chassis/slot/2/1/2.1.1.9	4.2
	odu2e:chassis/slot/1/8/1	odu2e:chassis/slot/2/1/2.1.1.9	4.2
	8gfc:chassis/slot/1/8/1	odu2:chassis/slot/2/1/2.1.1.9	4.3
	10gfc:chassis/slot/1/8/1	odu2e:chassis/slot/2/1/2.1.1.9	4.3
	10ge:chassis/slot/1/8/2	odu2e:chassis/slot/2/1/2.1.1.10	4.1
	oc192:chassis/slot/1/8/2	odu2:chassis/slot/2/1/2.1.1.10	4.2
	stm64:chassis/slot/1/8/2	odu2:chassis/slot/2/1/2.1.1.10	4.2
	odu2:chassis/slot/1/8/2	odu2:chassis/slot/2/1/2.1.1.10	4.2
	odu2e:chassis/slot/1/8/2	odu2e:chassis/slot/2/1/2.1.1.10	4.2
	8gfc:chassis/slot/1/8/2	odu2:chassis/slot/2/1/2.1.1.10	4.3
	10gfc:chassis/slot/1/8/2	odu2e:chassis/slot/2/1/2.1.1.10	4.3
	10ge:chassis/slot/1/8/3	odu2e:chassis/slot/2/1/2.1.2.1	4.1
	oc192:chassis/slot/1/8/3	odu2:chassis/slot/2/1/2.1.2.1	4.2
	stm64:chassis/slot/1/8/3	odu2:chassis/slot/2/1/2.1.2.1	4.2
	odu2:chassis/slot/1/8/3	odu2:chassis/slot/2/1/2.1.2.1	4.2
	odu2e:chassis/slot/1/8/3	odu2e:chassis/slot/2/1/2.1.2.1	4.2
	8gfc:chassis/slot/1/8/3	odu2:chassis/slot/2/1/2.1.2.1	4.3
	10gfc:chassis/slot/1/8/3	odu2e:chassis/slot/2/1/2.1.2.1	4.3
	10ge:chassis/slot/1/8/4	odu2e:chassis/slot/2/1/2.1.2.2	4.1
	oc192:chassis/slot/1/8/4	odu2:chassis/slot/2/1/2.1.2.2	4.2
	stm64:chassis/slot/1/8/4	odu2:chassis/slot/2/1/2.1.2.2	4.2
	odu2:chassis/slot/1/8/4	odu2:chassis/slot/2/1/2.1.2.2	4.2
	odu2e:chassis/slot/1/8/4	odu2e:chassis/slot/2/1/2.1.2.2	4.2
	8gfc:chassis/slot/1/8/4	odu2:chassis/slot/2/1/2.1.2.2	4.3
	10gfc:chassis/slot/1/8/4	odu2e:chassis/slot/2/1/2.1.2.2	4.3

Table 23: UFM6 Fixed Cross-Connect Mappings (continued)

Description	Client Interface	Line Interface	Introduced in Release
	10ge:chassis/slot/1/9/1	odu2e:chassis/slot/2/1/2.1.2.3	4.1
	oc192:chassis/slot/1/9/1	odu2:chassis/slot/2/1/2.1.2.3	4.2
	stm64:chassis/slot/1/9/1	odu2:chassis/slot/2/1/2.1.2.3	4.2
	odu2:chassis/slot/1/9/1	odu2:chassis/slot/2/1/2.1.2.3	4.2
	odu2e:chassis/slot/1/9/1	odu2e:chassis/slot/2/1/2.1.2.3	4.2
	8gfc:chassis/slot/1/9/1	odu2:chassis/slot/2/1/2.1.2.3	4.3
	10gfc:chassis/slot/1/9/1	odu2e:chassis/slot/2/1/2.1.2.3	4.3
	10ge:chassis/slot/1/9/2	odu2e:chassis/slot/2/1/2.1.2.4	4.1
	oc192:chassis/slot/1/9/2	odu2:chassis/slot/2/1/2.1.2.4	4.2
	stm64:chassis/slot/1/9/2	odu2:chassis/slot/2/1/2.1.2.4	4.2
	odu2:chassis/slot/1/9/2	odu2:chassis/slot/2/1/2.1.2.4	4.2
	odu2e:chassis/slot/1/9/2	odu2e:chassis/slot/2/1/2.1.2.4	4.2
	8gfc:chassis/slot/1/9/2	odu2:chassis/slot/2/1/2.1.2.4	4.3
	10gfc:chassis/slot/1/9/2	odu2e:chassis/slot/2/1/2.1.2.4	4.3
	10ge:chassis/slot/1/9/3	odu2e:chassis/slot/2/1/2.1.2.5	4.1
	oc192:chassis/slot/1/9/3	odu2:chassis/slot/2/1/2.1.2.5	4.2
	stm64:chassis/slot/1/9/3	odu2:chassis/slot/2/1/2.1.2.5	4.2
	odu2:chassis/slot/1/9/3	odu2:chassis/slot/2/1/2.1.2.5	4.2
	odu2e:chassis/slot/1/9/3	odu2e:chassis/slot/2/1/2.1.2.5	4.2
	8gfc:chassis/slot/1/9/3	odu2:chassis/slot/2/1/2.1.2.5	4.3
	10gfc:chassis/slot/1/9/3	odu2e:chassis/slot/2/1/2.1.2.5	4.3
	10ge:chassis/slot/1/9/4	odu2e:chassis/slot/2/1/2.1.2.6	4.1
	oc192:chassis/slot/1/9/4	odu2:chassis/slot/2/1/2.1.2.6	4.2
	stm64:chassis/slot/1/9/4	odu2:chassis/slot/2/1/2.1.2.6	4.2
	odu2:chassis/slot/1/9/4	odu2:chassis/slot/2/1/2.1.2.6	4.2
	odu2e:chassis/slot/1/9/4	odu2e:chassis/slot/2/1/2.1.2.6	4.2
	8gfc:chassis/slot/1/9/4	odu2:chassis/slot/2/1/2.1.2.6	4.3
	10gfc:chassis/slot/1/9/4	odu2e:chassis/slot/2/1/2.1.2.6	4.3

Table 23: UFM6 Fixed Cross-Connect Mappings (continued)

Description	Client Interface	Line Interface	Introduced in Release
	10ge:chassis/slot/1/10/1	odu2e:chassis/slot/2/1/2.1.2.7	4.1
	oc192:chassis/slot/1/10/1	odu2:chassis/slot/2/1/2.1.2.7	4.2
	stm64:chassis/slot/1/10/1	odu2:chassis/slot/2/1/2.1.2.7	4.2
	odu2:chassis/slot/1/10/1	odu2:chassis/slot/2/1/2.1.2.7	4.2
	odu2e:chassis/slot/1/10/1	odu2e:chassis/slot/2/1/2.1.2.7	4.2
	8gfc:chassis/slot/1/10/1	odu2:chassis/slot/2/1/2.1.2.7	4.3
	10gfc:chassis/slot/1/10/1	odu2e:chassis/slot/2/1/2.1.2.7	4.3
	10ge:chassis/slot/1/10/2	odu2e:chassis/slot/2/1/2.1.2.8	4.1
	oc192:chassis/slot/1/10/2	odu2:chassis/slot/2/1/2.1.2.8	4.2
	stm64:chassis/slot/1/10/2	odu2:chassis/slot/2/1/2.1.2.8	4.2
	odu2:chassis/slot/1/10/2	odu2:chassis/slot/2/1/2.1.2.8	4.2
	odu2e:chassis/slot/1/10/2	odu2e:chassis/slot/2/1/2.1.2.8	4.2
	8gfc:chassis/slot/1/10/2	odu2:chassis/slot/2/1/2.1.2.8	4.3
	10gfc:chassis/slot/1/10/2	odu2e:chassis/slot/2/1/2.1.2.8	4.3
	10ge:chassis/slot/1/10/3	odu2e:chassis/slot/2/1/2.1.2.9	4.1
	oc192:chassis/slot/1/10/3	odu2:chassis/slot/2/1/2.1.2.9	4.2
	stm64:chassis/slot/1/10/3	odu2:chassis/slot/2/1/2.1.2.9	4.2
	odu2:chassis/slot/1/10/3	odu2:chassis/slot/2/1/2.1.2.9	4.2
	odu2e:chassis/slot/1/10/3	odu2e:chassis/slot/2/1/2.1.2.9	4.2
	8gfc:chassis/slot/1/10/3	odu2:chassis/slot/2/1/2.1.2.9	4.3
	10gfc:chassis/slot/1/10/3	odu2e:chassis/slot/2/1/2.1.2.9	4.3
	10ge:chassis/slot/1/10/4	odu2e:chassis/slot/2/1/2.1.2.10	4.1
	oc192:chassis/slot/1/10/4	odu2:chassis/slot/2/1/2.1.2.10	4.2
	stm64:chassis/slot/1/10/4	odu2:chassis/slot/2/1/2.1.2.10	4.2
	odu2:chassis/slot/1/10/4	odu2:chassis/slot/2/1/2.1.2.10	4.2
	odu2e:chassis/slot/1/10/4	odu2e:chassis/slot/2/1/2.1.2.10	4.2
	8gfc:chassis/slot/1/10/4	odu2:chassis/slot/2/1/2.1.2.10	4.3
	10gfc:chassis/slot/1/10/4	odu2e:chassis/slot/2/1/2.1.2.10	4.3

Table 23: UFM6 Fixed Cross-Connect Mappings (continued)

Description	Client Interface	Line Interface	Introduced in Release
40GbE to/from subinterface within OTU4	40ge:chassis/slot/1/1	odu3:chassis/slot/2/1/1.1.1	4.4
	40ge:chassis/slot/1/2	odu3:chassis/slot/2/1/1.1.2	4.4
	40ge:chassis/slot/1/4	odu3:chassis/slot/2/1/1.1.2.1	4.4
	40ge:chassis/slot/1/5	odu3:chassis/slot/2/1/1.1.2.2	4.4
	40ge:chassis/slot/1/6	odu3:chassis/slot/2/1/2.1.1	4.4
	40ge:chassis/slot/1/7	odu3:chassis/slot/2/1/2.1.2	4.4
	40ge:chassis/slot/1/9	odu3:chassis/slot/2/1/2.1.2.1	4.4
	40ge:chassis/slot/1/10	odu3:chassis/slot/2/1/2.1.2.2	4.4

Provisioning a Transponding Cross-Connect on a UFM3 or UFM4

Use this procedure to provision a cross-connect that transponds between interfaces on a UFM3 or UFM4. This procedure transponds a 100-Gigabit Ethernet signal into an ODU4 as an example, but the same procedure can be used for other protocols. See [“Supported Cross-Connects” on page 122](#) for more information on what interfaces can be cross-connected.

1. Enter configuration mode.

```
bti7800# config
bti7800(config)#
```

2. Create the interfaces to be cross-connected. The following example shows the creation of a 100-Gigabit Ethernet interface and an ODU4 interface.

See [“Provisioning a Transport Interface” on page 116](#) for information on creating transport interfaces.

- a. Create the OTU4 interface. For example:

```
bti7800(config)# interface otu4:1/7/1/1
Value for 'type' [ethernetCsmacd,opticalChannel,otnOdu,otnOtu,...]: otnOtu
bti7800(config-interface-otu4:1/7/1/1)# frequency 193.1
bti7800(config-interface-otu4:1/7/1/1)# commit
Commit complete.
```

When you create an OTU4 interface on a UFM3 or UFM4, the system automatically creates the corresponding ODU4 interface and configures it for no multiplexing.

If you are cross-connecting an existing ODU4 interface that has been configured for multiplexing, you will need to change it to no multiplexing. For example:

```

bti7800(config)# interface odu4:1/7/1/1
bti7800(config-interface-odu4:1/7/1/1)# multiplex-mode no-multiplex
bti7800(config-interface-odu4:1/7/1/1)# commit
Commit complete.

```

- b. Create the 100-Gigabit Ethernet interface. For example:

```

bti7800(config)# interface 100ge:1/7/2/1
Value for 'type' [ethernetCsmacd,opticalChannel,otnOdu,otnOtu,...]:
ethernetCsmacd
bti7800(config-interface-100ge:1/7/2/1)# commit
Commit complete.

```

The following lists the interfaces created on the UFM in slot 7 (for example):

```

bti7800(config)# do show interface | include 1/7

```

Name	: 100ge:1/7/2/1
Name	: odu4:1/7/1/1
Name	: otu4:1/7/1/1

3. Configure the cross-connect.

The following example cross-connects the 100-Gigabit Ethernet interface with the ODU4 interface:

```

bti7800(config)# cross-connect 100ge:1/7/2/1 odu4:1/7/1/1
bti7800(config-cross-connect-100ge:1/7/2/1/odu4:1/7/1/1)#

```

4. Optionally, specify the service name.

For example:

```

bti7800(config-cross-connect-100ge:1/7/2/1/odu4:1/7/1/1)# service-name
circuit_17

```

5. Apply the changes.

```

bti7800(config-cross-connect-100ge:1/7/2/1/odu4:1/7/1/1)# commit
Commit complete.

```

6. Optionally, show the resulting cross-connect.

For example:

```

bti7800(config-cross-connect-100ge:1/7/2/1/odu4:1/7/1/1)# do show cross-connect
table | include circuit_17

```

2	100ge:1/7/2/1	odu4:1/7/1/1	2way	odu4	circuit_17
---	---------------	--------------	------	------	------------

Provisioning a Transponding Cross-Connect on a UFM6

Use this procedure to provision a cross-connect that transponds between a 100-Gbps client interface and an OTU4 line interface on a UFM6. This procedure transponds a 100-Gigabit Ethernet signal into an ODU4 as an example. See [“Supported Cross-Connects” on page 122](#) for more information on what interfaces can be cross-connected.

1. Enter configuration mode.

```
bti7800# config
bti7800(config)#
```

2. Create the interfaces to be cross-connected. See [“Provisioning a Transport Interface” on page 116](#) for information on creating transport interfaces.



NOTE: The cross-connect mapping between the client and line interfaces on a UFM6 is fixed and cannot be changed. Ensure that the interfaces you create conform to the required mapping. See [“Supported Cross-Connects” on page 122](#) for more information.

- a. Create the optical channel interface. For example:

```
bti7800(config)# interface och:1/5/2/1/1.1
Value for 'type' [ethernetCsmacd, opticalChannel, otnOdu, otnOtu, ...]:
opticalChannel
bti7800(config-interface-och:1/5/2/1/1.1)# frequency 192.1
bti7800(config-interface-och:1/5/2/1/1.1)# commit
Commit complete.
```

The optical channel represents the optical signal and contains attributes that are shared by all contained OTU4 signals. The optical channel interface must exist before you can create an OTU4 interface. For more information on creating an optical channel interface, see [“Provisioning an Optical Channel Interface” on page 120](#).

- b. Create the OTU4 interface and configure it as a non-multiplexed interface. When you create an OTU4 line interface on a UFM6, the system automatically creates the corresponding ODU4 interface and configures it for multiplexing. You will need to manually configure the ODU4 for non-multiplexing. For example:

```
bti7800(config)# interface otu4:1/5/2/1/1.1
Value for 'type' [ethernetCsmacd, opticalChannel, otnOdu, otnOtu, ...]: otnOtu
bti7800(config-interface-otu4:1/5/2/1/1.1)# commit
Commit complete.
bti7800(config-interface-otu4:1/5/2/1/1.1)# exit
bti7800(config)# interface odu4:1/5/2/1/1.1
bti7800(config-interface-odu4:1/5/2/1/1.1)# multiplex-mode no-multiplex
bti7800(config-interface-odu4:1/5/2/1/1.1)# commit
Commit complete.
```

- c. Create the 100-Gbps client interface. For example:

```
bti7800(config)# interface 100ge:1/5/1/1
Value for 'type' [ethernetCsmacd,opticalChannel,otnOdu,otnOtu,...]:
ethernetCsmacd
bti7800(config-interface-100ge:1/5/1/1)# commit
Commit complete.
```

The following lists the interfaces created on the UFM6 in slot 5 (for example):

```
bti7800(config)# do show interface | include 1/5

Name                : 100ge:1/5/1/1
Name                : odu4:1/5/2/1/1.1.1
Name                : otu4:1/5/2/1/1.1.1
Name                : och:1/5/2/1/1.1
```

3. Configure the cross-connect.

The following cross-connects the ODU4 line interface with the 100-Gbps client interface:

```
bti7800(config)# cross-connect odu4:1/5/2/1/1.1.1 100ge:1/5/1/1
bti7800(config-cross-connect-odu4:1/5/2/1/1.1.1 100ge:1/5/1/1)#
```

4. Optionally, specify the service name.

For example:

```
bti7800(config-cross-connect-odu4:1/5/2/1/1.1.1 100ge:1/5/1/1)# service-name
circuit_2129
```

5. Apply the changes.

```
bti7800(config-cross-connect-odu4:1/5/2/1/1.1.1 100ge:1/5/1/1)# commit
Commit complete.
```

6. Optionally, show the resulting cross-connect.

For example:

```
bti7800(config-cross-connect-odu4:1/5/2/1/1.1.1 100ge:1/5/1/1)# do show
cross-connect table
```

Cross-Connect	Source-Name	Destination-Name	Direction	Rate
1	odu4:1/5/2/1/1.1.1	100ge:1/5/1/1	2way	odu4

Provisioning a Muxponding Cross-Connect on a UFM3 or UFM4

Use this procedure to provision a cross-connect that muxponds between a 10-Gbps interface and a 10-Gbps subinterface within a higher-order ODU4 on a UFM3 or UFM4.

This procedure muxponds a 10-Gigabit Ethernet signal into an ODU2 as an example, but the same procedure can be used for other 10-Gbps protocols by cross-connecting other interfaces. See [“Supported Cross-Connects” on page 122](#) for information on the cross-connects these modules support.

1. Enter configuration mode.

```
bti7800# config
bti7800(config)#
```

2. Create the interfaces to be cross-connected. See [“Provisioning a Transport Interface” on page 116](#) for information on creating transport interfaces.

- a. Create the OTU4 interface and configure the automatically created ODU4 interface for multiplexing. For example:

```
bti7800(config)# interface otu4:1/7/1/1
Value for 'type' [ethernetCsmacd,opticalChannel,otnOdu,otnOtu,...]: otnOtu
bti7800(config-interface-otu4:1/7/1/1)# frequency 193.1
bti7800(config-interface-otu4:1/7/1/1)# commit
Commit complete.
bti7800(config-interface-otu4:1/7/1/1)# exit
bti7800(config)# interface odu4:1/7/1/1
bti7800(config-interface-odu4:1/7/1/1)# multiplex-mode gmp-capable
bti7800(config-interface-odu4:1/7/1/1)# commit
Commit complete.
```

When you configure the ODU4 interface for multiplexing, the system automatically creates 10 ODU2 subinterfaces; for example, odu2:1/7/1/1.1 to odu2:1/7/1/1.10.

- b. Create the 10-Gbps client interface. For example:

```
bti7800(config)# interface 10ge:1/7/2/1
Value for 'type' [ethernetCsmacd,opticalChannel,otnOdu,otnOtu,...]:
ethernetCsmacd
bti7800(config-interface-10ge:1/7/2/1)# commit
Commit complete.
```

The following lists the interfaces created on the UFM in slot 7 (for example):

```
bti7800(config)# do show interface | include 1/7
```

```
Name           : 10ge:1/7/2/1
Name           : odu2:1/7/1/1.1
Name           : odu2:1/7/1/1.2
Name           : odu2:1/7/1/1.3
Name           : odu2:1/7/1/1.4
Name           : odu2:1/7/1/1.5
Name           : odu2:1/7/1/1.6
Name           : odu2:1/7/1/1.7
Name           : odu2:1/7/1/1.8
Name           : odu2:1/7/1/1.9
Name           : odu2:1/7/1/1.10
```

```
Name : odu4:1/7/1/1
Name : otu4:1/7/1/1
```

3. If you are multiplexing into an ODU2e instead of an ODU2, delete the corresponding ODU2 subinterface and manually create the ODU2e subinterface. See [“Provisioning a Transport Interface” on page 116](#) for more information.

For example:

```
bti7800(config)# no interface odu2:1/7/1/1.1
bti7800(config)# interface odu2e:1/7/1/1.1
Value for 'type' [ethernetCsmacd,opticalChannel,otn0du,otn0tu,...]: otn0du
bti7800(config-interface-odu2e:1/7/1/1.1)# commit
Commit complete.
```

4. Configure the cross-connect.

The following example cross-connects the 10-Gbps client interface with one of the subinterfaces on the ODU4:

```
bti7800(config)# cross-connect 10ge:1/7/2/1 odu2:1/7/1/1.4
bti7800(config-cross-connect-10ge:1/7/2/1/odu2:1/7/1/1.4)#
```

5. Optionally, specify the service name.

For example:

```
bti7800(config-cross-connect-10ge:1/7/2/1/odu2:1/7/1/1.4)# service-name
circuit_1714
```

6. Apply the changes.

```
bti7800(config-cross-connect-10ge:1/7/2/1/odu2:1/7/1/1.4)# commit
Commit complete.
```

7. Optionally, show the resulting cross-connect.

For example:

```
bti7800(config-cross-connect-10ge:1/7/2/1/odu2:1/7/1/1.4)# do show cross-connect
table | include circuit_1714

2  10ge:1/7/2/1  odu2:1/7/1/1.4  2way  odu2  circuit_1714
```

Provisioning a Muxponding Cross-Connect on a UFM6

Use this procedure to provision a cross-connect that muxponds between a client interface and an ODU subinterface within a higher-order ODU4 on a UFM6. This procedure muxponds a 10-Gigabit Ethernet signal into an ODU2e within an ODU4 as an example, but the same procedure can be used for other 10-Gbps and 40-Gbps protocols by

cross-connecting other interfaces. See [“Supported Cross-Connects” on page 122](#) for information on the cross-connects this module supports.

1. Enter configuration mode.

```
bti7800# config
bti7800(config)#
```

2. Create the interfaces to be cross-connected. See [“Provisioning a Transport Interface” on page 116](#) for information on creating transport interfaces.



NOTE: The cross-connect mapping between the client interface and the line subinterface on the ODU4 is fixed and cannot be changed. Ensure that the interfaces you create conform to the required mapping. See [“Supported Cross-Connects” on page 122](#) for more information.

- a. Create the optical channel interface. For example:

```
bti7800(config)# interface och:1/5/2/1/1.1
Value for 'type' [ethernetCsmacd,opticalChannel,otnOdu,otnOtu,...]:
opticalChannel
bti7800(config-interface-och:1/5/2/1/1.1)# frequency 192.1
bti7800(config-interface-och:1/5/2/1/1.1)# commit
Commit complete.
```

The optical channel represents the optical signal and contains attributes that are shared by all contained OTU4 signals. The optical channel interface must exist before you can create an OTU4 interface. For more information on creating an optical channel interface, see [“Provisioning an Optical Channel Interface” on page 120](#).

- b. Create the OTU4 line interface. For example:

```
bti7800(config)# interface otu4:1/5/2/1/1.1.1
Value for 'type' [ethernetCsmacd,opticalChannel,otnOdu,otnOtu,...]: otnOtu
bti7800(config-interface-otu4:1/5/2/1/1.1.1)# commit
Commit complete.
```

When you create an OTU4 line interface on a UFM6, the system automatically creates the corresponding ODU4 interface and configures it for multiplexing. The multiplexed ODU4 interface contains 10 automatically created ODU2e subinterfaces; for example, `odu2e:1/5/2/1/1.1.1` to `odu2e:1/5/2/1/1.1.10`.

If you are cross-connecting an existing ODU4 interface that has not been configured for multiplexing, you will need to configure it for multiplexing. For example:

```
bti7800(config)# interface odu4:1/5/2/1/1.1.1
bti7800(config-interface-odu4:1/5/2/1/1.1.1)# multiplex-mode gmp-capable
bti7800(config-interface-odu4:1/5/2/1/1.1.1)# commit
Commit complete.
```

- c. Create the client interface. For example, this creates a 10Ge client interface for multiplexing into an ODU2 or ODU2e subinterface:

```
bti7800(config)# interface 10ge:1/5/1/1/1
Value for 'type' [ethernetCsmacd,opticalChannel,otn0du,otn0tu,...]:
ethernetCsmacd
bti7800(config-interface-10ge:1/5/1/1/1)# commit
Commit complete.
```

The following lists the interfaces created on the UFM in slot 5 (for example):

```
bti7800(config)# do show interface | include 1/5
```

```
Name           : 10ge:1/5/1/1/1
Name           : odu2e:1/5/2/1/1.1.1.1
Name           : odu2e:1/5/2/1/1.1.1.2
Name           : odu2e:1/5/2/1/1.1.1.3
Name           : odu2e:1/5/2/1/1.1.1.4
Name           : odu2e:1/5/2/1/1.1.1.5
Name           : odu2e:1/5/2/1/1.1.1.6
Name           : odu2e:1/5/2/1/1.1.1.7
Name           : odu2e:1/5/2/1/1.1.1.8
Name           : odu2e:1/5/2/1/1.1.1.9
Name           : odu2e:1/5/2/1/1.1.1.10
Name           : odu4:1/5/2/1/1.1.1
Name           : otu4:1/5/2/1/1.1.1
Name           : och:1/5/2/1/1.1
```

3. If you are multiplexing a 10-Gbps interface into an ODU2 or a 40-Gbps interface into an ODU3, delete the corresponding ODU2e subinterface and manually create the ODU2 or ODU3 subinterface. If you are creating an ODU3 subinterface, you will need to delete all ODU2e subinterfaces that use the same tributary slots as the ODU3. See [“Provisioning a Transport Interface” on page 116](#) for more information.

For example, this deletes an ODU2e subinterface and creates an ODU2 subinterface:

```
bti7800(config)# no interface odu2e:1/5/2/1/1.1.1.9
bti7800(config)# interface odu2:1/5/2/1/1.1.1.9
Value for 'type' [ethernetCsmacd,opticalChannel,otn0du,otn0tu,...]: otn0du
bti7800(config-interface-odu2:1/5/2/1/1.1.1.9)# commit
Commit complete.
```

4. Configure the cross-connect.

The following cross-connects the 10-Gbps interface with the associated ODU2e subinterface on the ODU4:

```
bti7800(config)# cross-connect 10ge:1/5/1/1/1 odu2e:1/5/2/1/1.1.1.1
bti7800(config-cross-connect-10ge:1/5/1/1/1 odu2e:1/5/2/1/1.1.1.1)#
```

5. Optionally, specify the service name.

For example:

```
bti7800(config-cross-connect-10ge:1/5/1/1/1 odu2e:1/5/2/1/1.1.1.1)# service-name
circuit_2129
```

6. Apply the changes.

```
bti7800(config-cross-connect-10ge:1/5/1/1/1 odu2e:1/5/2/1/1.1.1.1)# commit
Commit complete.
```

7. Optionally, show the resulting cross-connect.

For example:

```
bti7800(config-cross-connect-10ge:1/5/1/1/1 odu2e:1/5/2/1/1.1.1.1)# do show
cross-connect table
```

Cross-Connect	Source-Name	Destination-Name	Direction	Rate
1	10ge:1/5/1/1/1	odu2e:1/5/2/1/1.1.1.1	2way	odu2e

Release History Table

Release	Description
4.4	ODU3 subinterface
4.1	The UFM6 is supported starting with release 4.1.

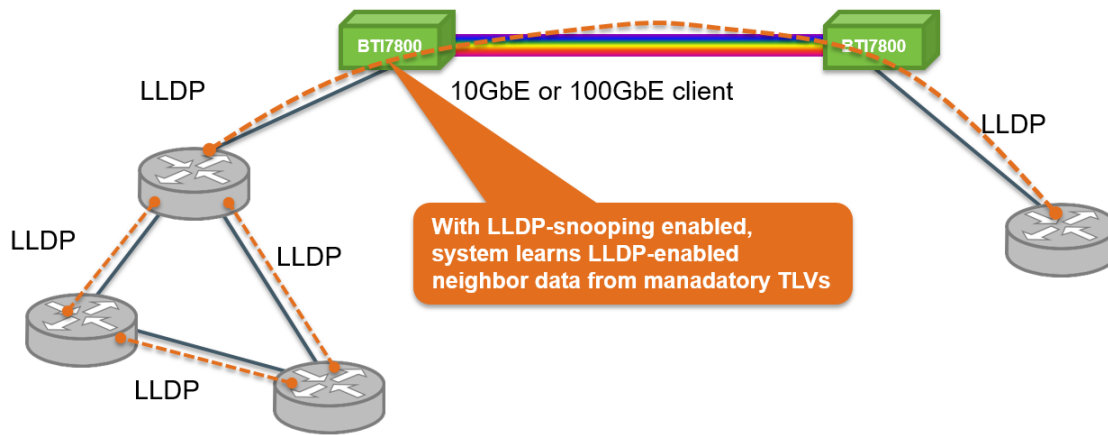
Link Layer Discovery Protocol (LLDP) Snooping

BT17800 transport interfaces configured for Ethernet (10ge and 100ge) can be provisioned to snoop Link Layer Discovery Protocol (LLDP) frames to gather information about attached equipment. This information can then be accessed via the CLI or NETCONF and used to identify neighbor devices.



NOTE: LLDP snooping is supported starting with release 4.1.

Figure 5: LLDP Snooping



LLDP data units, which are sent inside Ethernet frames at fixed intervals and identified by their destination Media Access Control (MAC) address and EtherType, carry device information in mandatory and optional type-length values (TLVs). Mandatory TLVs include device information such as chassis and port identification and system capabilities.

- [Configuring LLDP Snooping on an Ethernet Interface on page 145](#)
- [Supported LLDP TLVs on page 146](#)

Configuring LLDP Snooping on an Ethernet Interface

Use this procedure to enable or disable LLDP snooping on an Ethernet interface (10ge or 100ge).



NOTE: LLDP snooping is supported in the receive direction only and is disabled by default.

1. Enter configuration mode.

```
bti7800# config
bti7800(config)#
```

2. Configure LLDP snooping on an Ethernet interface.

For example, to enable LLDP snooping:

```
bti7800(config)# interface 10ge:1/2/1/1/1 lldp-snoop enable
bti7800(config-interface-10ge:1/2/1/1/1)# commit
Commit complete.
```

To disable LLDP snooping:

```
bti7800(config)# interface 10ge:1/2/1/1/1 lldp-snoop disable
```

```
bt17800(config-interface-10ge:1/2/1/1/1)# commit
Commit complete.
```

3. Repeat the previous step for each Ethernet interface for which you want to configure LLDP snooping.
4. Use the following **show** commands to either confirm the configuration changes or retrieve LLDP data.
 - **show interface lldp table** to retrieve a listing of all interfaces on which LLDP snooping is enabled.
 - **show interface lldp name:identifier** to retrieve LLDP neighbor data for an LLDP-enabled interface.
 - **show interface name:identifier** to view the value (**enabled** or **disabled**) of the **LLDP snooping** parameter for the specified interface.

Supported LLDP TLVs

BT17800 only supports mandatory LLDP TLVs (Table 24 on page 146), which provide information about a network-attached device (neighbor) for an LLDP-enabled Ethernet interface.

Table 24: Mandatory LLDP TLVs

TLV	Description	Range
Time to Live	The amount of time (in seconds) that received LLDP data units will be retained	0 to 65,535
Chassis ID Type	Chassis identifier type	<ul style="list-style-type: none"> chassis-component interface-alias port-component mac-address network-address interface-name local
Chassis ID	Chassis identifier as per chassis identifier type	String (1 to 255 characters)
Port ID Type	Port identifier type	<ul style="list-style-type: none"> interface-alias port-component mac-address network-address interface-name agent-circuit-id local
Port ID	Port identifier as per port identifier type	String (1 to 255 characters)

Table 24: Mandatory LLDP TLVs (continued)

TLV	Description	Range
Port Description	Port description (text)	String (0 to 255 characters)
System Name	Administratively assigned system name	String (0 to 255 characters)
System Description	System description (text)	String (0 to 255 characters)
System Capabilities Supported	Supported system capabilities	List containing any of the following:
System Capabilities Enabled	Enabled system capabilities	<ul style="list-style-type: none"> • repeater • bridge • vlan-access-point • router • telephone • docsis-cable-device • station-only • other • ip-v4 • ip-v6 • other
Management Address Type	Management address identifier type	<ul style="list-style-type: none"> • ip-v4 • ip-v6 • other
Management Address	Management address as per identifier type	String (0 to 255 characters)
Management Interface Subtype	Management interface number subtype	<ul style="list-style-type: none"> • if-index • system-port-number • unknown
Management Interface Number	Interface number that identifies the specific interface associated with the management address	32-bit integer
Management Interface OID	Object identifier (OID) that identifies the entity associated with the management address	String (OID format)

Release History Table

Release	Description
4.1	LLDP snooping is supported starting with release 4.1.

Transport (UFM) Performance Monitoring

Table 25 on page 148 lists the performance monitoring counters captured on a UFM. For the counter definitions, see the following:

- [Module and Device Statistics on page 205](#)
- [Optical and Physical Layer Statistics on page 206](#)
- [Protocol Statistics on page 210](#)

Table 25: UFM Performance Monitoring Counters

Type	Counters			
Module	-	cpu-load-avg	cpu-load-max	cpu-load-min
Transceiver ⁷	mod-temp	mod-temp-avg	mod-temp-max	mod-temp-min
	volt	volt-avg	volt-max	volt-min
Interface Statistics				

Table 25: UFM Performance Monitoring Counters (continued)

Type	Counters			
Optical / Physical	cc-opr ¹	cc-opr-avg	cc-opr-max	cc-opr-min
	cd ²	cd-avg	cd-max	cd-min
	cfo ²	cfo-avg	cfo-max	cfo-min
	dgd ²	dgd-avg	dgd-max	dgd-min
	fec-ber	fec-ber-avg	fec-ber-max	fec-ber-min
	fec-ber-delta-q ⁸	-	fec-ber-delta-q-max	fec-ber-delta-q-min
	fec-ber-x-corr ⁸	-	fec-ber-x-corr-max	fec-ber-x-corr-min
	fec-ber-x-q ⁸	-	fec-ber-x-q-max	fec-ber-x-q-min
	fec-ber-y-corr ⁸	-	fec-ber-y-corr-max	fec-ber-y-corr-min
	fec-ber-y-q ⁸	-	fec-ber-y-q-max	fec-ber-y-q-min
	fec-bitcr	fec-ucrcw	fec-0cr	fec-1cr
	lbc	lbc-avg	lbc-max	lbc-min
	ltemp ³	ltemp-avg	ltemp-max	ltemp-min
	opr	opr-avg	opr-max	opr-min
	opt	opt-avg	opt-max	opt-min
	opt-total ⁴	opt-total-avg	opt-total-max	opt-total-min
	osnr ⁴	osnr-avg	osnr-max	osnr-min
	snr ²	snr-avg	snr-max	snr-min
	snr-x ⁵	snr-x-avg	snr-x-max	snr-x-min
	snr-y ⁵	qsnr-y-avg	snr-y-max	snr-y-min
OTU	otu-bbe	otu-ber	otu-ber-avg	otu-ber-max
	otu-ber-min	otu-eb	otu-es	otu-ofs
	otu-ses			

Table 25: UFM Performance Monitoring Counters (continued)

Type	Counters			
ODU	odu-bbe	odu-ber	odu-ber-avg	odu-ber-max
	odu-ber-min	odu-eb	odu-es	odu-ses
Ethernet	bcast-pkts-rx	bcast-pkts-tx	drp-pkts-rx	fcse-pkts-rx
	fragments-rx	jabbers-rx	mcast-pkts-rx	mcast-pkts-tx
	octs-ok-rx	octs-ok-tx	octs-rx	osize-pkts-rx
	pcs-ses	pkts-ok-rx	pkts-ok-tx	pkts-paus-rx
	pkts-rx	pkts-tx	pkts-64-oct-rx	pkts-65-127-oct-rx
	pkts-128-255-oct-rx	pkts-256-511-oct-rx	pkts-512-1023-oct-rx	pkts-1024-1518-oct-rx
	pkts-over-1518-oct-rx	usize-pkts-rx		
SONET	ber-l	ber-avg-l	ber-max-l	ber-min-l
	cv-l	es-l	fc-l	ses-l
	ber-s	ber-avg-s	ber-max-s	ber-min-s
	cv-s	es-s	sefs-s	ses-s
SDH	ms-ber	ms-ber-avg	ms-ber-max	ms-ber-min
	ms-bbe	ms-eb	ms-es	ms-ses
	rs-ber	rs-ber-avg	rs-ber-max	rs-ber-min
	rs-bbe	rs-eb	rs-es	rs-ofs
	rs-ses			
Fibre channel	pcs-ses ⁶	pktsfcserx ⁶		

¹ The cc-opr counters (instantaneous/average/maximum/minimum) are supported on the 400G Coherent MSA XCVR on the UFM6 only (releases 4.3 and higher).

² The cd, cfo, dgd, and snr counters (instantaneous/average/maximum/minimum) are supported on the 100G Coherent MSA XCVR and 400G Coherent MSA XCVR only.

³ The ltemp counters (instantaneous/average/maximum/minimum) are supported on some transceivers only.

⁴ The opt-total and osnr counters (instantaneous/average/maximum/minimum) are supported on the 400G Coherent MSA XCVR on the UFM6 only.

⁵ The snr-x and snr-y counters (instantaneous/average/maximum/minimum) are supported on the 100G Coherent CFP (releases 2.1.1 and higher), the 100G Coherent MSA

XCVR on the UFM4 (releases 2.1.1 and higher), and the 400G Coherent MSA XCVR on the UFM6 (releases 4.1 and higher) only.

⁶ The pcs-ses and pktsfcserx counters are supported for fibre channel interfaces on the UFM6 starting in release 4.3.

⁷ For UFM6, the transceiver statistics are displayed when you show the statistics for the transceiver. For all other UFM6s, the transceiver statistics are displayed when you show the statistics for the interface associated with the transceiver.

⁸ The fec-ber-delta-q, fec-ber-x-corr, fec-ber-x-q, fec-ber-y-corr, and fec-ber-y-q counters are supported in release 4.5 for the following interfaces only:

- OTU4 interfaces on the 100G Coherent CFP
- OTU4 interfaces on the 100G Coherent MSA XCVR on the UFM4
- Optical channel interfaces on the 400G Coherent MSA XCVR on the UFM6

Release History Table

Release	Description
4.5	fec-ber-delta-q, fec-ber-x-corr, fec-ber-x-q, fec-ber-y-corr, and fec-ber-y-q counters
4.3	cc-opr counters
4.3	pcs-ses and pktsfcserx counters
2.1.1	snr-x and snr-y counters

CHAPTER 7

Optical Networking Solutions

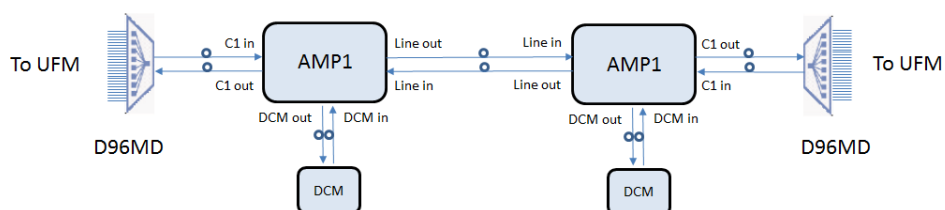
- [Terminal Amplifier Solutions on page 153](#)
- [Wavelength Protection Switch Solutions on page 159](#)

Terminal Amplifier Solutions

The 96-Channel Amplifier (AMP1) is a terminal amplifier that integrates two erbium-doped optical amplifiers to provide bidirectional amplification of DWDM optical signals in a point-to-point bookended configuration. The amplifier is optimized for 10-Gbps, 25-Gbps, and 100-Gbps signals, and includes an embedded optical supervisory channel (OSC) used for span loss control.

The AMP1 is designed to provide amplification of the composite signal in single span point-to-point applications between 96-Channel DWDM Mux/Demux modules as shown in [Figure 6 on page 153](#).

Figure 6: 96-Channel Amplifier Application



- [Provisioning a 96-Channel Amplifier Node on page 153](#)
- [Managing Optical Power on page 155](#)

Provisioning a 96-Channel Amplifier Node

Use this procedure to provision the 96-Channel Amplifier (AMP1) in a point-to-point configuration.

Prerequisites:

- The amplifier module is created. See [“Provisioning a Terminal Amplifier Module” on page 97](#).

1. Enter configuration mode.

```
bti7800# config
bti7800(config)#
```

2. Verify the amplifier that you want to configure is created.

For example, to verify that amp:1/11 is created:

```
bti7800(config)# do show amp | include amp:1/11
Amp Name                : amp:1/11
bti7800(config)#
```

3. Create the optical group for this amplifier.

For example, the following creates group 1:

```
bti7800(config)# amp group 1
Value for 'group-type' [eqLzLine,eqLzTerm,noEqLzLine,noEqLzTerm,...]: noEqLzTerm
bti7800(config-group-1)# exit
bti7800(config-amp)# commit
Commit complete.
```

The 96-Channel Amplifier can only be used in a non-equalizing terminal configuration. Therefore, its **group-type** must be **noEqLzTerm**.

4. Assign the amplifier to this group.

When the group is created, the degree is also created. A **noEqLzTerm** has only one degree (**degreenum 1**).

For example, to assign the 96-Channel Amplifier to group 1 degree 1:

```
bti7800(config-amp)# eqpt amp:1/11 groupnum 1 .
Value for 'degreenum' (<unsignedInt, 1 .. 4>): 1
bti7800(config-eqpt-amp:1/11)# exit
bti7800(config-amp)# commit
Commit complete
```

The system automatically creates all the ports on the amplifier.

```
bti7800(config-amp)# do show amp | include 1/11
Amp Name                : amp:1/11
Port Name                : osc:1/11/1/1.1
Port Name                : line:1/11/1/1
Port Name                : client:1/11/1/1
Port Name                : wdm:1/11/1/1
Port Name                : dcm:1/11/1/1
```

5. Configure the OSC settings.

For example, to configure far end identifier mismatch monitoring:

```
bti7800(config-amp)# osc osc:1/11/1/1.1
bti7800(config-osc-osc:1/11/1/1.1)# fe-im-mon true
bti7800(config-osc-osc:1/11/1/1.1)# exp-fe-ipaddr 10.1.1.1
bti7800(config-osc-osc:1/11/1/1.1)# exp-fe-grp 1
bti7800(config-osc-osc:1/11/1/1.1)# exp-fe-degree 1
bti7800(config-osc-osc:1/11/1/1.1)# exit
bti7800(config-amp)# commit Commit complete.
```

6. Configure port and wdm settings as required.

See “[Managing Optical Power](#)” on page 155 for details on the parameters to set for the specified applications.



NOTE: The fiber type must be configured for the system to automatically compensate for the tilt.

- To configure client port settings, use the **amp port client:1/11/1/1** command.
- To configure line port settings, use the **amp port line:1/11/1/1** command.
- To configure DCM port settings, use the **amp port dcm:1/11/1/1** command.
- To configure WDM settings, use the **amp wdm wdm:1/11/1/1** command.

7. When you are finished, apply the provisioning.

```
bti7800(config-amp)# commit
Commit complete.
```

The local amplifier node is created. Proceed to create the amplifier node at the far-end network element.

Managing Optical Power

There are two types of BTI7800 point-to-point network deployments: standard and 100-Gbps coherent-only. The standard system supports a mix of transceivers, for example, 100-Gbps coherent, 4x28-Gbps, and 10-Gbps, and supports a maximum supported span loss of 23 dB. The 100-Gbps coherent-only system supports only 100-Gbps coherent transceivers, and supports span losses greater than 23 dB.

The default post-amp gain value is set at 4.0 dB. To adjust the post-amp-gain you use the **amp wdm** CLI command.

- **Standard System Deployment:** The default post-amp gain is used for the first 40 channels. You adjust the post-amp gain when your system reaches 40, 80 and 96 channels.

- **100-Gbps Coherent-only Deployment:** The post-amp gain should be set to 5.0dB for the first 40 channels. You adjust the post-amp gain when your system reaches 40, 80 and 96 channels.



NOTE: If you are installing more than 40 channels during first-time installation, you must provision the additional channels before bringing all the channels into service.

To add channels after first-time installation, you must perform a post-amp gain adjust procedure, which is not covered in this guide. Adding channels after first-time installation should be performed during a maintenance window, although the BT17800 supports post-amp gain adjustments while the system is in service.

- [Managing Optical Power in a Standard Point-to-Point Deployment on page 156](#)
- [Managing Optical Power in a 100-Gbps Coherent Point-to-Point Deployment on page 157](#)

Managing Optical Power in a Standard Point-to-Point Deployment

The following sections provide information on the minimum required procedures to control optical power levels in a standard point-to-point deployment after first-time installation.



NOTE: Add channels in increasing order of the channel frequency starting with 191.80 THz, 1563.05 nm.

- [Verifying the OSC Receive Power for a Standard Point-to-Point Deployment on page 156](#)
- [Provisioning Tilt Control Parameters: Standard Deployments on page 157](#)
- [Provisioning Post-Amp Gain Control: Standard Deployments on page 157](#)

Verifying the OSC Receive Power for a Standard Point-to-Point Deployment

On low-loss spans it might be necessary to fit a fixed pad attenuator to the Line port of the 96-Channel Amplifier to avoid overload of the 1510 nm OSC receiver. The maximum supported power to the OSC receiver is -7 dBm.

For each amplifier, verify the OSC optical power received using the command: **show statistics current entity osc:chassisID/location/ BIC-1/<portNum>.<oscNum> binLength 1Minute**, and reference the parameter: **Optical power received**. As needed, adjust the pad to the Line port of the amplifier, based on the following values to operate at power levels up to 23 dBm:

- If the OSC optical power received is ≤ -7 dBm, do not fit a pad.
- If the OSC optical power received is between -2 and -7 dBm, fit a 5-dB pad to the Line port.
- If the OSC optical power received is > -2 dBm, fit a 10-dB pad to the Line port.

Provisioning Tilt Control Parameters: Standard Deployments

The following parameters on the 96-Channel Amplifier must be provisioned when the module is installed for the first-time:

- **DCM:** Must be associated to the amplifier. Use the command **amp eqpt**.
- **Fiber type:** Using the command **amp wdm**.

Once these values are configured, the amplifier automatically compensates for the tilt in the system.

Provisioning Post-Amp Gain Control: Standard Deployments

The default post-amp gain value is set at 4.0 dB.

You adjust the post-amp gain when your system reaches 40, 80 and 96 channels. To adjust the post-amp-gain you use the **amp wdm** CLI command, in Configuration model.

If you are installing more than 40 channels during first-time installation, you must provision the additional channels before bringing all the channels into service. To add channels during first-time installation use the command **amp wdm**.



NOTE: To add channels after first-time installation, you must perform a post-amp gain adjust procedure, which is not covered in this guide. Adding channels after first-time installation should be performed during a maintenance window, although the BTI7800 supports post-amp gain adjustments while the system is in service.

Managing Optical Power in a 100-Gbps Coherent Point-to-Point Deployment

The following sections provide information on the minimum required procedures to control optical power levels in a 100-Gbps coherent point-to-point deployment after first-time installation.



NOTE: Add channels in increasing order of the channel frequency starting with 191.80 THz, 1563.05 nm.



NOTE: DCMs (Dispersion Compensation Modules) are not used in a 100-Gbps coherent-only deployment.

- [Verifying the OSC Receive Power for a 100-Gbps Coherent Point-to-Point Deployment on page 158](#)
- [Managing a Receive Power Overload on page 158](#)
- [Provisioning Tilt Control Parameters: 100-Gbps Coherent Deployments on page 158](#)
- [Provisioning Post-Amp Gain Control: 100-Gbps Coherent Deployments on page 158](#)

Verifying the OSC Receive Power for a 100-Gbps Coherent Point-to-Point Deployment

On low-loss spans, it might be necessary to fit a fixed pad attenuator to the Line In port of the 96-Channel Amplifier to avoid overload of the 1510 nm OSC receiver. The maximum supported power to the OSC receiver is -7 dBm.

For each amplifier, verify the OSC optical power received using the command: **show statistics current entity osc:chassisID/location/ BIC-1/<portNum>.<oscNum> binLength 1Minute**, and reference the parameter: **Optical power received**. As needed, adjust the pad to the Line In port of the amplifier, based on the following values to operate at power levels up to 23 dBm:

- If the OSC optical power received is ≤ -7 dBm, do not fit a pad.
- If the OSC optical power received is between -2 and -7 dBm, fit a 5-dB pad to the Line port.
- If the OSC optical power received is > -2 dBm, fit a 10-dB pad to the Line port.

Managing a Receive Power Overload

To avoid an overload of the 100-Gbps transceivers, manually provision the attenuation of the client transmission loss to 5.0 dB using the command **amp port**.

Provisioning Tilt Control Parameters: 100-Gbps Coherent Deployments

The Fiber Type parameter on the 96-Channel Amplifier must be provisioned when the module is installed for the first-time. To provision the fiber type use the command **amp wdm**.

Once this is configured, the amplifier automatically compensates for the tilt in the system.

Provisioning Post-Amp Gain Control: 100-Gbps Coherent Deployments

The default post-amp gain value is set at 4.0 dB. To adjust the post-amp-gain you use the **amp wdm** CLI command, in Configuration mode.

The post-amp gain should be set to 5.0 db for the first 40 channels. You adjust the post-amp gain when your system reaches 40, 80 and 96 channels.

If you are installing more than 40 channels during first-time installation, you must provision the additional channels before bringing all the channels into service. To add channels during first-time installation use the command **amp wdm**.



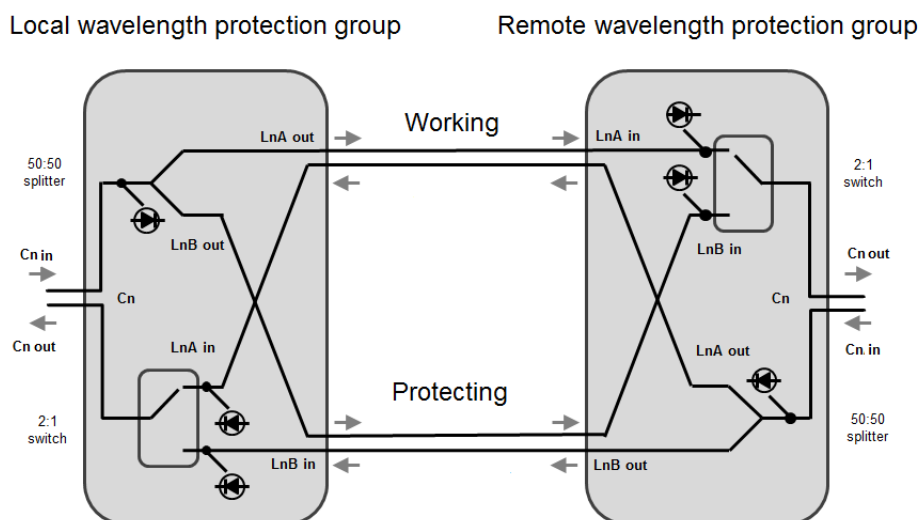
NOTE: To add channels after first-time installation, you must perform a post-amp gain adjust procedure, which is not covered in this guide. Adding channels after first-time installation should be performed during a maintenance window, although the BT17800 supports post-amp gain adjustments while the system is in service.

Wavelength Protection Switch Solutions

The WPS4 (BT8A78WPS4) provides 1+1 revertive or non-revertive optical protection switching.

Four wavelength protection groups can be provisioned on one module.

WPS4 modules function in a bookended configuration with one WPS4 being provisioned at the local node and one at the remote node.



A wavelength protection group consists of 3 ports (Cn_{out/in}, LnA_{out/in}, LnB_{out/in}) as shown in the diagram above.

At the local node, the signal received at the Cn_{in} port is split into two identical signals and transmitted out the LnA_{out} and LnB_{out} ports. These signals are received at the LnA_{in} and LnB_{in} ports at the remote node where an internal optical switch selects one of the incoming signals based on optical power levels. The selected signal is then transmitted out the Cn_{out} port.

Traffic transmitted from the remote node to the local node is handled in the same manner.

The path between the two LnA ports is called the working path. The path between the two LnB ports is called the protecting (or protection) path. Either path can be active. An incoming path is active if its signal is selected by the internal optical switch. The other path is in standby. Only one path can be active at any given time.



NOTE: Paths are unidirectional. For example, the working path can be active in one direction and standby in the opposite direction.

Should a fault occur on the active path causing the received power to fall below the loss of light threshold, an automatic protection switch occurs. After the fault has been cleared, traffic continues to be selected from the active path unless the group is configured for revertive switching. In revertive switching, traffic reverts to the working path (LnA) when the wait-to-revert time expires. In this case, if traffic is already on the working path, it remains on the working path.

The WPS4 provides the following functionality:

- Can protect a single wavelength or multiple wavelengths
- Supports operation on the following bands:
 - For extended C-band operation covering 1500 to 1570 nm
 - For L-band operation covering 1560 to 1620 nm
 - For O-band operation covering 1260 to 1360 nm
- Broadcast launch via a splitter to active and standby paths
- Active path selection via latching optical switch
- Automatic switching based upon received power levels
- Manual switching based upon provisioned switch state
- Monitoring of all input power levels
- [WPS4 Protection and Rapid Restoration Configurations on page 160](#)
- [Provisioning Wavelength Protection Groups and Ports on page 166](#)
- [Provisioning Customized LoLightRx Thresholds on page 172](#)
- [Performing User-Invoked Switches on the WPS4 on page 174](#)
- [Wavelength Protection Switch Alarms on page 177](#)
- [Wavelength Protection Switch Performance Monitoring on page 177](#)

WPS4 Protection and Rapid Restoration Configurations

The WPS4 supports the following applications:

- Optical Protection Switching - In Optical Protection Switching configurations, WPS4 protection switching operates within 50 ms of fault detection to ensure a minimum disruption of service. See [Table 26 on page 161](#).
- Rapid Restoration - In Rapid Restoration configurations, the time taken to restore traffic is dictated by the APSD or APR control systems between the local and remote WPS4. Therefore 50 ms protection switching is not guaranteed. The system will quickly and automatically restore service as soon as these controls resolve. This is typically in the order of seconds. See [Table 27 on page 161](#).

Table 26: WPS4 Protection Switching Configurations

Optical Protection Switching Configurations	LoLightRx Threshold
Unamplified line protection	Default
Unamplified channel protection	Default
Amplified line protection with unamplified protection path	Default
Amplified channel protection with amplified protection path	Customized

Table 27: WPS4 Rapid Restoration Configurations

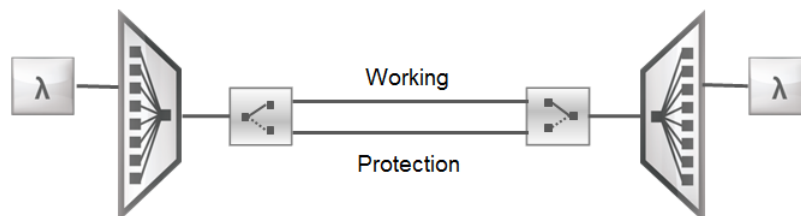
Rapid Restoration Configurations	LoLightRx Threshold
Amplified line restoration with unamplified protection path	Default
Amplified line restoration with amplified protection path	Default

If the optical solution you wish to use is not listed, please contact Juniper Networks Support.

- [Wavelength Protection Switch Unamplified Line Protection on page 161](#)
- [Wavelength Protection Switch Unamplified Channel Protection on page 162](#)
- [Wavelength Protection Switch Amplified Line Protection with an Unamplified Protection Path on page 162](#)
- [Wavelength Protection Switch Amplified Channel Protection with an Amplified Protection Path on page 163](#)
- [Wavelength Protection Switch Amplified Line Restoration with an Unamplified Protection Path on page 165](#)
- [Wavelength Protection Switch Amplified Line Restoration with an Amplified Protection Path on page 165](#)

Wavelength Protection Switch Unamplified Line Protection

The following example shows how the WPS4 can provide unamplified line protection within a network.



The optical protection switch solution:

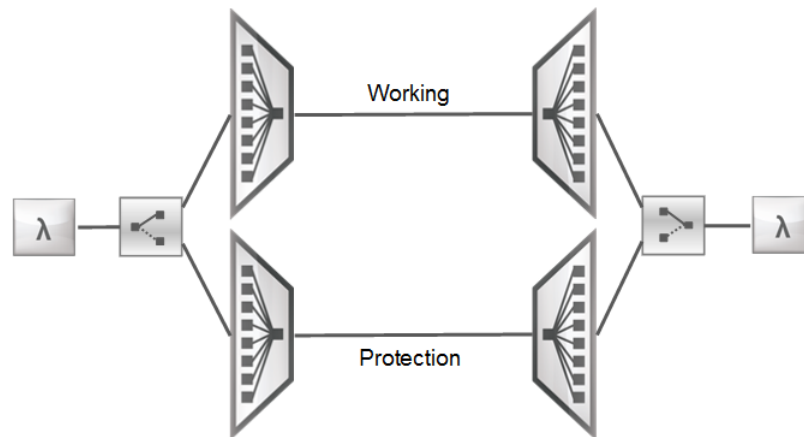
- Is a simple system configuration with diverse network paths on working and protection fiber pairs
- The default provisioning of the LoLightRx threshold (-35 dBm) should be used to protect for a fiber break on system fibers.



NOTE: This is the preferred configuration for unamplified systems as the optical multiplex section (OMS) is protected by a single protection group.

Wavelength Protection Switch Unamplified Channel Protection

The following example shows how the WPS4 can provide unamplified channel protection within a network.

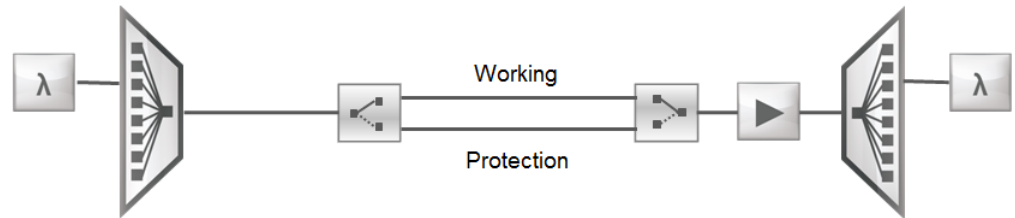


The optical protection switch solution:

- Provides per optical channel (OCh) protection configuration with diverse network paths on working and protection fiber pairs
- The default provisioning of LoLightRx threshold (-35dBm) should be used to protect for a fiber break on system fibers.

Wavelength Protection Switch Amplified Line Protection with an Unamplified Protection Path

The following example shows how the WPS4 can provide amplified line protection with an unamplified protection path within a network.



The optical protection switch solution:

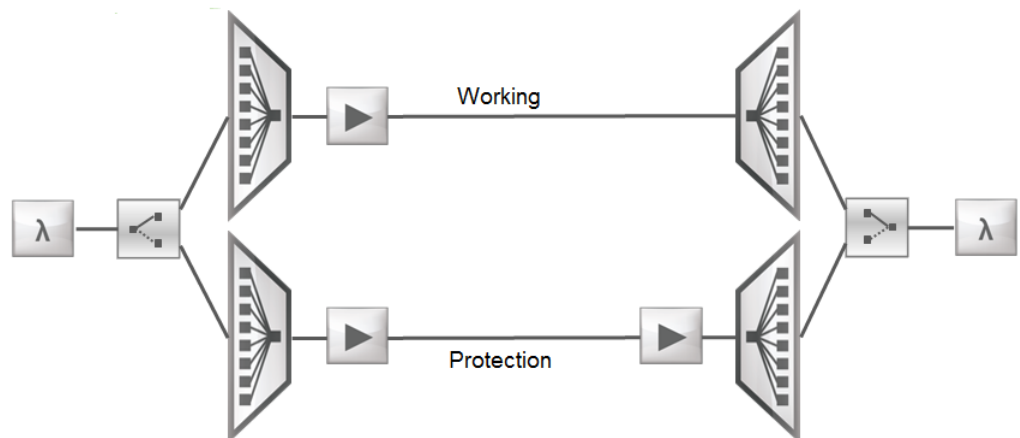
- Is a simple system configuration with diverse network paths on working and protection fiber pairs
 - Amplification allows for extended link budgets with BT17000 Series LGA/MGA/MGM amplifiers
- The default provisioning of the LoLightRx threshold (-35dBm) should be used to protect for a fiber break on system fibers
- Losses on Working and Protection paths should be balanced to within 2dB to avoid the need for amplifier gain adjustments after a protection event. This should be achieved by adding attenuation to the lowest loss path of the two
- Care must be taken with booster amplifiers as a protection event might trigger APR in EDFA.



NOTE: This is the preferred configuration for amplified systems as the optical multiplex section (OMS) is protected by a single protection group.

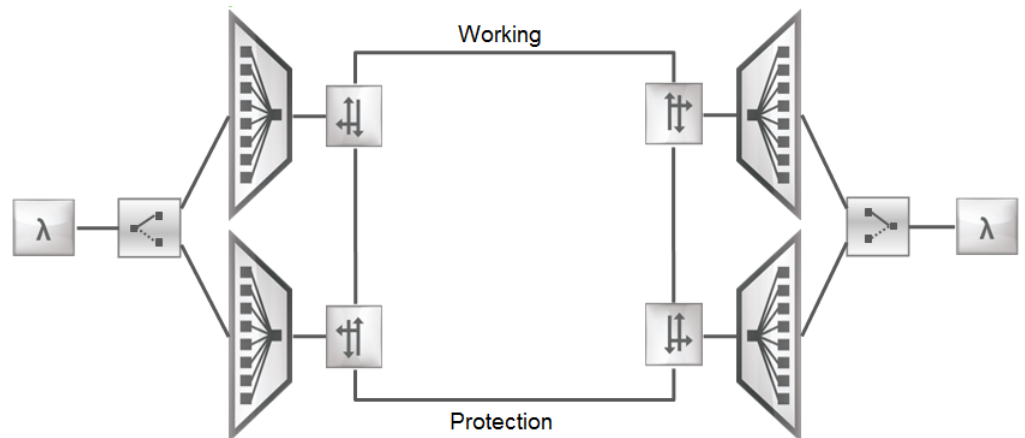
Wavelength Protection Switch Amplified Channel Protection with an Amplified Protection Path

The following example shows how the WPS4 can provide amplified channel protection with an amplified protection path within a network.

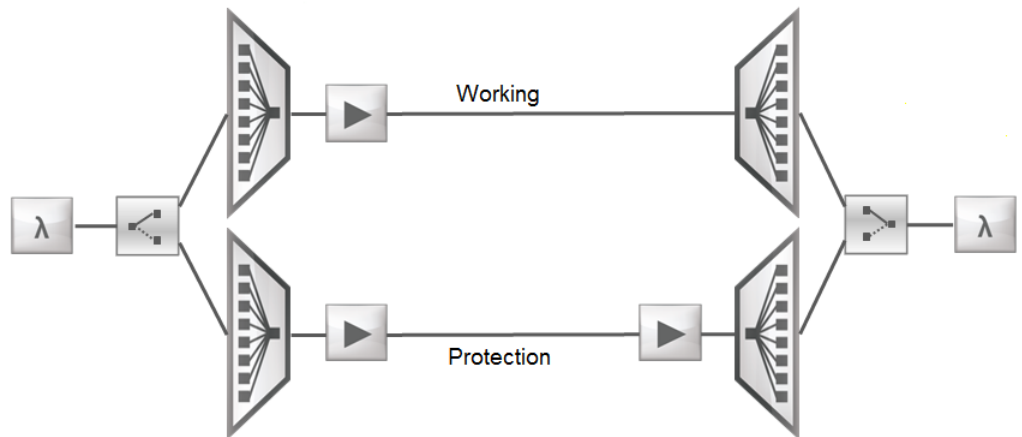


The optical protection switch solution:

- Is a simple system configuration with diverse network paths on working and protection fiber pairs
- Amplification allows for extended link budgets.
- Either or both paths can be amplified.
- A 50-GHz DWDM operation is supported via ROB496 ROADM



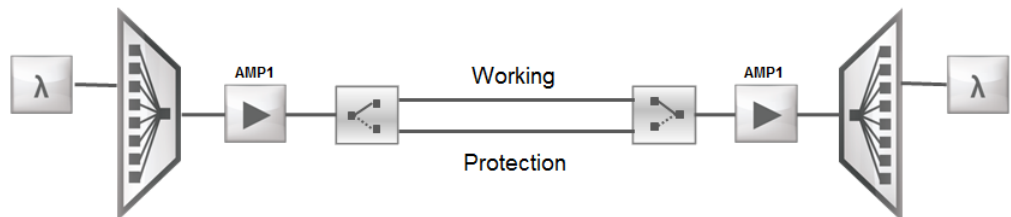
- A 100-GHz DWDM operation is supported via BTI7000 Series LGA/MGA/MGM optical amplifiers.



A custom provisioning of the WPS4's LoLightRx threshold is required when installing and provisioning the optical network. See [“Provisioning Customized LoLightRx Threshold” on page 172](#)

Wavelength Protection Switch Amplified Line Restoration with an Unamplified Protection Path

The following example shows how the WPS4 can provide amplified line restoration with an unamplified protection path.



The optical restoration switch solution:

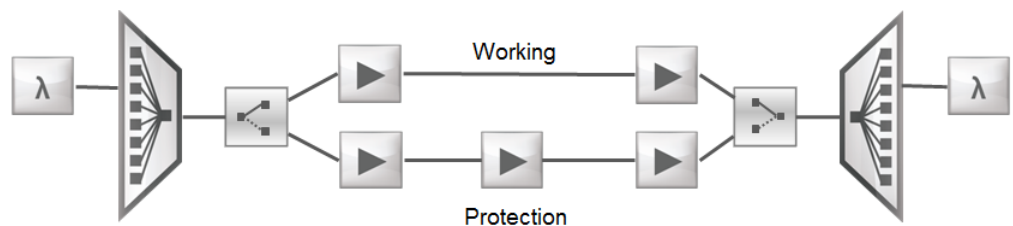
- Is a flexible system configuration with diverse network paths on working and protection fiber pairs
 - Amplification allows for extended link budgets with restoration supported using BT17800 AMP1 amplifiers
- Default provisioning of LoLightRx (-35 dBm) should be used to protect for a fiber break on system fibers
- Losses on Working and Protection paths should be balanced to within 2dB avoid the need for amplifier gain adjustments after a protection event. This should be achieved by adding attenuation to the lowest loss path of the two.



NOTE: This is the preferred configuration for amplified systems as the optical multiplex section (OMS) is protected by a single protection group.

Wavelength Protection Switch Amplified Line Restoration with an Amplified Protection Path

The following example shows how the WPS4 can provide amplified line restoration with an amplified protection path.



The optical restoration switch solution:

- Is a flexible system configuration with diverse network paths on working and protection fiber pairs
 - Amplification allows for extended link budgets using BTI7000 Series LGA/MGA/MGM optical amplifiers.
- The default provisioning of LoLightRx (-35dBm) should be used to protect for a fiber break on system fibers.
- The BTI7000 Series LGA/MGA/MGM optical amplifiers will turn off the output in the event of an input LOS event. The fault will propagate to the WPS4 as each downstream amp turns off. This might not complete within 50ms. Therefore this is Rapid Restoration rather than Protection. An automatic switch will still occur.



NOTE: It is possible to construct restoration solutions using the other amplifiers in the BTI Series portfolio but there are often deployment restrictions associated with these configurations. If these configurations are required, please contact Juniper Networks Support to evaluate your specific network requirement.

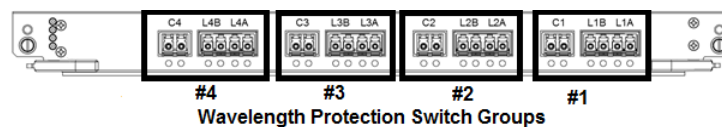
Provisioning Wavelength Protection Groups and Ports

Up to four wavelength protection groups can be provisioned on one module. A wavelength protection port can carry either a single wavelength or multiple wavelengths. The wavelength protection group number at the remote node is not required to match the wavelength protection group number of the WPS4 provisioned at the local node.

The wavelength protection ports are automatically created by the system when the group is provisioned. By default and under no line failures, LnA will be active.

LnA is the working port and LnB is the protecting port. This is a set configuration and cannot be changed.

The following table details the wavelength protection groups and their associated physical ports as detailed on Wavelength Protection Switch (WPS4) faceplate.



wavelength protection group	Associated wavelength protection group ports
wavelength protection group #1	C1 L1B L1A
wavelength protection group #2	C2 L2B L2A
wavelength protection group #3	C3 L3B L3A

wavelength protection group	Associated wavelength protection group ports
wavelength protection group #4	C4 L4B L4A

The wavelength ports (Cn, LnA, LnB) cannot be created independently of the group, nor can they be deleted. To delete a wavelength port you must delete the wavelength protection group it belongs to.

When a wavelength protection group is unprovisioned or deleted, the three wavelength ports associated with the group will be automatically deleted and line port A will be forced active, regardless of the received power.

The wavelength ports do not support the ability to shut down the laser. When the ports are optically connected, the WPS4 is capable of passing light from the Cn OUT, LnA OUT and LnB OUT ports at all times. Even when the module is not powered or when the module is not installed in the chassis.



NOTE: The Loss of Light Receive threshold (LoLightRx) must be set according to the optical link budget in order for the protection switch to operate as per specification.

- [Provisioning Wavelength Protection Groups on page 167](#)
- [Provisioning Wavelength Protection Ports on page 169](#)

Provisioning Wavelength Protection Groups

Use this procedure to provision the wavelength protection groups on a WPS4.

1. Provision the wavelength protection groups.

The following examples show how to provision four wavelength protection groups on the WPS4.

```

bti7800(config)# protection wavelength group wpsgroup:1/2/1
bti7800(config-protection-wavelength-group-wpsgroup:1/2/1)# commit
bti7800(config-protection-wavelength-group-wpsgroup:1/2/1)# exit
bti7800(config)#
bti7800(config)# protection wavelength group wpsgroup:1/2/2
bti7800(config-protection-wavelength-group-wpsgroup:1/2/2)# commit
bti7800(config-protection-wavelength-group-wpsgroup:1/2/2)# exit
bti7800(config)#
bti7800(config)# protection wavelength group wpsgroup:1/2/3
bti7800(config-protection-wavelength-group-wpsgroup:1/2/3)# commit
bti7800(config-protection-wavelength-group-wpsgroup:1/2/3)# exit
bti7800(config)#
bti7800(config)# protection wavelength group wpsgroup:1/2/4
bti7800(config-protection-wavelength-group-wpsgroup:1/2/4)# commit
bti7800(config-protection-wavelength-group-wpsgroup:1/2/4)#

```

2. Optional, provision revertive or non-revertive switching.

The default is non-revertive. The following example shows how to provision revertive switching.

```
bti7800(config-protection-wavelength-group-wpsgroup:1/2/4)# revertive-type
revertive bti7800(config-protection-wavelength-group-wpsgroup:1/2/4)# commit
bti7800(config-protection-wavelength-group-wpsgroup:1/2/4)#
```

3. Optional, provision additional wavelength protection group parameters.

At any wavelength protection group configuration mode, you can configure the parameters listed in the table below. See also the CLI command **protection wavelength group**.

Parameter	Description
protid	<p>A user-defined identifier of the protection group.</p> <p>0 to 32 alphanumeric characters</p> <p>Default : An empty string</p> <p>NOTE: This identifier is not required to match the remote node.</p>
remote-protid	<p>A user-defined identifier of the remote protection group.</p> <p>0 to 32 alphanumeric characters</p> <p>Default : An empty string</p> <p>NOTE: This identifier is not required to match the remote node.</p>
custom	<p>User-defined string.</p> <p>0 to 255 alphanumeric characters</p> <p>Default : An empty string</p>

4. Verify the wavelength protection group provisioning is correct.

Use the **show protection wavelength group** command to verify if the WPS4 provisioning is correct.

```
bti7800# show protection wavelength group
```

```

Group Name       : wpsgroup:1/1/1
Working          : wpsport:1/1/L1A
Working status   : Active
Protecting       : wpsport:1/1/L1B
Protecting status : Standby
Protection Id     : WPS456A
Remote Id        : WPS456BR
Revertive Type    : Non-Revertive
Revertive Time    : 600 seconds
Custom           : WPS456
Group Name       : wpsgroup:1/1/2
Working          : wpsport:1/1/L2A
Working status   : Active
```

```

Protecting          : wpsport:1/1/L2B
Protecting status   : Standby
Protection Id       : WPS459A
Remote Id          : WPS459BR
Revertive Type      : Non-Revertive
Revertive Time      : 600 seconds
Custom             : WPS459

```

You have successfully completed this procedure.

Related Commands

show running-config

show protection wavelength group table

Provisioning Wavelength Protection Ports

Use the following procedure to provision the wavelength protection ports on the WPS4.

1. Provision the lolight-rxth

The following example shows how to configure the loss of light threshold for each port in wavelength group.

```

bti7800(config)# protection wavelength port wpsport:1/3/1/C1A lolight-rxth
-25.0

bti7800(config-protection-wavelength-port-wpsport:1/3/1/C1A )# commit
bti7800(config-protection-wavelength-port-wpsport:1/3/1/C1A )# exit
bti7800(config)# protection wavelength port wpsport:1/3/1/L1A lolight-rxth
-30.0
bti7800(config-protection-wavelength-port-wpsport:1/3/1/L1A )# commit
bti7800(config-protection-wavelength-port-wpsport:1/3/1/L1A )# exit
bti7800(config)# protection wavelength port wpsport:1/3/1/L1B lolight-rxth
-30.0
bti7800(config-protection-wavelength-port-wpsport:1/3/1/L1B )# commit
bti7800(config-protection-wavelength-port-wpsport:1/3/1/L1B )# exit

```



NOTE: The lolight-rxth must be configured according to the optical link budget in order for the protection switch to operate as per specification. See also [“WPS4 Protection and Rapid Restoration Configurations” on page 160](#) and [“Provisioning Customized LoLightRx Threshold” on page 172](#).

2. Optional, provision additional wavelength port parameters.

The following additional wavelength port parameters can be provisioned.

Parameter	Description
id	<p>A user-defined identifier of the local wavelength protection port.</p> <p>0 to 32 alphanumeric characters</p> <p>Default : An empty string.</p> <p>NOTE: This identifier is not required to match the remote node.</p>
remote-id	<p>A user-defined identifier of the remote wavelength protection port.</p> <p>0 to 32 alphanumeric characters</p> <p>Default : An empty string.</p> <p>NOTE: This identifier is not required to match the remote node.</p>
custom	<p>User-defined string.</p> <p>0 to 255 alphanumeric characters</p> <p>Default : An empty string.</p>

3. Verify the wavelength port provisioning is correct.

Use the **show protection wavelength port** command to verify if the wavelength protection port provisioning is correct.

```
bti7800# show protection wavelength port
```

```

Port Name       : wpsport:1/1/C1
Protection Status :
Id              : WPS43811C1
Remote Id      : WPS43811C1R
Custom         : RED346711C1
LoLightRx Th   : -35.0 dBm
Opt.Pw.RX      : -3.5 dBm
Port Name       : wpsport:1/1/C2
Protection Status :
Id              : WPS43811C2
Remote Id      : WPS43811C2R
Custom         : RED346711C2
LoLightRx Th   : -35.0 dBm
Opt.Pw.RX      : -3.5 dBm
Port Name       : wpsport:1/1/L1A
Protection Status : Active
Id              : WPS43811L1A
Remote Id      : WPS43811L1AR
Custom         : RED346711L1A
LoLightRx Th   : -35.0 dBm
Opt.Pw.RX      : -2.5 dBm
Port Name       : wpsport:1/1/L1B
Protection Status : Standby
Id              : WPS43811L1B
Remote Id      : WPS43811L1BR

```

```

Custom          : RED346711L1B
LoLightRx Th    : -35.0 dBm
Opt.Pw.RX       : -2.6 dBm
Port Name       : wpsport:1/1/L2A
Protection Status : Active
Id              : WPS43811L2A
Remote Id       : WPS43811L2AR
Custom          : RED346711L2A
LoLightRx Th    : -35.0 dBm
Opt.Pw.RX       : -2.5 dBm
Port Name       : wpsport:1/1/L2B
Protection Status : Standby
Id              : WPS43811L2B
Remote Id       : WPS43811L2BR C
Custom          : RED346711L2B
LoLightRx Th    : -35.0 dBm
Opt.Pw.RX       : -2.6 dBm

```

4. Optional, view wavelength port statistics

Use the **show statistics** command to view wavelength port statistics.

```
bti7800# show statistics current wpsport:1/1/L1A
```

Current Statistics for wpsport:1/1/L1A

TIMESTAMP VALUE	LENGTH	VALIDITY	%SAMPLES	NAME
-----	-----	-----	-----	
2015-05-26T13:31:54+00:00 ...-2.50 dBm	unTimed	complete	100.0	Optical power received
2015-05-26T13:31:54+00:00 received ..-60.0 dBm	unTimed	complete	100.0	Min. optical power
2015-05-26T13:31:54+00:00 received ..-2.50 dBm	unTimed	complete	100.0	Max. optical power
2015-05-26T13:31:54+00:00 received ..-14.45dBm	unTimed	complete	100.0	Avg. optical power
2015-05-26T13:40:00+00:00 ...-2.50 dBm	1Minute	partial	38.3	Optical power received
2015-05-26T13:40:00+00:00 received ..-2.50 dBm	1Minute	partial	38.3	Min. optical power
2015-05-26T13:40:00+00:00 received ..-2.50 dBm	1Minute	partial	38.3	Max. optical power
2015-05-26T13:40:00+00:00 received ..-2.50 dBm	1Minute	partial	38.3	Avg. optical power
2015-05-26T13:31:54+00:00 ...-2.50 dBm	15Minute	partial	56.7	Optical power received
2015-05-26T13:31:54+00:00 received ..-60.0 dBm	15Minute	partial	56.7	Min. optical power
2015-05-26T13:31:54+00:00 received ..-2.50 dBm	15Minute	partial	56.7	Max. optical power
2015-05-26T13:31:54+00:00 received ..-14.42dBm	15Minute	partial	56.7	Avg. optical power
2015-05-26T13:31:54+00:00 ...-2.50 dBm	1Day	partial	0.5	Optical power received
2015-05-26T13:31:54+00:00 received ..-60.0 dBm	1Day	partial	0.5	Min. optical power
2015-05-26T13:31:54+00:00	1Day	partial	0.5	Max. optical power

```
received ..-2.50 dBm
2015-05-26T13:31:54+00:00 1Day partial 0.5 Avg. optical power
received ..-14.42dBm
```

You have successfully completed this procedure.

Related Commands

show running-config

show protection wavelength port

Provisioning Customized LoLightRx Thresholds

Use this procedure to set customized LoLightRx thresholds. For additional information see [“WPS4 Protection and Rapid Restoration Configurations” on page 160](#)

- [Provisioning Customized LoLightRx Threshold on page 172](#)

Provisioning Customized LoLightRx Threshold

You will be required to provision customized LoLightRx thresholds in the following network configurations:

- 50-GHz DWDM networks deploying WPS4 channel protection with BTI7000 Series ROB496 ROADM
- 100-GHz DWDM networks deploying WPS4 channel protection with BTI7000 Series LGA/MGA/MGM optical amplifiers.



NOTE: You might be required to provision the LoLightRx thresholds in network configurations which are not defined in [“WPS4 Protection and Rapid Restoration Configurations” on page 160](#). Contact Juniper Networks Support if you require further information.



NOTE: In networks deploying WPS4 channel protection with BTI7000 Series LGA/MGA/MGM optical amplifiers, this procedure should also be performed every time there are significant changes to the channel powers. We recommend that you reset the LoLightRx threshold if the receive power of a channel changes by more than +/- 2.5dB.

Before beginning this procedure ensure the ROB496 ROADM or Amp and the WPS4s are installed, provisioned and are connected in the network. The wavelength protection groups must be provisioned. The ROB496 ROADM or Amp must be provisioned with the channels up. The protection and working paths must be alarm free.

1. Note the received power on the wavelength protection ports LnA and LnB for the required channel.

The following commands show examples of how to display the received power on L1A and L1B.

```
bti7800# show statistics current wpsport:1/1/L1A
```

```
bti7800# show statistics current wpsport:1/1/L1B
```

2. Calculate the customized LoLightRx threshold values for LnA and LnB using the equations listed below.

```
Cn = ROB496 ROADM
LoLightRx threshold for LnA = Received Power on LnA (dBm)+ (- 6 dB)
LoLightRx threshold for LnB = Received Power on LnB (dBm)+ (- 6 dB)
```

```
Cn = BTI7000 Series LGA/MGA/MGM optical amplifiers
LoLightRx threshold for LnA = Received Power on LnA (dBm)+ (- 4.5 dB)
LoLightRx threshold for LnB = Received Power on LnB (dBm)+ (- 4.5 dB)
```

The following examples show how to calculate the LoLightRx thresholds.

Example 1: Cn = ROB496 ROADM

For example if the received power at LnA was -10 dBm and the received power at LnB was -15 dBm then the following applies:

Customized LoLightRx threshold LnA = -10 dBm - 6 dB = -16 dBm

Customized LoLightRx threshold LnB = -15 dBm - 6 dB = -21 dBm

Example 2: Cn = BTI7000 Series LGA/MGA/MGM optical amplifiers

For example if the received power at LnA was -10 dBm and the received power at LnB was -15 dBm then the following applies:

Customized LoLightRx threshold LnA = -10 dBm - 4.5 dB = -14.5 dBm

Customized LoLightRx threshold LnB = -15 dBm - 4.5 dB = -19.5 dBm

3. Provision the LoLightRx thresholds for LnA and LnB.

Example 1: Provisioning the LoLightRx thresholds for LnA and LnB when Cn = ROB496 ROADM

```
bti7800(config)# protection wavelength port wpsport:1/1/L1A lolight-rxth
-16.0
```

```
bti7800(config-protection-wavelength-port-wpsport:1/3/1/L1A) # commit
bti7800(config-protection-wavelength-port-wpsport:1/3/1/L1A)# exit
bti7800(config)# protection wavelength port wpsport:1/3/1/L1B lolight-rxth
-21.0
bti7800(config-protection-wavelength-port-wpsport:1/3/1/L1B)# commit
bti7800(config-protection-wavelength-port-wpsport:1/3/1/L1B)# exit
```

Example 2: Provisioning the LoLightRx thresholds for LnA and LnB when Cn = BTI7000 Series LGA/MGA/MGM optical amplifiers

```

bti7800(config)# protection wavelength port wpsport:1/1/1/L1A lolight-rxth
-14.5

bti7800(config-protection-wavelength-port-wpsport:1/3/1/L1A)# commit
bti7800(config-protection-wavelength-port-wpsport:1/3/1/L1A)# exit
bti7800(config)# protection wavelength port wpsport:1/3/1/L1B lolight-rxth
-19.5
bti7800(config-protection-wavelength-port-wpsport:1/3/1/L1B)# commit
bti7800(config-protection-wavelength-port-wpsport:1/3/1/L1B)# exit

```

4. Repeat this procedure for any other ports provisioned on the WPS4s.

Performing User-Invoked Switches on the WPS4

- [Manual Switch on page 174](#)
- [Forced Switch on page 174](#)
- [Lockout Switch on page 174](#)
- [Performing a Manual Wavelength Protection Switch on page 175](#)
- [Performing a Forced Wavelength Protection Switch on page 175](#)
- [Performing a Lockout Wavelength Protection Switch on page 176](#)

Manual Switch

A manual switch is applied to the active line and results in switching traffic away from the active line to the current standby line. The standby line will then become the new active line. A manual switch is not permitted if the standby line has a loss of signal. A manual switch does not disable automatic switching and does not require to be released.

Forced Switch

A forced switch is applied to the active line and results in switching traffic away from the active line to the current standby line. The standby line will then become the new active line. A forced switch is permitted even if the standby line is not alarm free. A forced switch can be provisioned even when the WPS4 is not present. It will persist until it is released.

Lockout Switch

A lockout switch is applied to the standby line and results in preventing traffic from switching to the standby line. A lockout switch is permitted even if the standby line is not alarm free. A lockout switch can be provisioned even when the WPS4 is not present. It will persist until it is released.



NOTE: Lockout and forced protection switch provisioning will persist in the system database.



NOTE: The `commit` function is not required when performing a user-invoked switch.

Revertive and Non-revertive Wavelength Protection Switching

In revertive switch operation, traffic will switch back to the working line after the fault has cleared and the wait-to-revert time has elapsed. The wait-to-revert time is 600 seconds and cannot be changed. Automatic, manual, forced and lockout switches will revert after they are released if the active line after release is protecting line (LnB).

In non-revertive switch operation traffic will not switch back to the active line. The default is non-revertive.

Performing a Manual Wavelength Protection Switch

User-invoked wavelength protection switches can be performed either in the operational or configuration mode. The **show protection wavelength group table** is performed in the operational mode only.



NOTE: The `commit` function is not required when performing a user-invoked switch.

1. Performing a manual wavelength protection switch

The following example shows how to perform a manual switch when the currently active line is L1A.

```
bt17800# protection wavelength switch manual wpsport:1/2/L1A
bt17800#
```

You have successfully completed this procedure.

Related Commands

`show protection wavelength group table`

Performing a Forced Wavelength Protection Switch

User-invoked wavelength protection switches can be performed either in the operational or configuration mode. The **show protection wavelength group table** is performed in the operational mode only.

A forced switch is performed on the active line and results in a switch away from the active line. The active line then becomes the standby line.



NOTE: The `commit` function is not required when performing a user-invoked switch.

1. Performing a forced wavelength protection switch.

The following example shows how to perform a forced switch when the currently active line is L1A.

```
bti7800# protection wavelength switch forced wpsport:1/2/L1A
bti7800#
```

2. Releasing a forced switch.

The following example shows how to release a forced switch when the currently standby line is L1B.

```
bti7800# protection wavelength switch release wpsport:1/2/L1B
bti7800#
```

You have successfully completed this procedure.

Related Commands

show protection wavelength group table

Performing a Lockout Wavelength Protection Switch

User-invoked wavelength protection switches can be performed either in the operational or configuration mode. The **show protection wavelength group table** is performed in the operational mode only.

A lockout switch is performed on the standby line and results in preventing traffic from switching to that line.



NOTE: The **commit** function is not required when performing a user-invoked switch.

1. Performing a lockout switch

The following example shows how to perform a lockout when the currently standby line is L2B:

```
bti7800# protection wavelength switch lockout wpsport:1/2/L2B
bti7800#
```

2. Releasing a lockout switch

The following example shows how to release a lockout switch when the currently standby line is L2B:

```
bti7800 # protection wavelength switch release wpsport:1/2/L2B
bti7800#
```

You have successfully completed this procedure.

Related Commands

show protection wavelength group table

Wavelength Protection Switch Alarms

Alarms and conditions can be viewed using the CLI. Autonomous notifications are available via NETCONF and SNMP.

The following alarms are supported on the WPS4:

- Port alarms:
 - loLightRx
- Module alarms:
 - eqptMiss
 - eqptMism

Wavelength Protection Switch Performance Monitoring

Performance monitoring is conducted on provisioned ports. Current and historical statistics are supported.

The types of physical layer performance monitoring parameters are listed in the following table:

Monitored Type	Montype	Description	Units
Optical Power Received	OPR	The power of the optical signal received on a port.	dBm

The optical power received on each port (Cn, LnA and LnB) is monitored and can be viewed using the CLI command **show statistics**.

An example is shown below.

```
bti7800# show statistics current wpsport:1/1/L1A
```

Current Statistics for wpsport:1/1/L1A

TIMESTAMP VALUE	LENGTH	VALIDITY	%SAMPLES	NAME
-----	-----	-----	-----	
2015-05-26T13:31:54+00:00 ...-2.50 dBm	unTimed	complete	100.0	Optical power received
2015-05-26T13:31:54+00:00 received ...-60.0 dBm	unTimed	complete	100.0	Min. optical power
2015-05-26T13:31:54+00:00 received ...-2.50 dBm	unTimed	complete	100.0	Max. optical power
2015-05-26T13:31:54+00:00	unTimed	complete	100.0	Avg. optical power

received ..-14.45dBm					
2015-05-26T13:40:00+00:00	1Minute	partial	38.3	Optical power received	
...-2.50 dBm					
2015-05-26T13:40:00+00:00	1Minute	partial	38.3	Min. optical power	
received ..-2.50 dBm					
2015-05-26T13:40:00+00:00	1Minute	partial	38.3	Max. optical power	
received ..-2.50 dBm					
2015-05-26T13:40:00+00:00	1Minute	partial	38.3	Avg. optical power	
received ..-2.50 dBm					
2015-05-26T13:31:54+00:00	15Minute	partial	56.7	Optical power received	
...-2.50 dBm					
2015-05-26T13:31:54+00:00	15Minute	partial	56.7	Min. optical power	
received ..-60.0 dBm					
2015-05-26T13:31:54+00:00	15Minute	partial	56.7	Max. optical power	
received ..-2.50 dBm					
2015-05-26T13:31:54+00:00	15Minute	partial	56.7	Avg. optical power	
received ..-14.42dBm					
2015-05-26T13:31:54+00:00	1Day	partial	0.5	Optical power received	
...-2.50 dBm					
2015-05-26T13:31:54+00:00	1Day	partial	0.5	Min. optical power	
received ..-60.0 dBm					
2015-05-26T13:31:54+00:00	1Day	partial	0.5	Max. optical power	
received ..-2.50 dBm					
2015-05-26T13:31:54+00:00	1Day	partial	0.5	Avg. optical power	
received ..-14.42dBm					

CHAPTER 8

Multichassis System

- [Multichassis System Configuration on page 179](#)
- [Setting Up a Multichassis System on page 180](#)
- [Converting a Multichassis System Into Two Single Chassis on page 184](#)
- [Replacing a Single CMM in a Satellite Chassis on page 186](#)
- [Replacing Both CMMs in a Satellite Chassis on page 187](#)

Multichassis System Configuration

The BT17800 supports a multichassis configuration where two BT17800 chassis can be managed as a single network element. The management planes of the two chassis are connected together by connecting the gigabit Ethernet EXP-1 (expansion) ports on the CMMs in one chassis to the EXP-1 ports on the CMMs in the other chassis. Since there are two CMMs in each chassis, there are two management links connecting the two chassis together (for redundancy). The data planes remain separate in a multichassis system.

Figure 7: Multiple Chassis Expansion Port



The chassis are distinguished by their chassis identifiers. The hub chassis is always **chassis:1** while the satellite chassis is **chassis:2**. The hub chassis provides management connectivity for the system, and controls the satellite chassis. All slot designations remain unchanged. For example, a UFM in slot 3 of the satellite chassis is identified as **ufm:2/3**.

All chassis must be equipped with CMMs. The CMMs take on different roles depending on where they reside. In the hub chassis, the CMMs act as active and standby system controller modules (SCMs), similar to a single chassis system. In the satellite chassis, the CMMs act as management relay modules (MRMs), and simply relay internal management traffic to and from the SCMs in the hub chassis. You log in to the active SCM in the hub chassis as you do in a single chassis system, by using the shared management IP address. You cannot log in directly to the MRMs in the satellite chassis. Management of the satellite chassis is performed through the SCMs in the hub chassis.

The following rules apply in a multichassis configuration:

- Only chassis of the same type can be connected to each other. A BTI7814 chassis can only be connected to another BTI7814 chassis. A BTI7802 chassis can only be connected to another BTI7802 chassis.
- The BTI7801 chassis cannot be connected in a multichassis system.
- The hub chassis contains two CMMs acting as SCMs. The satellite chassis contains two CMMs acting as MRMs.
- The CMM in slot A in the hub chassis must be connected to the CMM in slot A in the satellite chassis. Similarly, the CMM in slot B in the hub chassis must be connected to the CMM in slot B in the satellite chassis.

Once the multichassis system is set up, the SCMs in the hub chassis control the traffic modules in both chassis. If the active SCM goes down, the standby SCM takes over.

If both SCMs go down, the service modules in both chassis detect that SCM connectivity is lost. Service modules continue to pass traffic but do not update counters or raise alarms. This behavior, when both SCMs fail, is the same regardless of whether you are running a single chassis or a multichassis system. See [“CMM Failure or Removal” on page 41](#) for more information.



NOTE: For the satellite chassis, SCM connectivity can also be lost due to both inter-chassis links going down. In this situation, the behavior in the satellite chassis is the same as if both SCMs have gone down.

Setting Up a Multichassis System

Use this procedure to set up a multichassis system from two independent chassis. A multichassis system is managed as a single system, and consists of two chassis with their management planes connected together. The CMMs automatically detect that the management planes are connected together. Only minimal configuration is required.



NOTE: This procedure is service-affecting on the satellite chassis. Traffic will be affected. There is no rollback.

1. Back up the existing configuration and save a snapshot of the state on both chassis.
 - a. Log in to the CLI of one of the chassis using the shared management IP address.
 - b. Save the configuration database to a remote location.

For example:

```
bt17800# system database backup remote-url ftp://user@10.64.7.51
Value for 'password' (<string>): *****
bt17800# show system database

Backup Status
-----

CurrentStatus   : ready-to-backup
RemoteUrl       :
ftp://user@10.64.7.51/10.1.220.104_BT17800v1.6.0_18346_20150706_185955.tar.gz

NotificationMsg : Backup successful
```

Look for the **Backup successful** message in the output.

- c. Save the running configuration to a remote location.

For example:

```
bt17800# show running-config | nomore | save
10.1.220.104_running_config_20150706
Value for 'password' (<string>): *****
bt17800# copy file 10.1.220.104_running_config_20150706 remote-url
ftp://user@10.64.7.51/10.1.220.104_running_config_20150706
Value for 'password' (<string>):
```

- d. Save the state information to a remote location.

For example:

```
bt17800# show tech-support remote-url ftp://user@10.64.7.51
Value for 'password' (<string>):
Searching Inventory.....Done
Exploring data at Chassis:1 Collecting data from pld:1/2....Done
Collecting data from pld:1/5....Done Collecting data from pld:1/8....Done
Collecting data from pld:1/10....Done Collecting data from pld:1/11....Done

Collecting data from pld:1/13....Done Collecting data from cmm:1/A....Done

Creating archive..Done
Transferring file....
10.1.220.104_chassis-1_tech-support_2015-07-06_19-30-32.tar.gz
transferred successfully!
```

- e. Repeat for the second chassis.
2. Verify that the chassis you want to be the hub is ready for this procedure.

- a. Identify the chassis you want to be the hub and log in to its CLI using the shared management IP address.

- b. Ensure there are no outstanding CMM alarms on the hub chassis.

Use the **show conditions** command to list the outstanding faults on the system. Resolve any outstanding CMM faults before proceeding.

- c. Check to see if a second chassis is already configured.

You cannot configure a new multichassis system from an existing multichassis system. You must deprovision the existing multichassis system first.

To check if a second chassis is already configured:

```
bt17800# show system chassis
```

Serial-Number	Chassis ID
2413CR-010	1
2413CR-020	2

In this example, there is already a second chassis provisioned (serial number 2413CR-020). Follow the procedure in [“Converting a Multichassis System Into Two Single Chassis” on page 184](#) to properly convert this existing multichassis system into a single chassis system, and then start this procedure again.

If there is no second chassis provisioned, proceed to the next step.

3. Bring the chassis that you want to be the satellite back to an uncommissioned state.

This step is performed by bringing each CMM in the chassis back to an uncommissioned state one at a time. The CMM that is not being worked on must be unseated. See [“Uncommissioning a CMM” on page 264](#).

4. Unseat both CMMs in the chassis that you want to be the satellite.

5. Power-cycle the chassis that you want to be the satellite by unpowering and powering it back up.

6. Physically connect the two chassis together using Ethernet CAT5e UTP cables or better.

- a. Connect an Ethernet cable directly between the EXP-1 port on the CMM in slot A on the hub chassis and the EXP-1 port on the CMM in slot A on the satellite chassis.
- b. Connect an Ethernet cable directly between the EXP-1 port on the CMM in slot B on the hub chassis and the EXP-1 port on the CMM in slot B on the satellite chassis.



NOTE: Connect the Ethernet cables directly. Do not use a switch or a hub.

7. Reseat the CMMs in the satellite chassis. Ensure the CMMs are completely seated and connected to the backplane.

Once the satellite CMMs are seated, the satellite CMMs receive instructions over the inter-chassis links and assume the role of MRMs.

8. Assign a chassis identifier to the satellite chassis.

- a. Log in to the CLI using the shared management IP address.

By doing this, you are logging in to the active SCM on the hub chassis.

- b. Make sure that the system has detected the presence of the satellite chassis.

For example:

```
bti7800# show system chassis
```

Serial-Number	Chassis ID
2413CR-010	1
2413CR-011	

Do not proceed to the next step until the satellite chassis appears in the output.

In this example, the satellite chassis is identified by serial number 2413CR-011. Note that there is no chassis identifier associated with this chassis.

- c. Assign the chassis identifier. The chassis identifier for the satellite chassis must always be 2.

For example:



NOTE: Ensure that you enter the correct serial number in the command below. Double check before committing.

```
bti7800# config
```

```
bti7800(config)# system chassis 2413CR-011 chassis-id 2
bti7800(config-chassis-2413CR-011)# commit
Commit complete.
```

9. Verify that the satellite chassis is running the correct software and firmware.

By assigning a chassis identifier to the satellite chassis, the SCM recognizes that it must now manage the satellite chassis, and proceeds to upgrade the software and firmware on all modules in the satellite chassis in order to bring them to the software level that is running on the hub chassis. It can take 15 minutes or longer for the system to be brought to the correct software and firmware level. Until this upgrade is complete, equipment in the satellite chassis will not be operationally up.

Verify that the upgrade is complete by issuing the **show system version**, **show system firmware**, **show inventory**, and **show equipment** commands. You should see the correct software and firmware versions on all modules (except possibly the satellite CMM

firmware, which might need to be upgraded manually), and you should see all equipment in inventory.



NOTE: If the satellite CMMs require a firmware upgrade, you might need to do so manually. See [“Upgrading the CMM Firmware” on page 234](#) for information on how to do this.

10. Confirm that there are no new alarms caused by this procedure.

Use the **show conditions** command to see the list of outstanding faults.

11. Back up the new multichassis configuration and save the current state. This is useful for future troubleshooting purposes.

Use the **system database backup remote-url** and **show tech-support remote-url** commands.

The two single chassis systems have now become a multichassis system.

Converting a Multichassis System Into Two Single Chassis

Use this procedure to convert a multichassis system into two single chassis.



NOTE: This procedure is service-affecting on the satellite chassis. Traffic will be affected. There is no rollback.



CAUTION: We recommend that you perform this procedure in a maintenance window. If this procedure is incorrectly followed, you might bring the hub chassis into a state that can only be recovered by a system repair drive.

1. Log in to the CLI using the shared management IP address.
2. Back up the existing configuration and save a snapshot of the state of the multichassis system.
 - a. Save the configuration database to a remote location.

For example:

```
bt17800# system database backup remote-url ftp://john@10.64.7.51
Value for 'password' (<string>): *****
bt17800# show system database

Backup Status
-----
CurrentStatus   : ready-to-backup
```

```

RemoteUrl      :
ftp://john@10.64.7.51/10.1.220.104_BTI7800v1.6.0_18346_20150706_185955.tar.gz

NotificationMsg : Backup successful

```

Look for the **Backup successful** message in the output.

- b. Save the running configuration to a remote location.

For example:

```

bti7800# show running-config | nomore | save
10.1.220.104_running_config_20150706

Value for 'password' (<string>): *****
bti7800# copy file 10.1.220.104_running_config_20150706 remote-url
ftp://john@10.64.7.51/10.1.220.104_running_config_20150706
Value for 'password' (<string>):

```

- c. Save the state information to a remote location.

For example:

```

bti7800# show tech-support remote-url ftp://john@10.64.7.51

Value for 'password' (<string>):
Searching Inventory.....Done

Exploring data at Chassis:1
Collecting data from pld:1/2....Done
Collecting data from pld:1/5....Done
Collecting data from pld:1/8....Done
Collecting data from pld:1/10....Done
Collecting data from pld:1/11....Done
Collecting data from pld:1/13....Done
Collecting data from cmm:1/A....Done
Creating archive..Done
Transferring file....
10.1.220.104_chassis-1_tech-support_2015-07-06_19-30-32.tar.gz transferred
successfully!

```

3. Disconnect the inter-chassis cables.

You might see an alarm indicating a cable is disconnected.

4. Remove the satellite chassis from the system.

```

bti7800# show system chassis

Serial-Number    Chassis ID
-----
2413CR-010       1
2413CR-011       2
bti7800# config
bti7800(config)# no system chassis 2413CR-011
bti7800(config)# commit
Commit complete.

```



CAUTION: If you remove the hub chassis by mistake, the hub chassis will go into a state that can only be recovered by a system repair drive.

The hub chassis is now a single chassis system. Traffic on the hub chassis is unaffected and continues to run.

The satellite chassis is now separate from the hub chassis. You can now turn up the satellite chassis using the initial turn-up procedures.

5. Install and commission the satellite chassis using the procedures described in [“Turning Up the Software on the BT17800” on page 29](#) and [“Commissioning the BT17800 for the First Time” on page 30](#).

Both chassis are now single chassis systems.

Replacing a Single CMM in a Satellite Chassis

Use this procedure to replace one of the CMMs in a satellite chassis in a multichassis system. The CMMs in the satellite chassis act as Management Relay Modules (MRMs) that relay messages and commands between the active CMM in the hub chassis and the modules in the satellite chassis.

Prerequisites

- You have a USB drive containing the USB image for the replacement CMM. All four CMMs in a multichassis system must run the same release of software. The software image in the USB drive must therefore be at the same release as the software running on the hub chassis. For information on creating a USB drive, see [“Creating a BT17800 System Repair Drive” on page 269](#).
 - The replacement CMM is uncommissioned for this chassis.
 - Familiarize yourself with the CMM replacement procedures in the *BT17800 Series Hardware Overview and Installation Guide*.
1. Disconnect the inter-chassis Ethernet cable from the CMM being replaced.
This does not affect traffic on the service modules.
 2. Unseat and remove the CMM from the satellite chassis.
 3. Insert the replacement CMM but do not seat it yet.
 4. If the replacement CMM does not have the required software load, follow the procedure in [“Installing a Software Load on a CMM Using a System Repair Drive” on page 261](#) to install the required software load onto the replacement CMM.

5. Follow the procedure in [“Uncommissioning a CMM” on page 264](#) to uncommission the CMM and set the database to factory defaults.
6. Connect the inter-chassis Ethernet cable to the replacement CMM.
7. Log in to the shared management IP address for the system and verify that the replacement CMM is running properly.
 - a. Use the **show system** command to make sure the system recognizes the replacement CMM.
 - b. Use the **show system firmware** command to make sure the replacement CMM is running the correct level of firmware. If you see a ****FIRMWARE MISMATCH**** for firmware in the replacement CMM, then the respective firmware needs updating. For information on how to do this, see [“Upgrading the CMM Firmware” on page 234](#).

Replacing Both CMMs in a Satellite Chassis

Use this procedure to replace both CMMs in a satellite chassis in a multichassis system. The CMMs in the satellite chassis act as Management Relay Modules (MRMs) that relay messages and commands between the active CMM in the hub chassis and the modules in the satellite chassis.



WARNING: Service modules are automatically warm reloaded as part of this procedure. Software-based features on the service module (such as PM collection, APSD, APR, FPSD) are disabled while a service module warm reloads.

Prerequisites

- You have a USB drive containing the USB image for the replacement CMM. All four CMMs in a multichassis system must run the same release of software. The software image in the USB drive must therefore be at the same release as the software running on the hub chassis. For information on creating a USB drive, see [“Creating a BTI7800 System Repair Drive” on page 269](#).
 - The replacement CMMs are uncommissioned for this chassis.
 - Familiarize yourself with the CMM replacement procedures in the *BTI7800 Series Hardware Overview and Installation Guide*.
1. Disconnect the two inter-chassis Ethernet cables from the CMMs being replaced.
Depending on the software release, the service modules might undergo a warm reload. This does not affect traffic on the service modules. If the service modules undergo a warm reload, the modules do not boot back up until communication is reestablished with the CMM in the hub chassis at the end of this procedure.
 2. Unseat and remove both CMMs from the satellite chassis.

3. Insert one of the replacement CMMs into CMM slot A but do not seat it yet.
4. If the replacement CMM does not have the required software load, follow the procedure in [“Installing a Software Load on a CMM Using a System Repair Drive” on page 261](#) to install the required software load onto the replacement CMM.
5. Follow the procedure in [“Uncommissioning a CMM” on page 264](#) to uncommission the CMM and set the database to factory defaults.
6. Unseat the CMM.
7. Insert the second replacement CMM into CMM slot B but do not seat it yet.
8. Repeat step 4 to step 6 on the second CMM.

At the completion of this step, both CMMs should be unseated. They should also contain the required software image and be in an uncommissioned state.

9. Connect the two inter-chassis Ethernet cables to the replacement CMMs.
10. Seat both CMMs.

Once the replacement satellite CMMs are seated, the satellite CMMs receive instructions over the inter-chassis links and assume the role of MRMs. If the service modules were warm-reloaded earlier, they will now boot up.
11. Log in to the shared management IP address for the system and verify that the replacement CMMs are running properly.
 - a. Use the **show system** command to make sure the system recognizes the replacement CMMs.
 - b. Use the **show system firmware** command to make sure the replacement CMMs are running the correct level of firmware. If you see a ****FIRMWARE MISMATCH**** for firmware in the replacement CMMs, then the respective firmware needs updating. For information on how to do this, see [“Upgrading the CMM Firmware” on page 234](#).

CHAPTER 9

SNMP

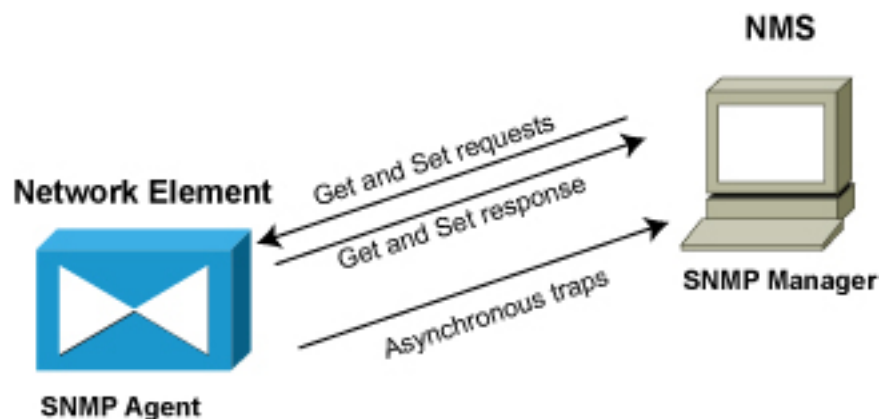
- [About SNMP on page 189](#)
- [Supported SNMP Functionality on page 190](#)
- [Supported MIBs on page 191](#)
- [Configuring SNMP on page 196](#)

About SNMP

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

The SNMP model consists of the SNMP manager (typically the NMS), the SNMP agent on the network element, and the management information base (MIB), which is the database of information used to manage the network element. The protocol exchange between the SNMP manager and the SNMP agent consists of requests made by the SNMP manager, the associated responses from the SNMP agent, and the asynchronous notifications or traps that the SNMP agent generates due to notable events occurring on the network element.

The following figure shows the interaction between the NMS and the network element using SNMP.



Information is stored as managed objects in MIBs, which are files that describe the managed objects in a structured representation. An object is one of a number of attributes of the managed device. Objects are organized into a tree structure, in which each object is a leaf node with its own unique object identifier (OID). With the OID, the SNMP manager can uniquely identify the managed object in its requests and in the responses and notifications from the SNMP agent.

Objects can be:

- **Scalar**—defines a single object instance.
- **Tabular**—defines multiple related object instances, such as in a table.

Supported SNMP Functionality

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

- **Get**—Allows the SNMP manager to retrieve one or more specific object values (on a device) from the SNMP agent. BT17800 supports the use of the *Get* operation to retrieve objects with read access.
- **GetNext**—Allows the SNMP manager to retrieve the next object instance in lexicographical order relative to a specified object. When an SNMP manager wants to “walk” through all elements of a table on an agent, it performs a series of *GetNext* operations using the last returned object as the argument for the succeeding *GetNext* operation.
- **GetBulk**—Allows the SNMP manager to retrieve multiple rows of tabular objects in a single operation.
- **Set**—Allows the SNMP manager to send one or more specific object values to the SNMP agent.
- **Trap**—Used by the agent to asynchronously notify the SNMP manager of an event.
- **Inform**—Traps sent by the agent for which acknowledgment is sent back.

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

Specifications

Parameter	Value
SNMP version	v2c
Trap receivers	Up to 10 trap receivers can be provisioned on one BT17800 system.
UDP port (traps)	Default: 162

Parameter	Value
UDP port (requests)	Default: 161 This value cannot be changed.
Read-only community string	Default: public
Read-write community string	Default: private

OSS Integration

Please note the following when integrating BTI7800 MIBs:

- Performance: It is the customer's responsibility to conduct testing to ensure that the NE interfaces meet their proposed usage needs. Juniper Networks makes no guarantees that any proposed usage will meet customer requirements.
- Changes between releases: SNMP MIBs are subject to change as support for new functionality is introduced. Although Juniper Networks makes every effort to maintain backward compatibility of BTI7800 MIBs across releases, backward compatibility cannot be guaranteed. Juniper Networks reserves the right to deprecate or remove support for obsolete MIB elements. For this reason, OSS integrators should not rely on functionality that is marked as deprecated, because there is a likelihood that it will not be supported in a subsequent release. Customers that integrate directly to the MIBs are responsible for all OSS development and integration testing that result from MIB changes between software releases.

Supported MIBs

You can download supported MIBs from <https://www.juniper.net/support/downloads> by selecting the desired product and release.



NOTE: The BTI7800 does not allow *create* access to any of the supported objects even if the supported object has a MAX-ACCESS value of *read-create*.

Table 28 on page 192 lists the objects supported from the standard MIBs.

Table 28: Standard MIBs

MIBs	RFC	Supported Objects (OID)
SYSTEM MIB	RFC3418	<p>The following objects from the System Group are supported:</p> <ul style="list-style-type: none"> • sysDescr (1.3.6.1.2.1.1.1) • sysObjectID (1.3.6.1.2.1.1.2) • sysContact (1.3.6.1.2.1.1.4) • sysName (1.3.6.1.2.1.1.5) • sysLocation (1.3.6.1.2.1.1.6) • sysServices (1.3.6.1.2.1.1.7) • sysORLastChange (1.3.6.1.2.1.1.8)
IF-MIB	RFC2863	<p>The following objects from the Interfaces Group are supported.</p> <ul style="list-style-type: none"> • ifTable (1.3.6.1.2.1.2.2) <ul style="list-style-type: none"> • ifEntry (1.3.6.1.2.1.2.2.1) <ul style="list-style-type: none"> • ifIndex (1.3.6.1.2.1.2.2.1.1) • ifDescr (1.3.6.1.2.1.2.2.1.2) • ifType (1.3.6.1.2.1.2.2.1.3) • ifMtu (1.3.6.1.2.1.2.2.1.4) • ifAdminStatus (1.3.6.1.2.1.2.2.1.7) • ifOperStatus (1.3.6.1.2.1.2.2.1.8) • ifXTable (1.3.6.1.2.1.31.1.1) <ul style="list-style-type: none"> • ifXEntry (1.3.6.1.2.1.31.1.1.1) <ul style="list-style-type: none"> • ifName (1.3.6.1.2.1.31.1.1.1.1) • ifLinkUpDownTrapEnable (1.3.6.1.2.1.31.1.1.1.14) • ifAlias (1.3.6.1.2.1.31.1.1.1.18) • snmpTraps (1.3.6.1.6.3.1.1.5) <ul style="list-style-type: none"> • linkDown (1.3.6.1.6.3.1.1.5.3) • linkUp (1.3.6.1.6.3.1.1.5.4) <p>NOTE: This MIB is supported for UFM interfaces and for virtual mgt interfaces.</p>

Table 28: Standard MIBs (continued)

MIBs	RFC	Supported Objects (OID)
IP-MIB (supported in releases 2.1.1 and higher)	RFC4293	<p>The following objects from the IPv4 address table are supported:</p> <ul style="list-style-type: none"> ipAddrTable (1.3.6.1.2.1.4.20) <ul style="list-style-type: none"> ipAddrEntry (1.3.6.1.2.1.4.20.1) <ul style="list-style-type: none"> ipAdEntAddr (1.3.6.1.2.1.4.20.1.1) ipAdEntIfIndex (1.3.6.1.2.1.4.20.1.2) - The index is assigned as follows: <ul style="list-style-type: none"> shared management IP: 5 CMM:1/A eth1 interface: 4101 CMM:1/B eth1 interface: 8197 ipAdEntNetMask (1.3.6.1.2.1.4.20.1.3) <p>NOTE: This MIB is supported for the shared management IP interface and for the management Ethernet ports (eth1) on both CMMs.</p>

Table 28: Standard MIBs (continued)

MIBs	RFC	Supported Objects (OID)
RMON-MIB (supported in releases 2.1.1 and higher)	RFC2819	<p>The following objects from the Ethernet statistics group are supported:</p> <ul style="list-style-type: none"> statistics (1.3.6.1.2.1.16.1) <ul style="list-style-type: none"> etherStatsTable (1.3.6.1.2.1.16.1.1) <ul style="list-style-type: none"> etherStatsEntry (1.3.6.1.2.1.16.1.1.1) <ul style="list-style-type: none"> etherStatsIndex (1.3.6.1.2.1.16.1.1.1.1) etherStatsDataSource (1.3.6.1.2.1.16.1.1.1.2) etherStatsDropEvents (1.3.6.1.2.1.16.1.1.1.3) etherStatsOctets (1.3.6.1.2.1.16.1.1.1.4) etherStatsPkts (1.3.6.1.2.1.16.1.1.1.5) etherStatsBroadcastPkts (1.3.6.1.2.1.16.1.1.1.6) etherStatsMulticastPkts (1.3.6.1.2.1.16.1.1.1.7) etherStatsCRCAlignErrors (1.3.6.1.2.1.16.1.1.1.8) - This counter considers packets up to a maximum of 9600 octets but otherwise conforms with the standard definition in the RMON MIB. etherStatsUndersizePkts (1.3.6.1.2.1.16.1.1.1.9) etherStatsOversizePkts (1.3.6.1.2.1.16.1.1.1.10) - This counter only considers packets whose length exceeds 9600 octets but otherwise conforms with the standard definition in the RMON MIB. etherStatsFragments (1.3.6.1.2.1.16.1.1.1.11) etherStatsJabbers (1.3.6.1.2.1.16.1.1.1.12) - This counter only considers packets whose length exceeds 9600 octets but otherwise conforms with the standard definition in the RMON MIB. etherStatsCollisions (1.3.6.1.2.1.16.1.1.1.13) etherStatsPkts64Octets (1.3.6.1.2.1.16.1.1.1.14) etherStatsPkts65to127Octets (1.3.6.1.2.1.16.1.1.1.15) etherStatsPkts128to255Octets (1.3.6.1.2.1.16.1.1.1.16) etherStatsPkts256to511Octets (1.3.6.1.2.1.16.1.1.1.17) etherStatsPkts512to1023Octets (1.3.6.1.2.1.16.1.1.1.18) etherStatsPkts1024to1518Octets (1.3.6.1.2.1.16.1.1.1.19) etherStatsOwner (1.3.6.1.2.1.16.1.1.1.20) etherStatsStatus (1.3.6.1.2.1.16.1.1.1.21) <p>NOTE: This MIB is supported for UFM ethernetCsmacd interfaces only.</p>

In addition to the objects supported in standard MIBs, the BT17800 supports a set of enterprise MIBs ([Table 29 on page 195](#)) that can be used to retrieve system inventory, provision equipment and facilities, and monitor faults through trap-based alarm notification and retrieval of active alarms and conditions.

Table 29: BTI7800 MIBs

MIBs	Description
BTI-MIB	Top-level BTI Series MIB.
BTI7800-MIB	Top-level BTI7800 MIB.
BTI7800-NOTIFICATIONS-MIB	Contains trap information for each alarm and condition.
BTI7800-CONDITIONS-MIB	Contains objects relating to the retrieval of active alarms and conditions.
BTI7800-EQUIPMENT-MIB	Contains objects relating to the system equipment.
BTI7800-INVENTORY-MIB	Contains objects relating to the system inventory.

BTI7800 enterprise MIBs have the following hierarchy within the enterprise (1.3.6.1.4.1) branch:

- btiSystems (1.3.6.1.4.1.18070)
 - btiProducts (1.3.6.1.4.1.18070.2)
 - bti7800 (1.3.6.1.4.1.18070.2.9)
 - BTI7800-CONDITIONS-MIB (1.3.6.1.4.1.18070.2.9.1)
 - BTI7800-NOTIFICATIONS-MIB (1.3.6.1.4.1.18070.2.9.2)
 - BTI7800-MIB (1.3.6.1.4.1.18070.2.9.3)
 - BTI7800-EQUIPMENT-MIB (1.3.6.1.4.1.18070.2.9.3.1)
 - BTI7800-INVENTORY-MIB (1.3.6.1.4.1.18070.2.9.3.2)

Load Order

You must only load MIB files that are associated with the software load running on the BTI7800 system. Always unload all previous versions of MIB files before installing new versions.



NOTE: The MIBs must be loaded in the order listed:

- BTI7800-NOTIFICATIONS-MIB
- BTI7800-CONDITIONS-MIB
- BTI7800-EQUIPMENT-MIB
- BTI7800-INVENTORY-MIB

Release History Table

Release	Description
2.1.1	IP-MIB
2.1.1	RMON-MIB

Configuring SNMP

Use this procedure to configure SNMP community strings and trap receivers.

1. Configure the community strings.



NOTE: In releases lower than release 4.3, you must have superuser privileges to provision SNMP community strings. In releases 4.3 and higher, you can provision SNMP community strings with the provisioning privilege.

- a. Configure the read-only community string.

For example:

```
bti7800(config)# snmp-server community R0 password
bti7800(config-community-R0)# commit
Commit complete.
bti7800(config-community-R0)# exit
bti7800(config)#
```

- b. Configure the read-write community string.

For example:

```
bti7800(config)# snmp-server community RW password
bti7800(config-community-RW)# commit
Commit complete.
bti7800(config-community-RW)# exit
bti7800(config)#
```

- c. Display the new configuration.

For example:

```
bti7800(config)# do show running-config snmp-server community

snmp-server community RW
password
!
snmp-server community R0
password
!
```

2. Configure the trap receiver.

- a. Specify the IP address of the trap receiver.

For example:

```
bt17800(config)# snmp-server host 10.1.1.1
bt17800(config-host-10.1.1.1)# commit
Commit complete.
bt17800(config-host-10.1.1.1)# exit
bt17800(config)#
```

- b. Repeat until you have configured all trap receivers.
- c. Display the trap receivers.

For example:

```
bt17800(config)# do show snmp host
```

Target-Name	IP-Address	Port	TimeOut-Value	Retry-Count	Tag-List
10.1.1.1 v2	10.1.1.1	162	1500	3	std_v2_t
10.2.2.2 v2	10.2.2.2	162	1500	3	std_v2_t

Release History Table

Release	Description
4.3	In releases 4.3 and higher, you can provision SNMP community strings with the provisioning privilege.

CHAPTER 10

NETCONF

- [About NETCONF on page 199](#)
- [Supported Features on page 201](#)
- [Event Notification Streams on page 202](#)
- [Supported YANG Modules on page 202](#)

About NETCONF

The Network Configuration protocol (NETCONF) is a network management protocol that enables management stations to monitor and configure network elements. Using XML encoding, NETCONF defines a set of operations for retrieving and modifying data from a device.

NETCONF is designed to have the following characteristics:

- **Atomicity**—Each transaction is atomic and cannot be divided. A transaction either succeeds or fails. If part of a transaction fails, the entire transaction fails.
- **Consistency**—The database is always consistent. All changes that are allowed to take place in the database are valid and compatible. Only successful transactions modify the database. Failed transactions do not modify the database in any way.
- **Isolation**—Transactions are isolated from each other. Only one transaction can apply to the database at any time. When multiple transactions are issued, the network element applies them sequentially.
- **Durability**—Committed data is stored in persistent memory that survives network element restarts and power outages.

[Figure 8 on page 200](#) shows a representation of how NETCONF can be conceptualized.

Figure 8: NETCONF Layers

Content	Network element YANG modules
Operations	Data retrieval and modification primitives (including filtering)
Messages	RPC-like communication and notifications
Secure Transport	Connection-oriented secure and reliable transport

The Secure Transport layer provides a secure and reliable connection for in-order delivery of NETCONF messages. An example of a secure transport protocol that meets NETCONF requirements is SSH. Support for NETCONF over SSH is mandatory.

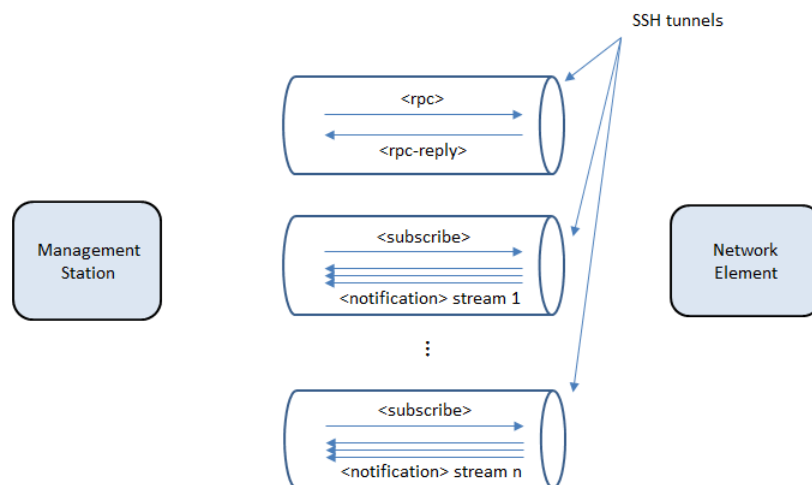
The Messages layer provides an RPC-like communication model to frame NETCONF requests and responses over the reliable transport provided by the Secure Transport layer. In the network receive direction, network data is read and delineated into NETCONF messages to present to the Operations layer. In the network transmit direction, RPCs from the Operations layer are framed and passed down to the Secure Transport layer for transmission.

The Operations layer provides the set of management primitives for retrieving and modifying NE data. This layer defines NETCONF protocol operations.

The Content layer consists of NE data represented by YANG modules. To allow ease of management, YANG modules clearly distinguish between NE configuration data and NE operational data.

Figure 9 on page 200 shows the communication connections between a management station and a network element.

Figure 9: Management Station to Network Element Communication Using NETCONF



The management station (NETCONF client) connects to the network element (NETCONF server) using a secure transport protocol. There is one connection for retrieving and modifying NE data, and one or more connections for notifications. When subscribing to notifications, the NETCONF client specifies the events of interest, and the NETCONF server sends matching events to the NETCONF client asynchronously when those events occur. Only subscribing clients receive notifications.

The BT17800 automatically accepts NETCONF session requests from authenticated users. No configuration is necessary to set up NETCONF on the BT17800.

Supported Features

Features	Support
NETCONF version	NETCONF 1.0, 1.1
Secure transport	SSH
Protocol operations	<ul style="list-style-type: none"> close-session: gracefully terminates the current NETCONF session create-subscription: subscribes to an event notification stream edit-config: modifies the configuration database get: retrieves data from the running configuration and NE statistics get-config: retrieves data from the running configuration kill-session: forces the termination of the specified NETCONF session
Capabilities	<ul style="list-style-type: none"> notification: supports delivery of asynchronous event notifications url: supports the <code><url></code> element in protocol operation <code><source></code> and <code><target></code> parameters writable-running: supports direct writes to the running configuration datastore xpath: supports XPath expressions in the <code><filter></code> element in information retrieval and notification subscription requests
Base notifications (NETCONF stream)	<ul style="list-style-type: none"> netconf-config-change: generated when the running configuration has been changed netconf-capability-change: generated when the capabilities have changed netconf-session-start: generated when a NETCONF session has started netconf-session-end: generated when a NETCONF session has ended
NETCONF protocol monitoring	<ul style="list-style-type: none"> capabilities: list of capabilities supported datastores: list of configuration datastores supported schemas: list of data model schemas supported sessions: list of all currently active NETCONF sessions statistics: NETCONF protocol counters get-schema: operation used to retrieve a schema
BT17800-specific YANG modules	See “Supported YANG Modules” on page 202 .

Event Notification Streams

The following event notification streams are supported:

Notification streams	Description
NETCONF	This is the standard stream for NETCONF base notifications.
DatabaseChange	Stream for database change notifications.
UpgradeEvent	Stream for software upgrade notifications.
DBRestoreBackup	Stream for configuration database restore backup and undo notifications.
StatusChange	Stream for status attribute change notifications.
ProtectionSwitch	Stream for protection switch notifications.



NOTE: The streams are not replay-capable.

Supported YANG Modules

The BT17800 YANG modules can be downloaded from <https://www.juniper.net/support/downloads> by selecting the desired product and release.

The following table lists the BT17800-specific YANG modules and indicates whether they can be used by third-party NETCONF clients. Only those modules labeled as "usable" can be used by customers running third-party clients. All other modules are for internal use or for the use of the prNX Service Manager.

Module	Description	Supported for third-party NETCONF clients	Introduced in Release
atlas-aaa.yang	The module defining user profile parameters.	Not for use by third-party NETCONF clients.	Before 2.1.1
atlas-amp.yang	The submodule defining 96-Channel Amplifier (AMPI) modules.	Not for use by third-party NETCONF clients.	Before 2.1.1
atlas-circuits.yang	The submodule defining transport cross-connects.	Not for use by third-party NETCONF clients.	Before 2.1.1
atlas-conditions.yang	The module defining BT17800 alarms and conditions.	Usable for fault management.	Before 2.1.1

Module	Description	Supported for third-party NETCONF clients	Introduced in Release
atlas-debug.yang	The submodule defining debug data.	Not for use by third-party NETCONF clients.	Before 2.1.1
atlas-dol-common.yang atlas-dol-hidden.yang atlas-dol.yang	Modules and submodules defining ROADM objects and parameters.	Not for use by third-party NETCONF clients.	2.1.1
atlas-equipment.yang	The submodule defining equipment objects.	Usable for inventory management.	Before 2.1.1
atlas-eth-if.yang	The submodule defining Ethernet interfaces.	Not for use by third-party NETCONF clients.	Before 2.1.1
atlas-if-protection.yang	The submodule defining interface protection.	Not for use by third-party NETCONF clients.	Before 2.1.1
atlas-interfaces.yang	The module defining interfaces.	Not for use by third-party NETCONF clients.	Before 2.1.1
atlas-internal.yang	The module defining internal objects.	Not for use by third-party NETCONF clients.	Before 2.1.1
atlas-lldp.yang	The submodule defining the information contained in LLDP TLVs (used for LLDP snooping).	Not for use by third-party NETCONF clients.	4.1
atlas-logging.yang	The submodule defining logging.	Not for use by third-party NETCONF clients.	Before 2.1.1
atlas-mgmt-interface.yang atlas-mgt-comn.yang atlas-mgt-static.yang atlas-mgt-vrf.yang atlas-mgt.yang	Modules and submodules defining management and management networking objects and parameters.	Not for use by third-party NETCONF clients.	2.1.1
atlas-notif.yang	The submodule defining notifications.	Not for use by third-party NETCONF clients.	Before 2.1.1
atlas-och-if.yang	The submodule defining OCH interfaces on the UFM6.	Not for use by third-party NETCONF clients.	4.1
atlas-otn-if.yang	The submodule defining OTU and ODU interfaces.	Not for use by third-party NETCONF clients.	Before 2.1.1
atlas-phy-if.yang	The submodule defining physical layer attributes common to all interfaces.	Not for use by third-party NETCONF clients.	Before 2.1.1

Module	Description	Supported for third-party NETCONF clients	Introduced in Release
atlas-products.yang	The module defining BT17800 orderable products.	Not for use by third-party NETCONF clients.	Before 2.1.1
atlas-snmp.yang	The module defining SNMP objects and parameters and inventory.	Not for use by third-party NETCONF clients.	Before 2.1.1
atlas-sonet-if.yang	The submodule defining SONET and SDH interfaces.	Not for use by third-party NETCONF clients.	Before 2.1.1
atlas-statistics.yang	The submodule defining PMs and statistics.	Usable for performance management. Not for historical PM use.	Before 2.1.1
atlas-systemDateTime.yang	The module defining system date and time.	Required by atlas-system.yang.	Before 2.1.1
atlas-system.yang	The submodule defining system-level attributes.	Usable for network element discovery. Requires atlas-systemDateTime.yang.	Before 2.1.1
atlas-types.yang	The module defining common parameter types used in other modules and submodules.	Required by most modules and submodules. Should be included for all use cases.	Before 2.1.1
atlas-user.yang	The submodule defining user management and authentication.	Not for use by third-party NETCONF clients.	Before 2.1.1
atlas-virtual-if.yang	The submodule defining virtual interfaces.	Not for use by third-party NETCONF clients.	2.1.1
atlas-wavelength-protection.yang	The submodule defining WPS protection groups.	Not for use by third-party NETCONF clients.	Before 2.1.1
atlas.yang	A top-level module containing various submodules.	Not for use by third-party NETCONF clients.	Before 2.1.1



NOTE: In addition to the BT17800 YANG modules, the BT17800 YANG implementation depends on a number of standard YANG modules. These are also supplied by Juniper Networks.

CHAPTER 11

Performance Monitoring

- [Statistics Collecting and Archiving on page 205](#)
- [Module and Device Statistics on page 205](#)
- [Optical and Physical Layer Statistics on page 206](#)
- [Protocol Statistics on page 210](#)
- [Effect of a Time Change on PMs on page 216](#)

Statistics Collecting and Archiving

The BT17800 provides comprehensive performance monitoring capabilities on all provisioned ports and interfaces. Performance monitoring statistics are continually collected and archived for physical device and optical performance parameters, as well as protocol-based counters and measurements.

- Up to 96 x 15-minute historical bins and 7 x 1-day historical bins are retained.
- Four current PM intervals are supported: 1 day, 15 minutes, 1 minute, untimed. The unTimed bin accumulates counts from the time performance monitoring on the module starts and does not roll over into a historical bin.
- Three historical PM intervals are supported: 1 day, 15 minutes, 1 minute

Module and Device Statistics

Table 30: Module and Device Statistics

Counter	Description	Units
cpu-load-avg	CPU load (average). The average of the 1-minute CPU load readings within the selected bin. CPU load is measured over 1-minute intervals.	%
cpu-load-max	CPU load (maximum). The maximum of the 1-minute CPU load readings within the selected bin.	%
cpu-load-min	CPU load (minimum). The minimum of the 1-minute CPU load readings within the selected bin.	%

Table 30: Module and Device Statistics (continued)

Counter	Description	Units
mod-temp	Module temperature.	°C
mod-temp-avg	Module temperature (average).	°C
mod-temp-max	Module temperature (maximum).	°C
mod-temp-min	Module temperature (minimum).	°C
volt	Supply voltage.	V
volt-avg	Supply voltage (average).	V
volt-max	Supply voltage (maximum).	V
volt-min	Supply voltage (minimum).	V

Optical and Physical Layer Statistics

Performance monitoring is conducted on a number of optical and physical layer attributes on UFM and optical modules.

Table 31: Optical Statistics

Counter	Description	Units
cc-opr	Coherent channel power received.	dBm
cc-opr-avg	Coherent channel power received (average).	dBm
cc-opr-max	Coherent channel power received (maximum).	dBm
cc-opr-min	Coherent channel power received (minimum).	dBm
cd	Chromatic dispersion. The chromatic dispersion of the received signal.	ps/nm
cd-avg	Chromatic dispersion (average).	ps/nm
cd-max	Chromatic dispersion (maximum).	ps/nm
cd-min	Chromatic dispersion (minimum).	ps/nm
cfo	Carrier frequency offset. The carrier frequency offset of the received signal.	MHz
cfo-avg	Carrier frequency offset (average).	MHz

Table 31: Optical Statistics (continued)

Counter	Description	Units
cfo-max	Carrier frequency offset (maximum).	MHz
cfo-min	Carrier frequency offset (minimum).	MHz
dgd	Differential group delay. The differential group delay of the received signal.	ps
dgd-avg	Differential group delay (average).	ps
dgd-max	Differential group delay (maximum).	ps
dgd-min	Differential group delay (minimum).	ps
fec-0cr	Number of bits corrected to 0	—
fec-1cr	Number of bits corrected to 1	—
fec-ber	FEC bit error rate	—
fec-ber-avg	FEC bit error rate (average)	—
fec-ber-maximum	FEC bit error rate (maximum)	—
fec-ber-minimum	FEC bit error rate (minimum)	—
fec-ber-delta-q	Delta Q of x and y polarization	dB
fec-ber-delta-q-min	Delta Q of x and y polarization (minimum)	dB
fec-ber-delta-q-max	Delta Q of x and y polarization (maximum)	dB
fec-ber-x-corr	X-polarization FEC bit error ratio	—
fec-ber-x-corr-max	X-polarization FEC bit error ratio (maximum)	—
fec-ber-x-corr-min	X-polarization FEC bit error ratio (minimum)	—
fec-ber-x-q	X-polarization pre-FEC Q	dB
fec-ber-x-q-max	X-polarization pre-FEC Q (maximum)	dB
fec-ber-x-q-min	X-polarization pre-FEC Q (minimum)	dB
fec-ber-y-corr	Y-polarization FEC bit error ratio	—
fec-ber-y-corr-max	Y-polarization FEC bit error ratio (maximum)	—

Table 31: Optical Statistics (continued)

Counter	Description	Units
fec-ber-y-corr-min	Y-polarization FEC bit error ratio (minimum)	–
fec-ber-y-q	Y-polarization pre-FEC Q	dB
fec-ber-y-q-max	Y-polarization pre-FEC Q (maximum)	dB
fec-ber-y-q-min	Y-polarization pre-FEC Q (minimum)	dB
fec-bitcr	FEC bits corrected.	–
fec-ucrcw	FEC uncorrectable codewords.	–
lbc	Laser bias current.	mA
lbc-avg	Laser bias current (average).	mA
lbc-max	Laser bias current (maximum).	mA
lbc-min	Laser bias current (minimum).	mA
ltemp	Laser temperature.	°C
ltemp-avg	Laser temperature (average).	°C
ltemp-max	Laser temperature (maximum).	°C
ltemp-min	Laser temperature (minimum).	°C
opt-back-ref-ratio	Optical back-reflection ratio The ratio of optical back reflection.	dB
opt-back-ref-ratio-min	Optical back-reflection ratio (minimum)	dB
opt-back-ref-ratio-max	Optical back-reflection ratio (maximum)	dB
opt-back-ref-ratio-avg	Optical back-reflection ratio (average)	dB
opt-back-ref-ratio-std-avg	Optical back-reflection ratio (standard deviation from average)	dB
opl-rx	Optical power loss receive. The optical power loss in the receive direction.	dB
opl-rx-avg	Optical power loss receive (average).	dB
opl-rx-max	Optical power loss receive (maximum).	dB

Table 31: Optical Statistics (continued)

Counter	Description	Units
opl-rx-min	Optical power loss receive (minimum).	dB
opr	Optical power received.	dBm
opr-avg	Optical power received (average).	dBm
opr-max	Optical power received (maximum).	dBm
opr-min	Optical power received (minimum).	dBm
opr-std-avg	Optical power received (standard deviation). An approximation of the variance of the power samples of the received optical signal.	dBm
opt	Optical power transmitted.	dBm
opt-avg	Optical power transmitted (average).	dBm
opt-max	Optical power transmitted (maximum).	dBm
opt-min	Optical power transmitted (minimum).	dBm
opt-std-avg	Optical power transmitted (standard deviation). An approximation of the variance of the power samples of the transmitted optical signal.	dBm
opt-total	Total (signal and noise) optical power transmitted.	dBm
opt-total-avg	Total (signal and noise) optical power transmitted (average).	dBm
opt-total-max	Total (signal and noise) optical power transmitted (maximum).	dBm
opt-total-min	Total (signal and noise) optical power transmitted (minimum).	dBm
osnr	Optical signal to noise ratio. The signal to noise ratio of the received optical signal.	dB
osnr-avg	Optical signal to noise ratio (average).	dB
osnr-max	Optical signal to noise ratio (maximum).	dB
osnr-min	Optical signal to noise ratio (minimum).	dB
snr	Signal to noise ratio. The signal to noise ratio of the received signal.	dB

Table 31: Optical Statistics (continued)

Counter	Description	Units
snr-avg	Signal to noise ratio (average).	dB
snr-max	Signal to noise ratio (maximum).	dB
snr-min	Signal to noise ratio (minimum).	dB
snr-x	X-polarization signal to noise ratio. The X-polarization signal to noise ratio of the received optical signal.	dB
snr-x-avg	X-polarization signal to noise ratio (average).	dB
snr-x-max	X-polarization signal to noise ratio (maximum).	dB
snr-x-min	X-polarization signal to noise ratio (minimum).	dB
snr-y	Y-polarization signal to noise ratio. The Y-polarization signal to noise ratio of the received optical signal.	dB
snr-y-avg	Y-polarization signal to noise ratio (average).	dB
snr-y-max	Y-polarization signal to noise ratio (maximum).	dB
snr-y-min	Y-polarization signal to noise ratio (minimum).	dB
span-length	The span length.	km

Protocol Statistics

Table 32: OTU Protocol Statistics

Counter	Description	Units
otu-bbe	OTU background block errors.	—
otu-ber	OTU bit error rate.	—
otu-ber-avg	OTU bit error rate (average).	—
otu-ber-max	OTU bit error rate (maximum).	—
otu-ber-min	OTU bit error rate (minimum).	—
otu-eb	OTU errored blocks.	—
otu-es	OTU errored seconds.	s

Table 32: OTU Protocol Statistics (continued)

Counter	Description	Units
otu-ofs	OTU out of frame seconds.	s
otu-ses	OTU severely errored seconds.	s
otu-uas	OTU unavailable seconds.	s

Table 33: ODU Protocol Statistics

Counter	Description	Units
odu-bbe	ODU background block errors.	—
odu-ber	ODU bit error rate.	—
odu-ber-avg	ODU bit error rate (average).	—
odu-ber-max	ODU bit error rate (maximum).	—
odu-ber-min	ODU bit error rate (minimum).	—
odu-eb	ODU errored blocks.	—
odu-es	ODU errored seconds.	s
odu-ses	ODU severely errored seconds.	s

Table 34: SONET Protocol Statistics

Counter	Description	Units
ber-l	Bit error rate instantaneous, line	—
ber-avg-l	Bit error rate average, line	—
ber-max-l	Bit error rate maximum, line	—
ber-min-l	Bit error rate minimum, line	—
cv-l	Coding violations, line	—
es-l	Errored seconds, line	s
fc-l	Failure count, line	—
ses-l	Severely errored seconds, line	s
ber-s	Bit error rate instantaneous, section	—

Table 34: SONET Protocol Statistics (continued)

Counter	Description	Units
ber-avg-s	Bit error rate average, section	—
ber-max-s	Bit error rate maximum, section	—
ber-min-s	Bit error rate minimum, section	—
cv-s	Coding violations, section	—
es-s	Errored seconds, section	s
sefs-s	Severely errored frame seconds, section	s
ses-l	Severely errored seconds, section	s

Table 35: SDH Protocol Statistics

Counter	Description	Units
ms-ber	Bit error rate instantaneous, multiplex section	—
ms-ber-avg	Bit error rate average, multiplex section	—
ms-ber-max	Bit error rate maximum, multiplex section	—
ms-ber-min	Bit error rate minimum, multiplex section	—
ms-bbe	Background block errors, multiplex section	—
ms-eb	Errored blocks, multiplex section	—
ms-es	Errored seconds, multiplex section	s
ms-ses	Severely errored seconds, multiplex section	s
rs-ber	Bit error rate instantaneous, regenerator section	—
rs-ber-avg	Bit error rate average, regenerator section	—
rs-ber-max	Bit error rate maximum, regenerator section	—
rs-ber-min	Bit error rate minimum, regenerator section	—
rs-bbe	Background block errors, regenerator section	—
rs-eb	Errored blocks, regenerator section	—
rs-es	Errored seconds, regenerator section	s

Table 35: SDH Protocol Statistics (continued)

Counter	Description	Units
rs-ofs	Out of frame seconds, regenerator section	s
rs-ses	Severely errored seconds, regenerator section	s

Table 36: Ethernet Layer 1 Statistics

Counter	Description	Units
pcs-ses	Severely errored seconds. The number of seconds during which any of the following occurs on the Ethernet interface or on a channel of the Ethernet interface: <ul style="list-style-type: none"> • Loss of Signal • Loss of Sync 	s

Table 37: Ethernet Layer 2 Statistics

Counter	Description	Units
bcast-pkts-rx	Broadcast packets received. The number of packets received excluding bad packets that are directed to a broadcast address.	—
bcast-pkts-tx	Broadcast packets transmitted.	
drp-pkts-rx	Dropped packets received. The number of packets that should be received by the device, but are not accepted due to an internal MAC sublayer receive error (that is, FIFO overrun).	—
fcse-pkts-rx	FCS error packets received. The number of packets received with a valid length but have either a bad Frame Check Sequence (FCS) or a bad FCS with a non-integral number of octets (Alignment Error).	—
fragments-rx	Fragments received.	
jabbers-rx	Jabbers received. The number of packets received that are longer than the maximum permitted packet size and have a bad Frame Check Sequence (FCS).	—
mcast-pkts-rx	Multicast packets received. The number of packets received excluding bad packets that are directed to a unicast address.	—

Table 37: Ethernet Layer 2 Statistics (continued)

Counter	Description	Units
mcast-pkts-tx	Multicast packets transmitted.	
octs-ok-rx	Good octets received. The total number of octets received excluding those counted in bad packets.	—
octs-ok-tx	Good octets transmitted.	
octs-rx	Total octets received. The total number of octets received including those counted in bad packets.	—
osize-pkts-rx	Oversized packets received. The number of packets received with more octets than the maximum permitted packet size (9600) and without errors.	—
pkts-paus-rx	Pause packets received.	
pkts-ok-rx	Good packets received. The total number of packets received excluding bad packets.	—
pkts-ok-tx	Good packets transmitted.	
pkts-rx	Total packets received. The total number of packets received including bad packets.	—
pkts-tx	Total packets transmitted. The total number of packets transmitted.	—
pkts-64-oct-rx	64 byte packets received. The total number of packets (including bad packets) received that are 64 octets in length (excluding framing bits but including FCS octets).	—
pkts-65-127-oct-rx	65 to 127 byte packets received. The total number of packets (including bad packets) received that are between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).	—
pkts-128-255-oct-rx	128 to 255 byte packets received. The total number of packets (including bad packets) received that are between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).	—

Table 37: Ethernet Layer 2 Statistics (continued)

Counter	Description	Units
pkts-256-511-oct-rx	256 to 511 byte packets received. The total number of packets (including bad packets) received that are between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).	—
pkts-512-1023-oct-rx	512 to 1023 byte packets received. The total number of packets (including bad packets) received that str between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).	—
pkts-1024-1518-oct-rx	1024 to 1518 byte packets received. The total number of packets (including bad packets) received that are between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).	—
pkts-over-1518-oct-rx	Packets over 1518 bytes received. The total number of packets (including bad packets) received that are between 1518 octets and the maximum Jumbo frame length (9600 octets), excluding framing bits but including FCS octets.	—
usize-pkts-rx	Undersized packets received. The number of packets received with fewer octets than the minimum permitted packet size (64) and without errors.	—

Table 38: Fibre Channel Statistics

Counter	Description	Units
pcs-ses	Severely errored seconds. The number of seconds during which any of the following occurs on the Fibre channel interface: <ul style="list-style-type: none"> • High BER • Loss of Signal • Loss of Sync • 8554 or more invalid blocks (applies to 10gfc interfaces) • 6845 or more invalid blocks (applies to 8gfc interfaces) The PCS-SES count is not incremented during seconds which are counted as PCS-UAS seconds.	s
pktsfcserx	FCSE packets. The number of packets received that had a valid length but had either a bad Frame Check Sequence (FCS) or a bad FCS with a non-integral number of octets (Alignment Error).	—

Effect of a Time Change on PMs

When the time is changed on the BTI7800, the timestamps on the current bins are not automatically adjusted.

To propagate the time change to the current PMs, perform a warm reload (**system reload warm module**) of the service modules after changing the time.

To avoid this, make sure the system time is synchronized with reliable NTP servers.

CHAPTER 12

Fault Monitoring and Reporting

- [Fault Monitoring on page 217](#)
- [Fault Reporting on page 217](#)
- [Fault Hierarchy on page 218](#)
- [Fault Severity on page 218](#)
- [Alarms and Conditions on page 219](#)

Fault Monitoring

Fault monitoring is conducted both at the physical layer, covering optical signals and channel-specific transceiver faults, and at the protocol layer with specific fault points defined for all the supported protocols. Monitoring is also conducted on the supporting BT17800 equipment, including the monitoring of the various sensors located throughout the chassis and on the modules.

A fault can be either an alarm or a condition. An (unmasked) alarm provides notification of a fault as the fault occurs. A condition is a fault that does not provide a notification, and is generally used for lower severity faults. You can configure whether a fault is an alarm or a condition by using the **conditions settings** CLI command. Alarms and conditions can be viewed through the **show alarms** and **show conditions** commands respectively.

Additionally, an alarm can be masked by other alarms. Alarm masking refers to the suppression of one or more alarm notifications because of the existence of another alarm indicating a higher priority fault or more accurately identifies the source of a fault. In this way, the operator does not get flooded with alarms when a fault occurs, thereby enabling quicker fault isolation and resolution.

Refer to “[Alarms and Conditions](#)” on [page 219](#) for the full list of alarms and conditions. For detailed information, see the *BT17800 Series Alarm and Troubleshooting Guide*.

Fault Reporting

Fault reporting is managed by setting the fault severity as follows:

- **critical/major/minor**: Active faults with critical, major or minor severity are reported with an autonomous alarm notification when the fault becomes active. When the fault is no longer active, a condition clear alarm is generated. All active faults, alarmed or non-alarmed, can be polled by retrieving a list of active conditions (**show conditions**).

All active faults with critical, major or minor severity alarm notifications can be polled by retrieving a list of active alarms (**show alarms**).

- **not-alarmed**: No notifications are generated when faults become active or are cleared, but the faults that are active can be polled by retrieving a list of active conditions (**show conditions**).

Additionally, a fault can be enabled or disabled. When a fault is disabled, the fault is not alarmed and does not appear in the output of the **show alarms** or **show conditions** command. By default, all faults are enabled.

Fault Hierarchy

When multiple faults are active against an entity, one or more faults might be suppressed from reporting according to the masking relationships that exist for the object's fault points. Masking of fault points is important in assisting with fault isolation when a single root cause might lead to multiple fault points being raised.

Masking relationships might also exist between fault points raised against different monitored objects. For example, if a Loss of Frame (LOF) fault is active against a single channel on an interface port, it masks the LOF fault against the interface entity, and so the reporting of the interface LOF condition is suppressed.

Fault Severity

Each fault point is associated with one of the following default severity types.

Table 39: Fault Severity

Severity	Description
Critical	A failure that is likely causing serious loss or interruption of traffic.
Major	A failure that could potentially lead to loss or interruption of traffic.
Minor	A failure that does not significantly affect traffic.
Not alarmed	A fault that results in a standing condition, not an alarm.
Not reported	A minor, major, or critical alarm not reported, because it is being masked by another alarm.

Faults with NR severity always behave as non-alarmed conditions. Notifications for raise and clear events are never generated for these faults, and active occurrences can be discovered only when the active conditions list is polled.

Alarms and Conditions

Table 40: Alarms and Conditions

Alarm/condition	Description	Default Severity	Service Affecting
airFilterAbsence	Air filter absent. No air filter has been detected in the BT17814 chassis. An air filter is mandatory in the BT17814 chassis. This alarm does not apply to the other chassis types.	Major	No
ais-l	Alarm indication signal, line, SONET. The local port has received an AIS-L signal from the NE at the far end of the fiber. This indicates that an SF condition exists upstream of (and towards) the local node.	Not alarmed	Yes
apr	Automatic power reduction. For safety reasons, the local port has automatically reduced laser power because it has detected optical back reflection exceeding the high threshold. This can occur if the fiber is not plugged in properly.	Critical	Yes
apsd	Automatic power shutdown. The local port has automatically shut down its laser because the receive optical power has dropped below the receive LOL threshold. This can occur if the fiber is not plugged in properly or if there is a problem at the far-end transmitter or if there is a problem in the fiber itself.	Critical	Yes
bdi	Backward defect indication, OTN. The local port has received a BDI signal from the NE at the far end of the fiber. This indicates that an SF condition exists downstream of (and away from) the local node.	Not alarmed	No
cfgFail	A 40ge interface has been provisioned on a client port on a UFM6, but the UFM6 cannot accept the provisioning because the correct SERDES configuration has not been applied. To apply the SERDES configuration, reseal or perform a cold reload of the UFM.	Not reported	Yes
contComS	Control communications failure, span section, amplifier. OSC control communications with the NE at the far end of the span section have failed. Check for OSC alarms on the far end NE and resolve.	Major	Yes

Table 40: Alarms and Conditions (continued)

Alarm/condition	Description	Default Severity	Service Affecting
diskHighUsage	<p>Disk high usage. Disk usage has exceeded 90%. This is typically caused by an over-accumulation of log files.</p> <p>Use the CLI logging commands to delete unwanted log files, to move log files off the NE, or to set up automatic log rotation.</p> <p>This alarm clears when disk usage falls below 70%.</p>	Major	No
envCurrentHighTh	Current above high threshold. The output current at the AC PEM is above the high current threshold.	Major	Yes
envCurrentLowTh	Current below low threshold. The output current at the AC PEM is below the low current threshold.	Major	Yes
envTempHighTh	Environment temperature above high threshold. The temperature at the indicated module has exceeded the high temperature threshold. The fan speed in the chassis is increased to the maximum.	Major	Yes
envTempLowTh	Environment temperature above low threshold. The temperature at the indicated module has exceeded (above) the low temperature threshold. The fan speed in the chassis begins to increase.	Not alarmed	Yes
envVoltHighTh	<p>Environment voltage above high threshold on the AC PEM.</p> <p>The input AC voltage is greater than 255 VAC.</p> <p>Continued operation might cause equipment damage.</p>	Major	Yes
envVoltLowTh	<p>Environment voltage below low threshold (on the PEM).</p> <p>AC PEM: The input AC voltage is less than 90 VAC.</p> <p>DC PEM: The input DC voltage is less than 40 VDC.</p> <p>Continued operation might cause equipment damage.</p>	Major	Yes
eqptBrownout	<p>Equipment brownout. The input voltage to a UFM has dropped below the brownout threshold.</p> <p>UFM3 and UFM4 modules are automatically cold reloaded.</p>	Major	Yes
eqptComm	Equipment management communications failure. The CMM is not able to communicate with the specified equipment. Depending on the reason behind this alarm, traffic might be affected.	Major	Yes
eqptDgrd	Equipment degrade. This is raised when UFM or BIC initialization fails.	Major	Yes

Table 40: Alarms and Conditions (continued)

Alarm/condition	Description	Default Severity	Service Affecting
eqptFail	Equipment fail. Either a hardware self test has detected faulty hardware or an automatic re-timer firmware upgrade has failed.	Critical	Yes
eqptMism	Equipment mismatch. The installed equipment does not match the provisioned equipment.	Critical	Yes
eqptMiss	Equipment missing. Equipment is provisioned but not physically installed.	Critical	Yes
fanSpeedLowTh	Fan speed below low threshold. This can be caused by a faulty cooling unit or by a problem with the power entry module.	Major	Yes
feci	Far end node configuration mismatch. Verify the configuration at the far end NE.	Major	Yes
feim	Far end node identification mismatch. Verify the configuration at the far end NE.	Major	Yes
firmUpgrdInProg	Firmware upgrade in progress.	Not alarmed	No
firmUpgrdFail	Firmware upgrade failed.	Major	No
firmUpgrdReqd	Firmware upgrade required. The version of firmware running on the module does not match the version of firmware required by the current software load.	Major	No
forced	Forced protection switch active. The operator has forced a protection switch. The force remains active until a switch release is invoked.	Not alarmed	No
highBer	High bit error rate. The local port has detected a bit error rate in the received signal higher than the threshold. This can be caused by a problem in the fiber or by excessive attenuation in the signal.	Major	No
invUnknown	Inventory unknown. The installed equipment is not recognized. Ensure that the software version supports the specified equipment.	Major	No
inventoryUnsupp	Inventory item not supported. A QSFP28 transceiver is installed in a port that supports only QSFP+ transceivers.	Major	Yes

Table 40: Alarms and Conditions (continued)

Alarm/condition	Description	Default Severity	Service Affecting
isisAdjDown	IS-IS adjacency down. An IS-IS adjacency has gone down. This link will no longer be considered for routing.	Major	Yes
laserFail	Laser failure.	Critical	Yes
laserTempHighTh	Laser temperature above high temperature threshold.	Major	No
laserTempLowTh	Laser temperature below low temperature threshold.	Major	No
lck	ODU locked. The port has received an ODU-LCK signal from the NE at the far end of the fiber. This indicates that a transmitting interface at an upstream node has been administratively disabled.	Critical	Yes
lf	Local fault. The local port has received an LF signal from the NE at the far end of the fiber. This indicates that an SF condition exists upstream of the local node.	Not alarmed	No
lockout	Lockout of protection. The operator has locked out a line for protection. The lockout protection switch remains active until a switch release is invoked.	Not alarmed	No
lof	Loss of frame alignment.	Critical	Yes
lolightRx	Loss of light, receive. The optical power received has dropped below the LOL threshold. NOTE: In some ROADM network topologies with ILAs deployed, amplified spontaneous emissions (ASE) might accumulate sufficiently to cause this alarm to clear on provisioned but unoccupied optical channels. (The ASE will not be high enough to affect optical performance, however.)	Critical	Yes
lolightTx	Loss of light, transmit. The optical power transmitted has dropped below the LOL threshold. NOTE: In some ROADM network topologies with ILAs deployed, amplified spontaneous emissions (ASE) might accumulate sufficiently to cause this alarm to clear on provisioned but unoccupied optical channels. (The ASE will not be high enough to affect optical performance, however.)	Major	Yes
lom	Loss of multiframe. The multiframe alignment process is in the out-of-multiframe (OOM) state.	Critical	Yes
los	Loss of signal. The local port has detected a loss of received signal power.	Critical	Yes

Table 40: Alarms and Conditions (continued)

Alarm/condition	Description	Default Severity	Service Affecting
loSpecRx	Loss out of specification, receive. The optical receive loss is outside the allowable range configured.	Critical	Yes
loSync	Loss of synchronization. The received signal cannot be synchronized.	Critical	Yes
lpbk	Loopback operated. The operator has initiated loopback on the local port.	Not alarmed This setting should not be changed.	No
memHighUsage	Memory high usage. Memory usage has exceeded 90%. This alarm clears when memory usage falls below 70%.	Major	No
modTempHighTh	Module temperature above high threshold. The temperature on the 100G Coherent MSA XCVR has exceeded the high temperature threshold.	Major	No
modTempLowTh	Module temperature below low threshold. The temperature on the 100G Coherent MSA XCVR is below the low temperature threshold.	Major	No
modTempShutdown	Module temperature shutdown. The 100G Coherent MSA XCVR has exceeded the high temperature shutdown threshold and has been shut down.	Critical	Yes
ms-ais	Multiplex section alarm indication signal, SDH. The local port has received an MS-AIS signal from the NE at the far end of the fiber. This indicates an SF condition upstream of the local node.	Not alarmed	Yes
ms-rdi	Multiplex section remote defect indication, SDH. The local port has received an MS-RDI signal from the NE at the far end of the fiber. This indicates an SF condition downstream of the local node.	Not alarmed	No
nonCoLocatedController	Controllers are in different chassis. In a multichassis configuration, the CMMs that act as the system controllers must be in the same chassis. Follow the instructions to set up a proper multichassis configuration.	Critical	Yes
obrHt	Optical back reflection high threshold exceeded. The optical back reflection has exceeded the high threshold. This can occur if the fiber is not plugged in properly.	Minor	Yes

Table 40: Alarms and Conditions (continued)

Alarm/condition	Description	Default Severity	Service Affecting
ochAis	Alarm indication signal, OCH. The OCH has received an AIS signal from the NE at the far end of the fiber. This indicates that an SF condition exists upstream of (and towards) the local node.	Not alarmed	Yes
ochOci	Open connection indication, OCH. The OCH has received an OCH-OCI signal from the NE at the far end of the fiber. This usually indicates a missing optical cross-connect upstream.	Critical	Yes
ochUeq	OCH unequipped.	Critical	Yes
oci	<p>Open connection indication, ODU. The interface has received an ODU-OCI signal from the NE at the far end of the fiber. This usually indicates a missing cross-connect upstream.</p> <p>NOTE: The local interface that receives the ODU-OCI signal raises this alarm only if the local interface is part of a cross-connect. If the local interface is not part of a cross-connect, the received ODU-OCI signal is ignored.</p> <p>An interface transmits an ODU-OCI signal downstream if the interface is open (that is, not part of any cross-connect).</p> <p>For multiplexed ODU interfaces, the ODU-OCI signal is transmitted (and therefore received) on the containing ODU interface, not on the individual ODU subinterfaces. The containing ODU interface transmits the ODU-OCI signal if none of the contained ODU subinterfaces is part of a cross-connect. The containing ODU interface stops transmitting the ODU-OCI signal if at least one of the contained ODU subinterfaces is part of a cross-connect. The ODU-OCI signal on multiplexed interfaces does not indicate which specific subinterface is open (that is, not part of a cross-connect).</p>	Critical	Yes
odtgMism	<p>ODTG Mismatch. The Optical Data Tributary Group (ODTG) configuration on a multiplexed interface is inconsistent at the two ends of the fiber. This means that the ODU subinterface cross-connected at the local end does not match the ODU subinterface cross-connected at the far end. This alarm is raised against the containing ODU4 interface.</p> <p>Verify that both ends are configured for the same ODU subinterface.</p>	Critical	Yes

Table 40: Alarms and Conditions (continued)

Alarm/condition	Description	Default Severity	Service Affecting
odu-ais	<p>ODU alarm indication signal. The interface has received an ODU-AIS signal from the NE at the far end of the fiber. This indicates that an SF condition exists upstream of (and towards) the local node.</p> <p>In addition to standard use of ODU-AIS signals, the BT17800 originates an ODU-AIS signal in the following situations:</p> <ul style="list-style-type: none"> • A multiplexed ODU subinterface transmits an ODU-AIS signal when the subinterface detects an ODTG tributary mismatch. See <i>odtgMism</i>. • On a UFM6, an optical channel transmits a default ODU4 signal containing ODU-AIS for each ODU4 interface not created. 	Not alarmed	Yes
oduMism	<p>ODU Mismatch. The ODU type in the received ODU signal does not match the expected type.</p> <p>Verify that both ends are configured for the same ODU (both ODU2 or both ODU2e or both ODU4).</p>	Not alarmed	No
omsAis	Alarm indication signal, OMS. The local OMS has received an AIS signal from the NE at the far end of the fiber. This indicates that an SF condition exists upstream of (and towards) the local node.	Not alarmed	Yes
oneCableDisconnected	One multichassis cable disconnected.	Major	Yes
oprHighTh	Optical power received above high threshold.	Major	No
oprLowTh	Optical power received below low threshold.	Major	No
oprHighFail	Optical power received high fail.	Not alarmed	No
optHighTh	Optical power transmitted above high threshold.	Major	No
optLowTh	Optical power received below low threshold.	Major	No
partitionFault	<p>Disk partition fault detected.</p> <p>Perform a warm reboot of the affected module.</p>	Major	No
posRxHigh	Receive power out of specification, high. The optical power received is above the high threshold.	Minor	Yes

Table 40: Alarms and Conditions (continued)

Alarm/condition	Description	Default Severity	Service Affecting
posRxLow	<p>Receive power out of specification, low. The optical power received is below the low threshold.</p> <p>NOTE: In some ROADM network topologies with ILAs deployed, amplified spontaneous emissions (ASE) might accumulate sufficiently to cause this alarm to clear on provisioned but unoccupied optical channels. (The ASE will not be high enough to affect optical performance, however.)</p>	Major	Yes
posTx	<p>Power out of specification, transmit. The optical power transmitted is below the POS low threshold, or above the POS high threshold.</p> <p>NOTE: In some ROADM network topologies with ILAs deployed, amplified spontaneous emissions (ASE) might accumulate sufficiently to cause this alarm to clear on provisioned but unoccupied optical channels. (The ASE will not be high enough to affect optical performance, however.)</p>	Critical	Yes
powerAbsent	<p>No power available.</p> <p>AC PEM: The input AC voltage to the PEM is less than 90 VAC or greater than 255 VAC, and the output DC voltage of the PEM is less than 40 VDC or greater than 60 VDC.</p> <p>DC PEM: The input and output DC voltages of the PEM are less than 40 VDC or greater than 60 VDC.</p> <p>Continued operation might cause equipment damage.</p>	Critical	Yes
prbs	PRBS test activated.	<p>Not alarmed</p> <p>This setting should not be changed.</p>	No
preFecBerTh	Pre-FEC bit error rate above high threshold.	Minor	No
pyldMism	<p>Payload mismatch, ODU. The expected payload type within the ODU signal is not the same as the received payload type.</p> <p>Verify the configuration along the payload path.</p>	Critical	Yes
rdi-l	Remote defect indication, line. The local port has received an RDI-L signal from the NE at the far end of the fiber. This indicates an SF condition exists downstream of the local node.	Not alarmed	No

Table 40: Alarms and Conditions (continued)

Alarm/condition	Description	Default Severity	Service Affecting
rf	Remote fault. The local port has received an RF signal from the NE at the far end of the fiber. This indicates that an SF condition exists at a node downstream of the local node.	Not alarmed	No
scmNmiDown	System controller management (SCM) interface down.	Major	Yes
scmNoNmConn	No network management connectivity on either system controller management (SCM) modules.	Critical	Yes
sd	Signal degrade. The local port is in a signal degrade state due to a sufficient number of errors in the received signal.	Minor	No
tLossRxHt	Loss above high threshold, receive. The measured optical power loss in the receive fiber is above the high threshold.	Minor	Yes
tLossRxLt	Loss below low threshold, receive. The measured optical power loss in the receive fiber is below the low threshold.	Minor	Yes
tim	Trace identifier mismatch. The expected trace identifier is different from the actual trace identifier received. Verify fiber connectivity and trace ID configuration at the far end. This alarm clears when the expected trace identifier is received.	Major	No
transmitterDegrade	Transmitter degrade (of the far-end transmitter). This alarm is raised by the receiver when the Delta-Q factor difference between X and Y polarization states of the received signal has reached the configured Delta-Q threshold. The alarm clears when the Delta-Q factor difference is below the configured Delta-Q threshold for three consecutive one-second intervals.	Major	No
upgr	Upgrade In progress. This alarm clears when the upgrade is finished.	Minor	Yes

Software and Firmware Upgrades

- [Upgrading the Software on page 229](#)
- [Upgrading the CMM Firmware on page 234](#)
- [Upgrading the Re-timer Firmware on a UFM6 on page 238](#)
- [Enabling Automatic CMM SHMM Firmware Upgrades on page 241](#)
- [Rolling Back a Software Upgrade on page 242](#)

Upgrading the Software

Use this procedure to upgrade the software on a BT17800. Upgrading the software is not service affecting. This procedure covers upgrading the software on the CMMs and on all of the traffic modules, but does not cover upgrading the firmware. For upgrading the CMM firmware, see [“Upgrading the CMM Firmware” on page 234](#).



NOTE: The system automatically upgrades traffic module firmware when needed. You do not need to explicitly upgrade firmware on the traffic modules.



WARNING: Service modules are automatically warm reloaded as part of this procedure. Software-based features on the service module (such as PM collection, APSD, APR, FPSD) are disabled while a service module warm reloads.

Prerequisites:

- In releases lower than release 4.3, you must have **superuser** privileges to upgrade the software. In releases 4.3 and higher, you can upgrade the software with the **provisioning** privilege.
- You have the IP address and login credentials of the (S)FTP server where the software package resides.
- The (S)FTP server must be reachable from the network on which the shared management IP address resides.

1. Log in to the CLI using the shared management IP address.

2. Verify that there are no alarms raised against the CMMs.

Use the **show alarms** command to view alarms on the chassis.

Resolve all CMM alarms before proceeding. You do not have to resolve non-CMM equipment alarms.



TIP: Use the **show alarms** command before and after the upgrade to determine if new alarms are raised from the upgrade.

3. If you are running with two CMMs, verify that the CMMs are synchronized.

The CMMs are synchronized when the HA Status is In Sync.

For example (only relevant output is shown):

```
bt17800# show system
Active Controller      : cmm:1/A
Backup Controller     : cmm:1/B
HA Status              : In Sync
```

4. Specify the IP address of the (S)FTP server, the login credentials, and the file path for the software package. The software is packaged as an RPM file.

For example:

```
bt17800# system upgrade remote-url
ftp://user@172.25.5.100/sw/bt17800-sys-1.6.0-14211.x86_64.rpm
Value for 'password' (<string>):
```

Enter the (S)FTP server password when prompted.

5. Verify that the remote-url has been specified correctly.

For example (actual output might differ):

```
bt17800# show system upgrade
Current Status        : URL set

Module   URL Status      URL
-----
cmm:1/A   URL set
ftp://user@172.25.5.100/sw/bt17800-sys-1.6.0-14211.x86_64.rpm
```

6. Start the download.

Use the **system upgrade download** command to start the download.

```
bti7800# system upgrade download
bti7800#
```

7. Check on the status of the download.

You can check on the status of the download by issuing the **show system upgrade** command periodically.

For example (partial output only, actual output might differ):

```
bti7800# show system upgrade

Current Status      : download-in-progress

Module   Download Status   Start Time           Notification Message
-----
cmm:1/A  download-in-progress 2015-01-20T19:48:30+00:00 Download in progress
100.0 MB Downloaded
```

```
bti7800# show system upgrade

Current Status      : download-in-progress

Module   Download Status   Start Time           Notification Message
-----
cmm:1/A  download-in-progress 2015-01-20T19:48:30+00:00 Download Finished
Unroll Started
```

```
bti7800# show system upgrade

Current Status      : download-success

Module   Download Status   Start Time           Notification Message
-----
cmm:1/A  download-success 2015-01-20T19:48:30+00:00 Download & Unroll
successful, Ready for Commit
```

The software package has been downloaded to local storage.

8. Use the **system upgrade commit** command to load the software packages onto the respective modules on the chassis.

For example:

```
bti7800# system upgrade commit
CAUTION: Would you like to Proceed? [no,yes] yes
```

9. Check on the status of the commit.

You can check on the status of the commit by issuing the **show system upgrade** command periodically.

For example (partial output only, actual output might differ):

```
bti7800# show system upgrade
```

```
Current Status      : commit-in-progress
```

Module	Commit Status	Commit Start Time	Notification Message
cmm:1/A	commit-in-progress	2015-01-20T19:51:54+00:00	COMMIT IN PROGRESS
cmm:1/B	commit-in-progress	2015-01-20T19:51:54+00:00	COMMIT IN PROGRESS



NOTE: The CMMs are upgraded first. When the CMMs are being upgraded, you will lose management connectivity. Wait several minutes before connecting to the shared management IP address again. Once you log back in, continue to check on the status of the commit.

```
bti7800# show system upgrade
```

```
Current Status      : commit-in-progress
```

Module	Commit Status	Commit Start Time	Notification Message
cmm:1/A	commit-success	2015-01-20T20:01:12+00:00	COMMIT SUCCESS
cmm:1/B	commit-success	2015-01-20T20:01:12+00:00	COMMIT SUCCESS
ufm:1/1	commit-success	2015-01-20T20:03:31+00:00	COMMIT SUCCESS
ufm:1/11	commit-success	2015-01-20T20:03:32+00:00	COMMIT SUCCESS
ufm:1/13	commit-success	2015-01-20T20:03:32+00:00	COMMIT SUCCESS
ufm:1/14	commit-success	2015-01-20T20:03:32+00:00	COMMIT SUCCESS
ufm:1/2	commit-success	2015-01-20T20:03:31+00:00	COMMIT SUCCESS
ufm:1/3	commit-success	2015-01-20T20:03:32+00:00	COMMIT SUCCESS
ufm:1/4	commit-success	2015-01-20T20:03:31+00:00	COMMIT SUCCESS
ufm:1/5	commit-success	2015-01-20T20:03:32+00:00	COMMIT SUCCESS
ufm:1/6	commit-success	2015-01-20T20:03:32+00:00	COMMIT SUCCESS
ufm:1/8	commit-success	2015-01-20T20:03:32+00:00	COMMIT SUCCESS
ufm:1/9	commit-success	2015-01-20T20:03:32+00:00	COMMIT SUCCESS

The commit is finished when the **Current Status** shows **commit-success**.

For example:

```
bti7800# show system upgrade
```

```
Current Status      : commit-success
```

Module	Commit Status	Commit Start Time	Notification Message
cmm:1/A	commit-success	2015-01-20T20:01:12+00:00	COMMIT SUCCESS
cmm:1/B	commit-success	2015-01-20T20:01:12+00:00	COMMIT SUCCESS
ufm:1/1	commit-success	2015-01-20T20:03:31+00:00	COMMIT SUCCESS
ufm:1/11	commit-success	2015-01-20T20:03:32+00:00	COMMIT SUCCESS
ufm:1/13	commit-success	2015-01-20T20:03:32+00:00	COMMIT SUCCESS
ufm:1/14	commit-success	2015-01-20T20:03:32+00:00	COMMIT SUCCESS
ufm:1/2	commit-success	2015-01-20T20:03:31+00:00	COMMIT SUCCESS
ufm:1/3	commit-success	2015-01-20T20:03:32+00:00	COMMIT SUCCESS
ufm:1/4	commit-success	2015-01-20T20:03:31+00:00	COMMIT SUCCESS
ufm:1/5	commit-success	2015-01-20T20:03:32+00:00	COMMIT SUCCESS
ufm:1/6	commit-success	2015-01-20T20:03:32+00:00	COMMIT SUCCESS

```

ufm:1/8  commit-success  2015-01-20T20:03:32+00:00  COMMIT SUCCESS
ufm:1/9  commit-success  2015-01-20T20:03:32+00:00  COMMIT SUCCESS

Module      Download Status      Download Start Time      Notification Message
-----
cmm:1/A     download-success     2015-01-20T19:48:30+00:00  Download successful

Module      URL Status  URL
-----
cmm:1/A     URL set
ftp://user@172.25.5.100/sw/bti7800-sys-1.6.0-14211.x86_64.rpm

Software Rollback : Rollback eligibility has not been evaluated

```



NOTE: Starting with release 4.2, the system automatically retries the system upgrade commit command if the initial commit fails.

10. Check over the system.

- a. Use the **show system version** command to verify that all modules are running the new version of software.
- b. Use the **show equipment** command to verify that all modules are up and running.
- c. Use the **show alarms** command to verify that no unexpected alarms have been raised due to the upgrade.
- d. Use the **show system firmware** command to see if the CMM firmware also needs to be upgraded.

If you see ****FIRMWARE MISMATCH**** in the CMM output, refer to [“Upgrading the CMM Firmware” on page 234](#).



NOTE: The firmware on traffic modules is automatically upgraded. When a traffic module comes up, a check is performed for a firmware mismatch. If a mismatch exists, the firmware on the traffic module is automatically upgraded.

Release History Table

Release	Description
4.3	In releases 4.3 and higher, you can upgrade the software with the provisioning privilege.
4.2	Starting with release 4.2, the system automatically retries the system upgrade commit command if the initial commit fails.

Upgrading the CMM Firmware

Use this procedure to upgrade the CMM firmware. Various hardware components on the CMM require firmware for management and control. The CMM firmware upgrade procedure is not service affecting.



NOTE: The system automatically upgrades most traffic module firmware when needed. You do not need to explicitly upgrade most firmware on the traffic modules. The exception is the re-timer firmware. See [“Upgrading the Re-timer Firmware on a UFM6” on page 238](#) for more information on the re-timer firmware.

Prerequisites:

- In releases lower than release 4.3, you must have **superuser** privileges to upgrade the firmware. In releases 4.3 and higher, you can upgrade the firmware with the **provisioning** privilege.

- Log in to the CLI using the shared management IP address.
- Use the **show system firmware** command to verify that the CMM firmware needs to be upgraded.

For example (partial output only):

```
bti7800# show system firmware
```

Module	Module Type	Device	Firmware
cmm:1/A	CMM	L2-switch	WebStaX (stackable) 2.80f_BTISYSTEMS_R2
FIRMWARE MISMATCH			
		SHMM	Shelf Manager Ver.: 3.1.1.7
Chassis Product ID: BTI 14 Slot Rev 1.1			
FIRMWARE MISMATCH			
Carrier Product ID: BTI-CMM Rev 1.2 **FIRMWARE MISMATCH**			
a2f-upgrade.dat: v1.4			
rc.shmm700-hpd1: v1.0 **FIRMWARE MISMATCH**			
shelfman.conf: v1.0			

```

cmm:1/B CMM          L2-switch  WebStaX (stackable) 2.80f_BTISYSTEMS_R2
**FIRMWARE MISMATCH**
                        SHMM       Shelf Manager Ver.: 3.1.1.7
                        Chassis Product ID: BTI 14 Slot Rev 1.1
**FIRMWARE MISMATCH**
                        Carrier Product ID: BTI-CMM Rev 1.2 **FIRMWARE
Mismatch**
                        a2f-upgrade.dat: v1.4
                        rc.shmm700-hpd1: v1.0 **FIRMWARE MISMATCH**
                        shelfman.conf: v1.0

```

If you see ****FIRMWARE MISMATCH****, then the respective firmware needs updating and you can proceed to the next step. A ****FIRMWARE MISMATCH**** designation means that the firmware version packaged with the currently running software is different from the currently running firmware version.

3. Verify that there are no unexpected alarms raised against the CMMs.

Use the **show alarms** command to view alarms on the chassis. You should see the **firmUpgrdReqd** alarm, which indicates that a firmware upgrade is required.

Resolve all unexpected CMM alarms before proceeding. You do not have to resolve non-CMM equipment alarms.



TIP: Use the **show alarms** command before and after the upgrade to determine if new alarms are raised from to the upgrade.

4. If you are running with two CMMs, verify that the CMMs are synchronized.

The CMMs are synchronized when the HA Status is In Sync.

For example (only relevant output is shown):

```

bti7800# show system
Active Controller      : cmm:1/A
Backup Controller     : cmm:1/B
HA Status              : In Sync

```

5. Upgrade the L2-switch firmware if there is a mismatch.



NOTE: The CMM might raise an **eqptComm** alarm when upgrading the L2-switch firmware. This is normal. The alarm eventually clears after the firmware is upgraded.

- a. Use the **system upgrade firmware l2-switch** command to upgrade the L2-switch firmware.

For example (partial output only, actual output might differ):

```

bti7800# system upgrade firmware l2-switch chassis:1

This action will upgrade both Master and Slave (if present) l2-switch. It
may take several minutes to complete and cannot be interrupted meanwhile.

Do you want to continue? (yes/no): yes

Upgrading l2-switches is in progress, Please wait...
Copying file....Done
Setting IP...Done
Upgrading with Redboot...Done

Preparing to upgrade with WebStaX.....
Upgrading with WebStaX.....Done

Successfully upgraded with WebStaX image!
Updating local files...

Current Version: WebStaX (stackable) 3.41f_BTISYSTEMS_R3.3
Deleting temp file.....

bti7800#

```

- b. Use the **show system firmware** command to verify that the L2-switch is running the new firmware.

For example (partial output only, actual output might differ):

```

bti7800# show system firmware

```

Module	Module Type	Device	Firmware
cmm:1/A	CMM	L2-switch	WebStaX (stackable) 3.41f_BTISYSTEMS_R3.3
cmm:1/B	CMM	L2-switch	WebStaX (stackable) 3.41f_BTISYSTEMS_R3.3

6. Upgrade the SHMM firmware if there is a mismatch.

- a. Use the **system upgrade firmware shmm** command to upgrade the SHMM firmware.

For example (partial output only, actual output might differ):

```

bti7800# system upgrade firmware shmm module chassis:1

This action will upgrade both Active and Standby (if present) ShMM.
Do you want to continue? (yes/no): yes

Verifying whether upgrade is required...Upgrade required, performing upgrade

Upgrading Chassis HPDL of Active SHMM...Done
Upgrading Shelfman Conf of Active SHMM.....Done
Upgrading Chassis HPDL of Backup SHMM...Done
Upgrading Shelfman Conf of Backup SHMM.....Done
Rebooting the SHMM for Changes to take effect...Done
Verifying upgrade...SHMM Upgrade was successful, Updating Local Files...

```

Done
bti7800#



NOTE: This command can take up to 30 minutes to complete.

- b. Use the **show system firmware** command to verify that the SHMM is running the new firmware.

For example (partial output only, actual output might differ):

bti7800# show system firmware

Module	Module Type	Device	Firmware
cmm:1/A	CMM	L2-switch	WebStaX (stackable) 3.41f_BTISYSTEMS_R3.3
		SHMM	Shelf Manager Ver.: 3.4.2.1 Chassis Product ID: BTI 14 Slot Rev 1.9 Carrier Product ID: BTI-CMM Rev 1.4 a2f-upgrade.dat: v1.4 rc.shmm700-hpdl: v1.1 shelfman.conf: v1.3 Kernel Build Date: 2/4/2015
cmm:1/B	CMM	L2-switch	WebStaX (stackable) 3.41f_BTISYSTEMS_R3.3
		SHMM	Shelf Manager Ver.: 3.4.2.1 Chassis Product ID: BTI 14 Slot Rev 1.9 Carrier Product ID: BTI-CMM Rev 1.4 a2f-upgrade.dat: v1.4 rc.shmm700-hpdl: v1.1 shelfman.conf: v1.3 Kernel Build Date: 2/4/2015

7. Check over the system.
- Use the **show system version** command to verify that all modules are running the new version of software.
 - Use the **show equipment** command to verify that all modules are up and running.
 - Use the **show alarms** command to verify that no unexpected alarms have been raised due to the upgrade.
 - Use the **show system firmware** command to verify that the CMM is running the new firmware.

Release History Table

Release	Description
4.3	In releases 4.3 and higher, you can upgrade the firmware with the provisioning privilege.

Upgrading the Re-timer Firmware on a UFM6

Use this procedure to upgrade the re-timer firmware on UFM6 modules. This procedure is supported in releases 4.3 and higher.

The UFM6 contains re-timer firmware on each of the dual-mode ports (client ports 1, 2, 6, 7). When you upgrade the software from a release compatible with one re-timer version to a release compatible with another re-timer version, the system raises a Firmware Upgrade Required (firmUpgrdReqd) alarm. To clear the alarm, you should upgrade the re-timer firmware on all UFM6 modules in the system.

Table 41 on page 238 shows the different re-timer versions available and the software releases that they are compatible with.

Table 41: UFM6 Re-timer Versions

Re-timer Version	Packaged with Software Release	Compatible with Software Release
D013	—	4.1, 4.2
D015	4.3 and higher	4.1, 4.2, 4.3, and higher

For example, if you upgrade your system from release 4.1 or 4.2 to release 4.3, you should also upgrade the re-timer firmware to version D015 on the dual-mode ports on all applicable UFM6 modules.

A dual-mode port running an older version of the re-timer firmware behaves as follows in a system running a software release that is not compatible with the older version of the re-timer firmware:

- All existing interfaces and cross-connects associated with that port continue to run normally.
- New interfaces cannot be created on that port.

You can upgrade the re-timer firmware on the UFM6 in one of two ways:

- Reseat or perform a cold reload of the UFM6. Once the UFM6 boots back up, it will automatically upgrade the re-timer firmware on all dual-mode ports to the latest version. This automatic upgrade also occurs if you insert a UFM6 that is running an older version of the re-timer firmware into the chassis. Note that you can cause a cold reload without explicitly issuing the cold reload command. For example, changing the administrative status of the UFM6 from up to down and back to up causes a cold reload of the module.

- Upgrade the re-timer firmware manually using CLI commands. The remainder of this section describes this procedure.



NOTE: Upgrading the re-timer firmware is service affecting on the port where the firmware is being upgraded.



WARNING: Once the re-timer upgrade has started on any port, you must let the upgrade proceed to completion and not issue any commands that interfere with the upgrade. Without limiting the generality of the foregoing, this includes warm and cold reloads (and removal) of the containing UFM6, system software upgrades and rollback, CMM firmware upgrades, system database restoration, CMM commissioning, and CMM replacement.

1. Determine the UFM6 modules that require re-timer firmware upgrades.

For example:

```
bti7800# show system firmware retimer
```

Module	Port Number	Device	Firmware
ufm:1/14	1	Retimer	D013 **Firmware Mismatch**
ufm:1/14	2	Retimer	D013 **Firmware Mismatch**
ufm:1/14	6	Retimer	D013 **Firmware Mismatch**
ufm:1/14	7	Retimer	D013 **Firmware Mismatch**

Ports that require an upgrade are shown with a ****Firmware Mismatch****.

2. Disable the port on which you want to upgrade the re-timer firmware.

For example:



NOTE: This is service affecting for the port.

```
bti7800# config
```

```
Entering configuration mode terminal
```

```
bti7800(config)# equipment chassis:1 module ufm:1/14 transceiver qsfp:1/14/1/2
admin-status down
```

```
bti7800(config-transceiver-qsfp:1/14/1/2)# commit
```

```
Commit complete.
```

```
bti7800(config-transceiver-qsfp:1/14/1/2)# end
```

```
bti7800#
```

If you want to upgrade the re-timer firmware on more than one port, repeat this step for the other ports.

3. Upgrade the re-timer firmware.

For example:

```
bti7800# system upgrade firmware retimer module ufm:1/14 port 2
```

If you want to upgrade the re-timer firmware on all ports on the module, use the **system upgrade firmware retimer module ufm:1/14 port all** command but be sure to disable all dual-mode ports on the UFM6 first.

4. To see which ports are being upgraded, check the outstanding conditions. A Firmware Upgrade In Progress (firmUpgrdInProg) condition is raised against the port during the upgrade. For example:

```
bti7800# show conditions | inc rtmr
rtmr:1/14/1/1                                firmUpgrdInProg
non-alarmed 2017-05-17T17:29:24-04:00      not-reported      false
      Firmware upgrade in progress
rtmr:1/14/1/2                                firmUpgrdInProg
non-alarmed 2017-05-17T17:29:24-04:00      not-reported      false
      Firmware upgrade in progress
rtmr:1/14/1/7                                firmUpgrdInProg
non-alarmed 2017-05-17T17:29:24-04:00      not-reported      false
      Firmware upgrade in progress
```



NOTE: A re-timer upgrade can take 10 minutes or more to complete.



WARNING: Once the re-timer upgrade has started on any port, you must let the upgrade proceed to completion and not issue any commands that interfere with the upgrade. Without limiting the generality of the foregoing, this includes warm and cold reloads (and removal) of the containing UFM6, system software upgrades and rollback, CMM firmware upgrades, system database restoration, CMM commissioning, and CMM replacement.

After the upgrade is complete, the firmUpgrdInProg condition is cleared on the port. If the re-timer firmware on the dual-mode ports on all UFM6 modules have been upgraded to the proper version, the firmUpgrdReqd alarm is cleared.

If the upgrade fails, a Firmware Upgrade Failed (firmUpgrdFail) alarm is raised against the port. In this situation, reissue the upgrade command.

Release History Table

Release	Description
4.3	Use this procedure to upgrade the re-timer firmware on UFM6 modules.

Enabling Automatic CMM SHMM Firmware Upgrades

Use this procedure to enable automatic SHMM firmware upgrades on a CMM.



NOTE: This feature is supported starting with release 2.1.1.

When SHMM auto-upgrade is enabled, the CMM automatically upgrades the SHMM firmware when new SHMM firmware is detected during a software upgrade.

Specifically, SHMM auto-upgrade works as follows:

- When a CMM boots up, it checks whether its SHMM firmware and whether the SHMM firmware on the other CMM match the firmware version associated with the currently active software. This occurs every time a CMM boots up, including when a CMM is being upgraded to new software.
- If there is a mismatch, the CMM raises a Firmware Upgrade Required (firmUpgrdReqd) alarm, proceeds to upgrade the SHMM firmware, and raises a Firmware Upgrade in Progress (firmUpgrdInProg) condition. The automatic upgrade starts only when all CMMs have come up and are synchronized. Note that the firmUpgrdReqd alarm applies to other firmware as well, so you should use the **show system firmware** command to check whether you need to manually upgrade other firmware.
- If more than one CMM in a single or multichassis system requires SHMM firmware upgrades, the firmware is upgraded on the CMMs sequentially.
- Once an automatic SHMM firmware upgrade is in progress, it cannot be cancelled and it should not be interrupted. CLI commands that conflict with this are rejected.

1. Enter global configuration mode.

For example:

```
bti7800# config
Entering configuration mode terminal
bti7800(config)#
```

2. Enable automatic SHMM firmware upgrades.

For example:

```
bti7800(config)# system shmm-firmware autoupgrade enabled
This commit will cause Shelf Manager firmware to be upgraded under system
control.
Are you sure ? [YES,no] yes
```

```
bt17800(config)# commit
Commit complete.
```

After you enable automatic SHMM firmware upgrades, the SHMM firmware is automatically upgraded if new SHMM firmware is detected when you next perform a software upgrade.

If you enable automatic SHMM firmware upgrades when a SHMM Firmware Upgrade Required (firmUpgrdReqd) alarm is in effect, an automatic upgrade is not performed until the CMM reloads (for example, **system reload warm cmm:1/A**).

Release History Table

Release	Description
2.1.1	Use this procedure to enable automatic SHMM firmware upgrades on a CMM.

Rolling Back a Software Upgrade

Use this procedure to roll back a software upgrade to the release from which you upgraded. This procedure covers rolling back the software upgrade on the CMMs and on all of the traffic modules. Both the software and the configuration are rolled back.



CAUTION: This procedure is service affecting.



NOTE: You can only roll back software if you have made no hardware changes and made no hardware replacements in the system. Once you make a hardware change, you cannot roll back software.

Prerequisites:

- In releases lower than release 4.3, you must have **superuser** privileges to roll back a software upgrade. In releases 4.3 and higher, you can roll back a software upgrade with the **provisioning** privilege.

1. Log in to the CLI using the shared management IP address.

2. In order to roll back the upgrade, the upgrade itself must have been successful.

Use the **show system upgrade** command to verify that the upgrade was successful.

For example (partial output only):

```
bt17800# show system upgrade
Current Status      : commit-success
Software Rollback   : Rollback eligibility has not been evaluated
```

If the **Current Status** is **commit-success**, then you can attempt to roll back the upgrade.

The **show system upgrade** output contains a message describing the **Software Rollback** status. Whether a rollback can be performed successfully or not depends on a number of internal conditions. The message **Software Rollback : Rollback eligibility has not been evaluated** means that those conditions have not been checked yet. Those conditions are only checked after you initiate the rollback command. Once you initiate the rollback command, this message will change to reflect the rollback progress or display an error message if the rollback attempt has failed.

3. Perform the software rollback.

Use the **system upgrade rollback** command to perform the rollback. For example:

```
bti7800# system upgrade rollback
```

```
CAUTION: Software rollback may affect traffic and configuration,
Would you like to proceed? [no,yes] yes bti7800#
```

In response to the rollback command, the system performs cursory sanity checks to see if the rollback request is permitted to proceed. If any of these checks fails, the system returns an error message immediately, and the command fails. If the rollback request is permitted to proceed, then the CLI prompt is returned.



NOTE: The request can still fail at a later stage. If this occurs, the reason for failure will be provided in the output of the **show system upgrade** command.

4. Check on the status of the rollback.

You can check on the status of the rollback by issuing the **show system upgrade** command periodically.

For example (partial output only):

```
bti7800# show system upgrade
```

```
Current Status      : Rollback in progress
```



NOTE: During rollback, you will lose management connectivity. Wait several minutes before connecting to the shared management IP address again. Once you log back in, continue to check on the status of the rollback.

```
bti7800# show system upgrade
```

```
Current Status      : Rollback succeeded -- previous application and
configuration restored
```

Proceed to the next step only after the rollback has succeeded.

5. Roll back the CMM firmware if needed.

If you upgraded to new CMM firmware after you upgraded to the new software, you will need to roll back the firmware to the previous version. To do this, use the same procedure as you used to upgrade the CMM firmware. See [“Upgrading the CMM Firmware” on page 234](#).

6. Roll back firmware on the traffic modules if needed.

The system automatically rolls back traffic module firmware if the firmware was upgraded. In some older releases, this rollback is not automatic, and you will need to explicitly roll back the traffic module firmware to the previous version. Use the **system upgrade firmware ipmc** command to roll back the traffic module firmware if the firmware does not roll back automatically. You will see the Firmware Upgrade Required (firmUpgrdReqd) alarm in this case.

7. Cold reboot all modules in the system.

If you are rolling back to release 2.0 or higher, the system automatically performs a cold reload of all modules as part of 3, and you can skip to the next step. Otherwise, cold reboot all modules as follows:

- If you are rolling back to a release that supports the **system reload all cold** command, then issue that command to perform a cold reload of all modules.
- If you are rolling back to a release that does not support the **system reload all cold** command, then use the **system reload cold** command on each module individually.

8. After all modules have rebooted successfully, check over the system.

- a. Use the **show system version** command to verify that all modules have rolled back to the previous version of software.
- b. Use the **show equipment** command to verify that all modules are up and running.
- c. Use the **show alarms** command to verify that no unexpected alarms have been raised due to the rollback.

Release History Table

Release	Description
4.3	In releases 4.3 and higher, you can roll back a software upgrade with the provisioning privilege.

Maintenance and Troubleshooting

- [Monitoring Environmental Sensors on page 245](#)
- [System Event Logs on page 247](#)
- [Resetting the Database to the Factory-Default Configuration on page 249](#)
- [Backing Up the Configuration Database on page 249](#)
- [Restoring the Database from a Backup Without Affecting Service on page 251](#)
- [Restoring the Database from a Backup from the CLI on page 257](#)
- [Replacing the CMM in a Single CMM System on page 259](#)
- [Installing a Software Load on a CMM Using a System Repair Drive on page 261](#)
- [Uncommissioning a CMM on page 264](#)

Monitoring Environmental Sensors

Use this procedure to display environmental measurements such as fan speed and system temperature.

The BT17800 has sensors deployed in various locations on the chassis. By periodically examining these sensor readings, you can monitor the overall health of the system.

You can display all readings or readings for a particular type of sensor.

1. To display all readings:

```
bt17800# show environment
```

2. To display readings for a specific type of sensor:

- a. To show the readings for the temperature sensors on all modules:

For example (output truncated for clarity):

```
bt17800# show environment temperature
```

```
Temperatures Chassis:1
```

Module	Sensor	Measurement
amp:1/4	DS75 Temp 1	33 deg C
amp:1/4	DS75 Temp 3	48 deg C

```

amp:1/4    LM84BIQA Temp      33 deg C
amp:1/4    Line card Temp     49 deg C
bic:1/1/1  BIC Temp          63 deg C
bic:1/1/1  DS75 Temp BIC A    40 deg C
bic:1/1/2  BIC Temp          50 deg C
bic:1/1/2  DS75 Temp BIC B    34 deg C

```

- b. To show the readings for the fan speed sensors on the cooling units:

For example:

```
bti7800# show environment fanspeed
```

```
Fan Speed Chassis:1
```

Module	Sensor	Measurement
fan:1/1	Fan RPM	5080 rpm(97%)
fan:1/2	Fan RPM	5160 rpm(99%)
fan:1/3	Fan RPM	5200 rpm(100%)
fan:1/4	Fan RPM	5160 rpm(99%)



NOTE: The RPM measurement shown for either a BTI7814 Booster Fan (BT8A78FAN9) or a 2-Slot Chassis Cooling Module (BT8A78FAN2) is an average of the RPM values of the individual fans in the cooling module.

- c. To show the readings for the power sensors on the PEMs:

For example:

```
bti7800# show environment power
```

```
Power Chassis:1
```

Module	Sensor	Measurement
pem:1/1	PEM AC A1 Power	Power Present
pem:1/2	PEM AC A2 Power	Power Present
pem:1/3	PEM AC B1 Power	Power Present
pem:1/4	PEM AC B2 Power	Power Present

- d. To show the readings for the voltage sensors on all modules:

For example (output truncated for clarity):

```
bti7800# show environment voltage
```

```
Voltages Chassis:1
```

Module	Sensor	Measurement
pem:1/1	PEM AC A1, Vin	236.000 Volts
pem:1/1	PEM AC A1, Vout	53.000 Volts
pem:1/2	PEM AC A2, Vin	234.000 Volts
pem:1/2	PEM AC A2, Vout	53.000 Volts

```

pem:1/3    PEM AC B1, Vin    235.000 Volts
pem:1/3    PEM AC B1, Vout   53.000 Volts
pem:1/4    PEM AC B2, Vin    236.000 Volts
pem:1/4    PEM AC B2, Vout   53.000 Volts
ufm:1/2    12V_MAIN          11.820 Volts
ufm:1/2    2V5_CORE          2.439 Volts
ufm:1/2    2V5_IO            2.439 Volts
ufm:1/2    3V3_MAIN          3.281 Volts
ufm:1/2    3V3_STBY          3.241 Volts
ufm:1/2    5V_MAIN           4.920 Volts
ufm:1/2    ADC_1V2_GIGE      1.275 Volts

```

- e. To show the readings for the current sensors on the BTI7814 AC PEMs:

For example:

```
bti7800# show environment current
```

```
Current Chassis:1
```

Module	Sensor	Measurement
pem:1/1	PEM AC A1, Iout	0.000 Amps
pem:1/2	PEM AC A2, Iout	10.400 Amps
pem:1/3	PEM AC B1, Iout	10.100 Amps
pem:1/4	PEM AC B2, Iout	0.000 Amps

System Event Logs

An event is a problem, a configuration change, or some other noteworthy incident that occurs on the system. Events generate system log messages. BTI7800 system logs provide the following information:

Table 42: System Log Information

Message Type	Log Description	Information Displayed
Audit	Messages associated with user login and logout events.	Username User group Time Interface used to access (if available) Login/Logout
Configuration	Messages associated with system configuration, including modifications and deletions.	Username Time Creating/Modification/Deletion Committed configuration changes.

Table 42: System Log Information (continued)

Message Type	Log Description	Information Displayed
Command action	Messages associated with system commands.	Username Time Command Command success/failure
Operational state change logs	Messages associated with changes to the following: 1. Interface Operational State 2. Alarms/Conditions Raised/Cleared 3. Equipment Operational State	Time Interface/Equipment/Entity Name State/Alarm/Condition

You can generate and collect system log files using the CLI. The following table lists the logging commands.

Table 43: CLI Logging Commands

Command Mode	Command	Description
Operational	logging archives	Provides copy, remove and show functions for system logs.
Configuration	logging customer-log facility-id	Sets the facility identifier in customer log files.
	logging logrotate	Manages the system log files. This command provides the following functions: <ul style="list-style-type: none"> • Sets the period that a log file is kept. • Specifies the remote server to which to move the log file when the log file is rotated out of local storage. • Sets the number of log files to keep in local storage. • Sets the size of the log files.
	logging module	Specifies the software module for which you want to collect event data.
	logging protocol	Specifies the protocol for which you want to collect event data.
	logging remote-server	Specifies remote syslog servers that receive a copy of the system log files. You can configure up to four servers.

For detailed CLI command information, refer to the *BT17800 Series Command Line Reference Guide*.

Resetting the Database to the Factory-Default Configuration

Use this procedure to reset the database to the factory-default configuration from the CLI.



NOTE: This procedure removes all existing provisioning settings and is service affecting.

1. Back up the existing configuration. This is optional.
 - a. Save the configuration database to a remote location.
See “Backing Up the Configuration Database” on page 249.
 - b. Save the running configuration to a remote location.

For example:

```
bti7800# show running-config | nomore | save
10.1.220.104_running_config_20150706
Value for 'password' (<string>): *****
bti7800# copy file 10.1.220.104_running_config_20150706 remote-url
ftp://user@10.64.7.51/10.1.220.104_running_config_20150706
Value for 'password' (<string>):
```

2. Reset the database.

For example:

```
bti7800# system database restore factory-default
This is a service-affecting action that will overwrite the configuration
database with default values and perform an automatic reload all cold.
Do you wish to continue? [no,yes] yes
```

The CLI session closes and both CMMs and all service modules cold reload into the factory-default configuration. This might take several minutes. All existing service module configuration is erased and traffic is affected. The CMM remains commissioned and commissioning data is retained.

Backing Up the Configuration Database

Use this procedure to back up the configuration database to a remote location or to local chassis storage.



NOTE: On the BTI7801, the CMM automatically backs up its configuration database to local chassis storage every 60 minutes. This occurs even if you do not explicitly make changes to the database.

1. Back up the configuration database.

- a. To back up the database to a remote location:

For example:

```
bti7800# system database backup remote-url sftp://user@10.64.7.51
Value for 'password' (<string>): *****
```

- b. To back up the database to local chassis storage:

```
bti7800# system database backup local
```

This command might take 15 minutes or more to complete.



NOTE: This option is available only for the BTI7801.

2. Verify that the database has been backed up.

For example:

```
bti7800# show system database

Backup Status
-----
CurrentStatus   : ready-to-backup
RemoteUrl       :
sftp://user@10.64.7.51/10.1.220.104_BTI7800v1.6.0_18346_20150706_185955.tar.gz

NotificationMsg : Backup successful
```

Look for the **Backup successful** message in the output.



NOTE: This backed-up configuration can only be restored on a compatible CMM and chassis:

- A configuration database is specific to a software version. In order to restore a backed-up database onto a replacement CMM, you must ensure that the replacement CMM is running the same software version as the software version running when the backup was created.
- In releases lower than 4.2, a configuration database is also specific to a chassis. You can only restore a backed-up database to a replacement CMM on a chassis if the database was backed up from that chassis. You cannot restore a database to a CMM on a chassis if the database was backed up from another chassis.

Starting with release 4.2, this restriction is relaxed. You can restore a backed-up database to any chassis of the same chassis type (BTI7801 to BTI7801, BTI7802 to BTI7802, BTI7814 to BTI7814).

Release History Table

Release	Description
4.2	Starting with release 4.2, this restriction is relaxed. You can restore a backed-up database to any chassis of the same chassis type (BT17801 to BT17801, BT17802 to BT17802, BT17814 to BT17814).

Restoring the Database from a Backup Without Affecting Service

Use this procedure to restore the database on an uncommissioned CMM without affecting service. This procedure first commissions the CMM and then restores the database.

It is primarily used for in-service replacement of a CMM in a chassis that has no active CMMs, such as in a system where the sole CMM in a single CMM chassis or both CMMs in a dual CMM chassis have failed.

This procedure does not affect service as long as the database being restored matches the existing service provisioning on the chassis.



WARNING: Service modules are automatically warm reloaded as part of this procedure. Software-based features on the service module (such as PM collection, APSD, APR, FPSD) are disabled while a service module warm reloads.



NOTE: The backed-up configuration must be compatible with the software and chassis:

- A configuration database is specific to a software version. In order to restore a backed-up database onto a replacement CMM, you must ensure that the replacement CMM is running the same software version as the software version running when the backup was created.
- In releases lower than 4.2, a configuration database is also specific to a chassis. You can only restore a backed-up database to a replacement CMM on a chassis if the database was backed up from that chassis. You cannot restore a database to a CMM on a chassis if the database was backed up from another chassis.

Starting with release 4.2, this restriction is relaxed. You can restore a backed-up database to any chassis of the same chassis type (BT17801 to BT17801, BT17802 to BT17802, BT17814 to BT17814).

Prerequisites

- If you are replacing a CMM in a chassis, see [“Replacing the CMM in a Single CMM System” on page 259](#) before starting this procedure.

- The configuration database that you want to restore is compatible with the chassis and with the software version on the CMM.
 - The replacement CMM is uncommissioned for this chassis.
1. Seat the CMM into slot A. If your system has two CMMs, leave the other CMM unseated.
 2. Log in locally to the CMM in slot A over the craft serial or craft Ethernet port.
For information on how to do this, see [“Logging In to the CMM Craft Ethernet or Craft Serial Ports” on page 45.](#)

3. Enter setup mode. This is known as the commissioning shell.

```
localhost console
localhost login: admin
Password:

Shell Help: List of the commands you can use:
setup - Commission the CMM
cli    - Open CLI interface to the system
reboot - Reboot the CMM
exit   - Logout

scml:~$ setup

Welcome to the BTI 7800 Series - CMM Commissioning Application!
Note: This process commissions one CMM at a time.
Type 'help' or '?' for the list of the commands. Press '<Ctrl> + C' at
any time to exit.
(cmm-setup)$
```

4. To see the list of available commands, type **help**.



NOTE: The commands in the commissioning shell should only be used on an uncommissioned system. Do not use the commissioning shell commands as a substitute for regular CLI commands.

5. Set the time zone.

For example:

```
(cmm-setup)$ settz

Please identify a location so that time zone rules can be set
correctly.
Please select a continent or ocean.
1) Africa
2) Americas
3) Antarctica
4) Arctic Ocean
5) Asia
6) Atlantic Ocean
```

- 7) Australia
- 8) Europe
- 9) Indian Ocean
- 10) Pacific Ocean
- 11) none - I want to specify the time zone using the Posix TZ format.
#?

Follow the series of menu-driven options to set the time zone.



NOTE: You must manually set the correct time zone, date, and time even if you use NTP servers. The BTI7800 requires a correct clock at all times, including the period prior to the establishment of NTP server connectivity. Use of NTP servers is recommended.

6. Set the date.

For example:

```
(cmm-setup)$ setdate
Set the system date and confirm setting.

The current date is 2015-01-01.
Enter the new date (in the format YYYY-MM-DD): 2015-06-12
System Date will be set to 2015-06-12
Confirm (yes/no/abort): yes

System Date is set to 2015-06-12
```

7. Set the time.

For example:

```
(cmm-setup)$ settime
Set the system time and confirm setting.

The current time is 00:02:48, Timezone is America/New_York.
Enter the new time (in 24-hour format-- HH:MM:SS): 12:13:00
System time will be set to 12:13:00
Confirm (yes/no/abort): yes

System time is set to 12:13:00
```

8. Set up the networking parameters.



NOTE: All parameters are required to be set for proper operation of the BTI7800.

For example:

```
(cmm-setup)$ commission
```

Set the parameters required for initial, basic CMM setup and system management, and confirm the settings.

Controller Id: 1

Note: The System Management (Shared), Individual CMM, and Default Gateway IP Addresses must be in the same network.

Enter System Management (Shared) Address (a.b.c.d): 10.10.1.22

Enter Management Netmask (/N or a.b.c.d): 255.255.255.0

Enter Default Gateway Address (a.b.c.d): 10.10.1.1

Enter NTP Server address (a.b.c.d): 192.168.35.251

Enter DNS Server address (a.b.c.d): 10.10.1.1

You have entered following values:

Controller ID	: 1
System Management (Shared) Address	: 10.10.1.22
Management Netmask	: 255.255.255.0
Default Gateway Address	: 10.10.1.1
NTP servers	: 192.168.35.251
DNS servers	: 10.10.1.1

Confirm (yes/no/abort): yes

Do you wish to reset the database to factory defaults? This will impact traffic.
Confirm (yes/no):

9. Since you are restoring the database instead of setting it to factory defaults, type no.

For example:

Do you wish to reset the database to factory defaults? This will impact traffic.
Confirm (yes/no): no

No database restore to factory defaults will be performed. It is highly recommended that you perform a `restorelocaldb` or `restoreremotedb` operation immediately.

The following values are set:

Controller ID	: 1
System Management (Shared) Address	: 10.10.1.22
Management Netmask	: 255.255.255.0
Default Gateway Address	: 10.10.1.1
NTP servers	: 192.168.35.251
DNS servers	: 10.10.1.1


If you are going to restore a database as part of commissioning, do that next - otherwise, reboot for IP settings to take effect.

10. Restore the database.

- a. To restore the database from a backed-up configuration file stored at a remote location:

For example:

This command finishes by performing an automatic warm reload of the CMM and all modules. The commissioning shell displays a set of log messages as the CMM reboots.

-  **NOTE:** This option is available only for the BTI7801.

```
Size: 303602  
Status: 'valid'  
yyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyy  
yyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyy  
yyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyy  
yyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyy  
yyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyyy
```

Do you want to restore the database from the local chassis? (yes/no)
Warning: This command will perform an automatic warm restart of the system.

yes

This command might take 15 minutes or more, and finishes by performing an automatic warm reload of the CMM and all modules.

11. You will be logged out as the CMM reboots. When you see the login prompt, log back in to the craft serial or craft Ethernet port and start the commissioning shell.

```
localhost console
localhost login: admin
Password:

Shell Help: List of the commands you can use:
setup - Commission the CMM
cli - Open CLI interface to the system
reboot - Reboot the CMM
exit - Logout

scm1:~$ setup

Welcome to the BTI 7800 Series - CMM Commissioning Application!
Note: This process commissions one CMM at a time.
Type 'help' or '?' for the list of the commands. Press '<Ctrl> + C' at
any time to exit.
(cmm-setup)$
```

12. Reboot the CMM. This last reboot is required to ensure the CMMs and all service modules are synchronized.

```
(cmm-setup)$ reboot
```

Do you want this CMM to reboot? (yes/no) : yes

Broadcast message from root@scm1 (pts/0) (Fri Jun 12 12:41:37 2015):

The system is going down for reboot NOW!

The CMM in slot A reboots into the specified configuration and assumes the role of the active system controller module (SCM). Service modules are also rebooted. This might take several minutes. Proceed to the next step after the CMM finishes rebooting.

- 13. If you have a dual CMM system, seat the other CMM into slot B. The CMM in slot B will now synchronize with the CMM in slot A. This might take several minutes. When this is finished, the Active LED on the CMM in slot B turns green.
- 14. Log in to the CLI using the shared management IP address and verify that the CMMs are synchronized if applicable. For information on how to log in to the CLI, see [“Logging In to the CLI” on page 44](#).

The examples below have been edited to show only the relevant output.

In a dual CMM system, the CMMs are synchronized when the HA Status is In Sync:

```
bti7800# show system

Active Controller      : cmm:1/A
Backup Controller     : cmm:1/B
HA Status             : In Sync
```

In a single CMM system, only the active controller is listed:

```
bti7800# show system

Active Controller      : cmm:1/A
HA Status             : Not Ready
```

The chassis is now commissioned and the database restored.

Release History Table

Release	Description
4.2	Starting with release 4.2, this restriction is relaxed. You can restore a backed-up database to any chassis of the same chassis type (BTI7801 to BTI7801, BTI7802 to BTI7802, BTI7814 to BTI7814).

Restoring the Database from a Backup from the CLI

Use this procedure to restore the database from a previously backed-up configuration file from the CLI.

This procedure is primarily used when restoring a database on a chassis that is not in service.



NOTE: This procedure removes the existing configuration and is service affecting.



NOTE: If you are restoring the database from a previously backed-up configuration file, the backed-up configuration must be compatible with the software and chassis:

- A configuration database is specific to a software version. In order to restore a backed-up database onto a replacement CMM, you must ensure that the replacement CMM is running the same software version as the software version running when the backup was created.
- In releases lower than 4.2, a configuration database is also specific to a chassis. You can only restore a backed-up database to a replacement CMM on a chassis if the database was backed up from that chassis. You cannot restore a database to a CMM on a chassis if the database was backed up from another chassis.

Starting with release 4.2, this restriction is relaxed. You can restore a backed-up database to any chassis of the same chassis type (BTI7801 to BTI7801, BTI7802 to BTI7802, BTI7814 to BTI7814).

1. Back up the existing configuration. This is optional.

- a. Save the configuration database to a remote location.

See [“Backing Up the Configuration Database” on page 249](#).

- b. Save the running configuration to a remote location.

For example:

```
bti7800# show running-config | nomore | save
10.1.220.104_running_config_20150706
Value for 'password' (<string>): *****
bti7800# copy file 10.1.220.104_running_config_20150706 remote-url
ftp://user@10.64.7.51/10.1.220.104_running_config_20150706
Value for 'password' (<string>):
```

2. Restore the database.

- a. To restore the CMM from a backed-up configuration file stored at a remote location:

For example:

```
bti7800# system database restore remote
sftp://user@10.1.1.1/10.75.0.5-BTI7800v2.1.0_23151_20160309_205021.tar.gz
Value for 'password' (<string>):
This is a service-affecting action that will overwrite the configuration
database and perform an automatic reload all cold.
Do you wish to continue? [no,yes] yes
```

- b. To restore the CMM from a backed-up configuration file stored in local chassis storage:



NOTE: This option is available only for the BTI7801.

```
bti7800# system database restore local
```

This is a service-affecting action that will overwrite the configuration database and perform an automatic reload all cold.
Do you wish to continue? [no,yes] yes

This command might take 15 minutes or more to complete.

The CLI session closes and the CMM and all modules cold reload into the specified configuration. This might take several minutes. All existing service module configuration is replaced and traffic is affected. The CMM remains commissioned.

To log back in to the CLI, use the shared management IP address configured in the backup.

Release History Table

Release	Description
4.2	Starting with release 4.2, this restriction is relaxed. You can restore a backed-up database to any chassis of the same chassis type (BTI7801 to BTI7801, BTI7802 to BTI7802, BTI7814 to BTI7814).

Replacing the CMM in a Single CMM System

Use this procedure to replace the CMM in a single CMM system.



WARNING: Service modules are automatically warm reloaded as part of this procedure. Software-based features on the service module (such as PM collection, APSD, APR, FPSD) are disabled while a service module warm reloads.

Prerequisites

- Familiarize yourself with the concepts described in [“CMM Replacement” on page 41](#).
 - Familiarize yourself with the CMM replacement procedures in the *BTI7800 Series Hardware Overview and Installation Guide*.
 - The replacement CMM is uncommissioned for this chassis.
1. If the CMM that you want to replace is currently up and running, back up the current configuration database.

See [“Backing Up the Configuration Database” on page 249](#) for instructions on how to do this.
 2. Remove the CMM from the chassis.

3. Insert the replacement CMM.
4. Check to see what software load is contained in the replacement CMM.

To see what software release the replacement CMM contains, log in to the craft port and use the **show** command in the commissioning shell. For example:

```
Last login: Fri Mar 18 13:15:56 2016 from server.example.com

Shell Help:
List of the commands you can use:
setup - Commission the CMM
cli    - Open CLI interface to the system
reboot - Reboot the CMM
exit   - Logout

scm1:~$ setup

Welcome to the BTI 7800 Series - CMM Commissioning Application!
Note: This process commissions one CMM at a time. Type 'help' or '?' for the
list of the commands. Press '<Ctrl> + C' at any time to exit.

(cmm-setup)$ show
Controller ID           : 1
Management Shared IP Address : 10.1.220.104
Management Netmask      : 255.192.0.0
Individual CMM IP       : None
Default Gateway Address  : 10.1.1.1
NTP Server Address       : 172.25.0.61
DNS Server Address       : 172.25.0.61
Current Time             : 11:20:45
Current Date             : 2016-04-06
Time Zone                : America/Toronto
OS Version               : 2.0.0 21522
Application Version      : 2.1.0 23298
```

The above example output shows that the CMM is running Application Version release 2.1.0.

If you want the CMM to run a different software load, use the procedure described in [“Installing a Software Load on a CMM Using a System Repair Drive”](#) on page 261 to install the software load that you want to run.



NOTE: A configuration database is specific to a software version. When you restore a backed-up database onto a replacement CMM, that CMM must run the same software version as the software version running on the original CMM when the backup was created. You cannot restore a configuration database from a CMM running one software version to a CMM running a different software version.

5. Configure the replacement CMM to boot up with the configuration database saved in step 1 (or otherwise saved previously).

See [“Restoring the Database from a Backup Without Affecting Service”](#) on page 251 for instructions on how to do this.



NOTE: If you do not have a backed-up configuration database, then you will need to restore the replacement CMM back to factory defaults. You will need to reconfigure the system. Service will be affected.

Installing a Software Load on a CMM Using a System Repair Drive

Use this procedure to install a software load on a CMM using a system repair drive. This is typically performed at initial system turn-up, during CMM replacement, or when network-based methods cannot be used.

Each CMM has a USB port from which it can boot. The USB port has the highest priority in the boot sequence. If a bootable device is attached to the USB port, then the CMM will try to boot from that device first.



CAUTION: This procedure erases all software, configuration, and commissioning data from the CMM.



WARNING: Service modules are automatically warm reloaded as part of this procedure. Software-based features on the service module (such as PM collection, APSD, APR, FPSD) are disabled while a service module warm reloads.

Prerequisites:

- Obtain or create a system repair drive with the desired software image. For information on how to do this, see [“Creating a BTI7800 System Repair Drive”](#) on page 269.

1. Ensure the CMM on which you want to perform this installation is unseated from the chassis and that the chassis does not have an active CMM running.

If the chassis has an active CMM, the active CMM might automatically install its software load onto this CMM at the end of this procedure.

2. Plug in the system repair drive to the USB port of the CMM.
3. Reseat the CMM.

The CMM automatically boots to the installation utility on the system repair drive.

4. Connect locally to the craft port of the resealed CMM.

For information on how to do this, see [“Logging In to the CMM Craft Ethernet or Craft Serial Ports” on page 45.](#)

5. At the prompt, log in using the username **admin** and password **admin**.

These credentials are hardcoded when booting from the system repair drive.

```
localhost console

localhost login: admin
Password:
Welcome to the Bti OS & Application Installation shell.  Type help or ? to
list commands.

(bti7800-installer) ?

Main Command List
-----
install_system reboot show_current_install show_debug_logs show_sw_version

Miscellaneous
-----
help
```

6. To see the software version that is to be loaded, use the **show_sw_version** command.
7. To see the software version that is currently loaded on the CMM, use the **show_current_install** command.
8. Install the software.

Use the command **install_system** to start the installation.

You are prompted to verify if you want to proceed with the software installation. Choose **yes** to continue. For example:

```
(bti7800-installer) install_system

WARNING: This will erase all data on this CMM.
Are you sure you want to continue? [yes / no] yes
Proceeding with System installation
>> Verifying system image
Confirm installation of version 1.5.3-17482
Are you sure you want to continue? [yes / no] yes

>> Extracting files
>> Checking install target
>> Installing OS >> Partitioning media
.....
>> Installing system OS on media
.....

>> Running post OS installation tasks .....
>> Installing Application
.....
```

```

** System install finished successfully - remove the USB key & reboot
**
(bti7800-installer)

```

The installation process re-partitions and reformats the local drives and file systems, installs the base operating system, and installs the BTI7800 software. This step might take several minutes to complete.

9. Remove the system repair drive when prompted and reboot the CMM.

At the prompt type **reboot**.

Here is a sample output. Actual output might differ.

```

(bti7800-installer) reboot
System is going down for a reboot

.....
.....
.....

Starting rpcbind daemon...done.
net.ipv4.conf.default.rp_filter = 0
net.ipv4.conf.all.rp_filter = 0
Running postinst /etc/rpm-postinsts/100...
adding crontab
Running postinst /etc/rpm-postinsts/101...
update-alternatives: Linking //usr/sbin/sendmail to sendmail.postfix
Adding system startup for /etc/init.d/postfix.
Starting atd: OK
INIT: Entering runlevel: 3
Starting system message bus: dbus.
Starting OpenBSD Secure Shell server: sshd
generating ssh RSA key...
generating ssh ECDSA key...
generating ssh DSA key...
done.
Starting Advanced Configuration and Power Interface daemon: acpid.
acpid: starting up

acpid: 1 rule loaded

acpid: waiting for events: event logging is off

Starting domain name service: namedwrote key file "/etc/bind/rndc.key"
.
starting DNS forwarder and DHCP server: dnsmasq...
dnsmasq: failed to bind listening socket for 10.127.31.239: Address already
in use
Starting irqbalance: done
creating NFS state directory: done
Installing knfsd (copyright (C) 1996 okir@monad.swb.de).
starting 8 nfsd kernel threads: done
starting mountd: done
starting statd: done
Starting ntpd: done
Starting network management services:netlink: 12 bytes leftover after parsing

```

```

attributes.
snmpd[1706]: Created directory: /var/lib/net-snmp

snmpd[1706]: Created directory: /var/lib/net-snmp/cert_indexes

snmpd[1706]: Created directory: /var/lib/net-snmp/mib_indexes

snmpd.
snmpd[1708]: NET-SNMP version 5.7.2

Starting system log daemon...0
Starting Postfix...postfix/postfix-script: starting the Postfix mail system
Successful
starting : fruinfo... done.
Starting crond: OK
Starting tcf-agent: OK
Stopping Bootlog daemon: bootlogd.

localhost console
localhost login: admin
Password: localhost:~$
Welcome to the BTI 7800 Series - CMM Commissioning Application

```

The CMM is now running with the software load from the system repair drive. It is ready for commissioning or restoration from a backup configuration. The CLI is not available until commissioning or restoration is performed.

Uncommissioning a CMM

Use this procedure to uncommission a CMM. It is recommended that you uncommission a CMM before removing it from a chassis and placing it into storage (for example, as a spare). Uncommissioning resets the configuration database to the factory default configuration and removes all commissioning settings. It ensures that the CMM behaves predictably when you later insert it into a chassis.



WARNING: Service modules are automatically warm reloaded as part of this procedure. Software-based features on the service module (such as PM collection, APSD, APR, FPSD) are disabled while a service module warm reloads.



NOTE: This procedure removes all existing provisioning and commissioning settings.

1. Uncommissioning is performed on one CMM at a time.

In a dual CMM chassis, seat the CMM you want to uncommission and unseat the other CMM. If you want to uncommission both CMMs, work on the active CMM first and unseat the standby CMM.

In a single CMM chassis, seat the CMM you want to uncommission.

In a satellite chassis in a multichassis system, leave both MRMs seated.

2. Log in to the CMM locally over the craft serial or craft Ethernet port.

For information on how to do this, see [“Logging In to the CMM Craft Ethernet or Craft Serial Ports” on page 45](#).

3. Enter setup mode.

```
localhost console
localhost login: admin
Password:

Shell Help:
List of the commands you can use:
setup - Commission the CMM cli      - Open CLI interface to the system
reboot - Reboot the CMM
exit   - Logout

scm1:~$ setup

Welcome to the BTI 7800 Series - CMM Commissioning Application!
Note: This process commissions one CMM at a time.
Type 'help' or '?' for the list of the commands. Press '<Ctrl> + C' at any
time to exit.
(cmm-setup)$
```

4. Reset the database to the factory-default configuration and remove all commissioning settings.

For example:

```
(cmm-setup)$ factorydefaults
Do you want to set factory default setting? (yes/no) : yes
```

After a short time, the following message is shown:

```
Please reboot CMM for changes to take effect.
(cmm-setup)$
```

5. Reboot the CMM.

```
(cmm-setup)$ reboot
```

```
Do you want this CMM to reboot? (yes/no) : yes  
Broadcast message from root@scm1 (pts/0) (Fri Jun 12 12:41:37 2015):  
The system is going down for reboot NOW!
```

The CMM reboots into a uncommissioned state with the factory-default configuration. When the CMM finishes rebooting, you will see the login prompt. This might take several minutes.

In a dual CMM chassis, if you want to uncommission the second CMM, unseat the newly uncommissioned CMM, reseal the second CMM, and repeat this procedure.

The CMM is now ready for commissioning.

Appendix

- Retrieving a BTI7800 Software Image on page 267
- Creating a BTI7800 System Repair Drive on page 269
- BTI7800 Port Usage on page 277
- DWDM 50-GHz Wavelength Plan on page 278
- Interoperability with BTI7000 Series Network Elements on page 283

Retrieving a BTI7800 Software Image

Use this procedure to retrieve a BTI7800 software image from the Juniper Networks software download page. BTI7800 software is available as an RPM file or as a gzipped USB image.

- Download the RPM file if you are upgrading software using CLI commands.
- Download the gzipped USB image if you are upgrading software using a system repair drive. A system repair drive installs software onto a CMM from the USB port.

Prerequisites

- A computer running Linux, Mac OS X, or Windows
 - Internet access capable of transferring large files
 - A user login account on www.juniper.net
 - If using Windows, a file archiver program (to gunzip the USB image)
1. Use your browser to go to <https://www.juniper.net/support/downloads>.
 2. From the By Series drop-down list, select **BTI7800 Series** and then select the desired chassis type from the BTI7800 family.

The browser displays the download page for the selected chassis type.



NOTE: The same software image is used for all BTI7800 chassis types.

3. Click the **Software** tab.

4. Select the desired software release from the Version drop-down list.
5. Click the RPM file or gzipped USB image that you want to download.
6. If you are not already logged in, the browser displays a login screen.
 - a. Enter your **User ID** and **Password**.
 - b. Read through the EULA, select **I Agree**, and click **Proceed** if you agree with the terms of the EULA.
7. The download begins automatically. If your operating system prompts you to save or open the file, choose the **Save File** option or equivalent.

Depending on the speed of your Internet connection, the download might take 30 minutes or longer.

The RPM filename is in the format **bti7800-sys-sw_version.x86_64.rpm**.

The USB image is a GZIP compressed file. The filename is in the format **bti7800-usb-sw_version.gz**.

8. On your browser, go back to the download page and click on **MD5 SHA1** to view the checksum of the corresponding download. Note that the checksums are different between the RPM file and the gzipped USB image.

Both the MD5 and SHA1 checksums appear in a pop-up window.

9. Verify the checksum of the downloaded image with the expected checksum. The examples below verify the MD5 checksum for a gzipped USB image download.
 - a. On a Linux command line, for example:

```
$ ls
bti7800-usb-4.1.0-25947.gz
$ md5sum bti7800-usb-4.1.0-25947.gz
file-checksum bti7800-usb-4.1.0-25947.gz
```

- b. In a Mac OS X terminal window, for example:

```
$ ls
bti7800-usb-4.1.0-25947.gz
$ md5 bti7800-usb-4.1.0-25947.gz
file-checksum bti7800-usb-4.1.0-25947.gz
```

- c. On a Windows command line, for example:

```
C:\Users\Public\Downloads>dir bti7800*
Volume in drive C is Windows
Volume Serial Number is D095-F11F

Directory of C:\Users\Public\Downloads
```

```

05/29/2017 12:30 PM      805,967,922 bti7800-usb-4.1.0-25947.gz
                1 File(s)      805,967,922 bytes
                0 Dir(s)  120,532,914,176 bytes free

C:\Users\Public\Downloads>certutil -hashfile bti7800-usb-4.1.0-25947.gz MD5
MD5 hash of file bti7800-usb-4.1.0-25947.gz:
file-checksum
CertUtil: -hashfile command completed successfully.

```

Compare the *file-checksum* from the output of the command with the checksum displayed in step 8. If the checksums do not match, download the image again and re-verify the checksum.

10. Copy the downloaded file to the desired location.

- Copy the RPM file to the FTP server that you use to distribute software loads to your network elements.
- Copy the gzipped USB image to a location that is accessible from the computer that you are using to create the system repair drive.

If you are downloading an RPM file, you have completed this procedure.

If you are downloading a gzipped USB image, proceed to the next step.

11. Uncompress the gzipped USB image.

a. On a Linux command line, for example:

```

$ gunzip bti7800-usb-4.1.0.gz
$ ls
bti7800-usb-4.1.0

```

- b. On Mac OS X, double-click the gzipped file to uncompress and save the extracted image.
- c. On Windows, download and use a file archiver utility (for example, 7zip) to uncompress and save the extracted image.

The USB image has been downloaded and extracted successfully. You can now proceed to create the system repair drive.

Creating a BTI7800 System Repair Drive

BTI7800 software is released as an RPM as well as a USB image. The RPM is used for regular software installation while the USB image is used to create a system repair drive.

A system repair drive is a USB drive that can be used to boot up and install software on a BTI7800 CMM. The system repair drive contains the USB image of the software release you want to install along with some basic utilities.

- [Using Linux to Create a BTI7800 System Repair Drive on page 270](#)
- [Using Mac OS X to Create a BTI7800 System Repair Drive on page 272](#)
- [Using Windows to Create a BTI7800 System Repair Drive on page 275](#)

Using Linux to Create a BTI7800 System Repair Drive

Use this procedure on Linux to create a system repair drive that can be used to boot a BTI7800 CMM from the USB port.

Prerequisites

- A Linux PC with a USB 3.0 port and root/sudo access.
- A USB 3.0 flash drive (minimum 8GB).
- The BTI7800 USB image (can be downloaded from <https://www.juniper.net/support/downloads>). The software is provided as a gzipped file. You must gunzip the downloaded file before starting this procedure. See [“Retrieving a BTI7800 Software Image” on page 267](#) for more information.

1. Determine the assigned names of the existing drives on the Linux PC.

For example:

```
$ ls -l /dev/disk/by-id/
total 0
drwxr-xr-x 2 root root 320 Jul 10 08:51 ./
drwxr-xr-x 5 root root 100 Jul 9 09:37 ../
lrwxrwxrwx 1 root root 9 Jun 16 08:02 ata-GCR-8483B -> ../../sr1
lrwxrwxrwx 1 root root 9 Jun 16 08:02 ata-LG_CD-RW_CED-8120B -> ../../sr0
lrwxrwxrwx 1 root root 9 Jun 16 08:02 ata-Maxtor_6E040L0_E1MWCDE -> ../../sda
lrwxrwxrwx 1 root root 10 Jun 16 08:02 ata-Maxtor_6E040L0_E1MWCDE-part1 ->
../../sda1
lrwxrwxrwx 1 root root 10 Jun 16 08:02 ata-Maxtor_6E040L0_E1MWCDE-part2 ->
../../sda2
lrwxrwxrwx 1 root root 10 Jun 16 08:02 ata-Maxtor_6E040L0_E1MWCDE-part5 ->
../../sda5
lrwxrwxrwx 1 root root 9 Jun 16 08:02 scsi-SATA_Maxtor_6E040L0_E1MWCDE ->
../../sda
lrwxrwxrwx 1 root root 10 Jun 16 08:02 scsi-SATA_Maxtor_6E040L0_E1MWCDE-part1
-> ../../sda1
lrwxrwxrwx 1 root root 10 Jun 16 08:02 scsi-SATA_Maxtor_6E040L0_E1MWCDE-part2
-> ../../sda2
lrwxrwxrwx 1 root root 10 Jun 16 08:02 scsi-SATA_Maxtor_6E040L0_E1MWCDE-part5
-> ../../sda5
lrwxrwxrwx 1 root root 9 Jul 9 09:27
usb-Verbatim_STORE_N_GO_070233A4889E0848-0:0 -> ../../sdb
lrwxrwxrwx 1 root root 10 Jul 9 09:28
usb-Verbatim_STORE_N_GO_070233A4889E0848-0:0-part1 -> ../../sdb1
```

2. Attach the USB drive to your Linux PC.
3. Determine the name that Linux has assigned to the newly attached USB drive by re-issuing the same command.

For example:

```
$ ls -l /dev/disk/by-id/
total 0
drwxr-xr-x 2 root root 320 Jul 10 08:51 ./
drwxr-xr-x 5 root root 100 Jul 9 09:37 ../
lrwxrwxrwx 1 root root 9 Jun 16 08:02 ata-GCR-8483B -> ../../sr1
lrwxrwxrwx 1 root root 9 Jun 16 08:02 ata-LG_CD-RW_CED-8120B -> ../../sr0
lrwxrwxrwx 1 root root 9 Jun 16 08:02 ata-Maxtor_6E040L0_E1MWYCDE -> ../../sda
lrwxrwxrwx 1 root root 10 Jun 16 08:02 ata-Maxtor_6E040L0_E1MWYCDE-part1 ->
../../sda1
lrwxrwxrwx 1 root root 10 Jun 16 08:02 ata-Maxtor_6E040L0_E1MWYCDE-part2 ->
../../sda2
lrwxrwxrwx 1 root root 10 Jun 16 08:02 ata-Maxtor_6E040L0_E1MWYCDE-part5 ->
../../sda5
lrwxrwxrwx 1 root root 9 Jun 16 08:02 scsi-SATA_Maxtor_6E040L0_E1MWYCDE ->
../../sda
lrwxrwxrwx 1 root root 10 Jun 16 08:02 scsi-SATA_Maxtor_6E040L0_E1MWYCDE-part1
-> ../../sda1
lrwxrwxrwx 1 root root 10 Jun 16 08:02 scsi-SATA_Maxtor_6E040L0_E1MWYCDE-part2
-> ../../sda2
lrwxrwxrwx 1 root root 10 Jun 16 08:02 scsi-SATA_Maxtor_6E040L0_E1MWYCDE-part5
-> ../../sda5
lrwxrwxrwx 1 root root 9 Jul 10 08:51
usb-Kingston_DT_100_G2_0019E06B0840CCA06702241A-0:0 -> ../../sdc
lrwxrwxrwx 1 root root 10 Jul 10 08:51
usb-Kingston_DT_100_G2_0019E06B0840CCA06702241A-0:0-part1 -> ../../sdc1
lrwxrwxrwx 1 root root 9 Jul 9 09:27
usb-Verbatim_STORE_N_G0_070233A4889E0848-0:0 -> ../../sdb
lrwxrwxrwx 1 root root 10 Jul 9 09:28
usb-Verbatim_STORE_N_G0_070233A4889E0848-0:0-part1 -> ../../sdb1
```

In this example, the new USB drive is **/dev/sdc**.

4. If your Linux is configured to automount USB devices, then you must unmount the USB drive.
 - a. Check if the USB drive is mounted.

For example:

```
$ df
Filesystem      1K-blocks    Used Available Use% Mounted on
/dev/sda1       38485652 15095980  21434704  42% /
udev            504448      4      504444   1% /dev
tmpfs           102352      652     101700   1% /run
none            5120        0        5120    0% /run/lock
none            511756      0      511756   0% /run/shm
/dev/sdc1       15130624   883536   14247088  6% /mnt/usb2
```

In this example, the partition `/dev/sdc1` is mounted at mount point `/mnt/usb2`. If your USB drive is not mounted, proceed to 5.

- b. Unmount the USB drive partition.

For example:

```
$ sudo umount /mnt/usb2
```

5. Use the command line disk imaging utility to transfer the USB image onto the USB drive. A disk imaging utility restores a drive image to a drive.

For example:



CAUTION: This command erases all data on the target USB drive. Ensure you specify the correct USB drive in this command.

```
$ ls
bti7800-usb-1.6.0

$ sudo dd if=./bti7800-usb-1.6.0 of=/dev/sd bs=10M
Password:

731+1 records in
731+1 records out
7665960960 bytes (7.7 GB) copied, 630.255 s, 12.2 MB/s
$
```

where `if` is the input file (name of the USB image), and `of` is the output file (path to the USB drive). All drives are located in the `/dev` directory.



NOTE: This process might take a few minutes on faster USB drives, and up to 30 minutes on slower USB drives. No indication of progress is provided.

6. Remove the USB drive.

You have created a system repair drive that can be used to boot a BTI7800 CMM from the USB port.

Using Mac OS X to Create a BTI7800 System Repair Drive

Use this procedure on Mac OS X to create a system repair drive that can be used to boot a BTI7800 CMM from the USB port.

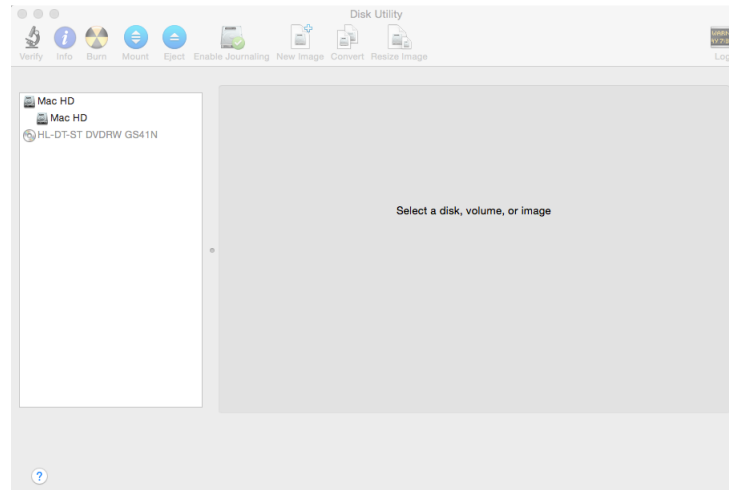
Prerequisites

- A Mac OS X machine with a USB 3.0 port and sudo access.
- A USB 3.0 flash drive (minimum 8GB).

- The BTI7800 USB image (can be downloaded from <https://www.juniper.net/support/downloads>). The software is provided as a zipped file. You must gunzip the downloaded file before starting this procedure. See “[Retrieving a BTI7800 Software Image](#)” on page 267 for more information.

1. Open **Launchpad** and select **Disk Utility**.

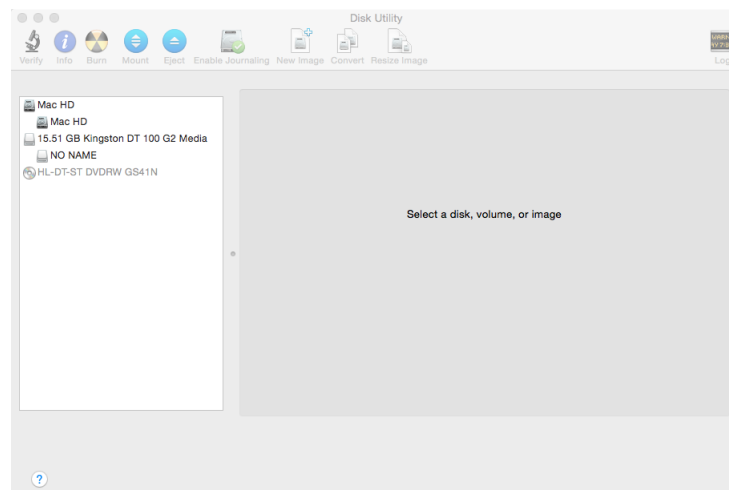
The **Disk Utility** window appears. This window lists all the drives in the system.



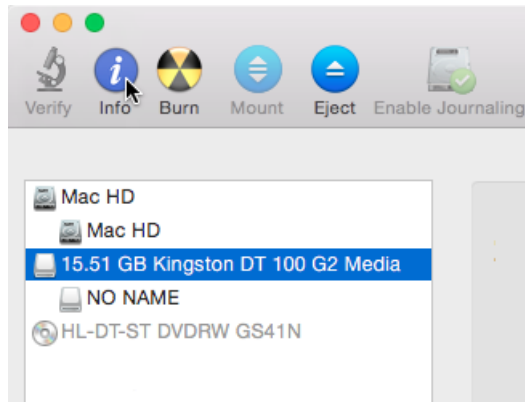
In this example, the only hard drive in the system is the internal hard drive. If you have existing USB drives attached, you will see them listed here.

2. Attach the USB drive to your Mac.

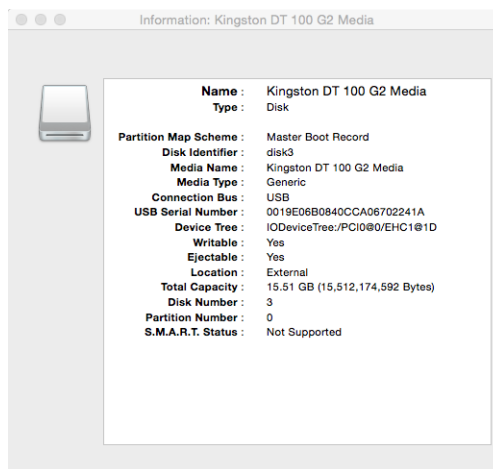
The newly attached USB drive appears in the **Disk Utility** window.



3. Determine the name that Mac OS X has assigned to the newly attached USB drive.
Highlight the USB drive entry and click the **Info** icon.



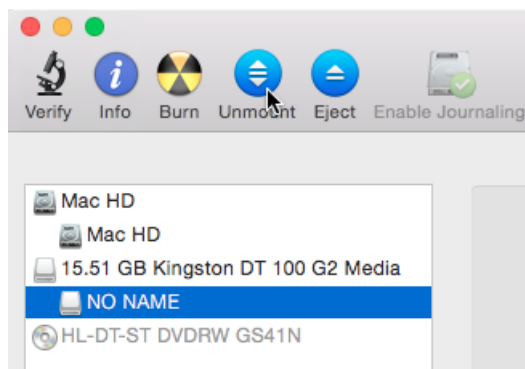
The Information window appears with more detailed information on the USB drive.



In this example, the Disk Identifier assigned by Mac OS X to this drive is **disk3**.

4. Unmount the USB drive partition. The partition must be unmounted to prevent access during the imaging process.

Select the USB drive partition entry and click **Unmount**.



5. Use the built-in command line disk imaging utility to transfer the USB image onto the USB drive. A disk imaging utility restores a drive image to a drive.

Open a Terminal session and navigate to the location that contains the USB image.



CAUTION: The imaging command erases all data on the target USB drive. Ensure you specify the correct USB drive in this command. In this example, the USB drive is `disk3`. Your USB drive assignment might be different.

For example:

```
$ ls
bti7800-usb-1.6.0

$ sudo dd if=./bti7800-usb-1.6.0 of=/dev/disk3 bs=10m
Password:

731+1 records in
731+1 records out
7665960960 bytes transferred in 1440.480677 secs (5321808 bytes/sec)
$
```

where `if` is the input file (name of the USB image), and `of` is the output file (path to the USB drive). All drives are located in the `/dev` directory.



NOTE: This process might take a couple of minutes on faster USB drives and up to 30 minutes on slower USB drives. No indication of progress is provided.

6. Eject the USB drive by clicking the **Eject** icon.

You have created a system repair drive that can be used to boot a BTI7800 CMM from the USB port.

Using Windows to Create a BTI7800 System Repair Drive

Use this procedure on Windows 7 to create a system repair drive that can be used to boot a BTI7800 CMM from the USB port.

Prerequisites

- A Windows 7 PC with a USB 3.0 port.



NOTE: This procedure assumes the use of Windows 7. The procedure might be different for other versions of Windows.

- A USB 3.0 flash drive (minimum 8GB).

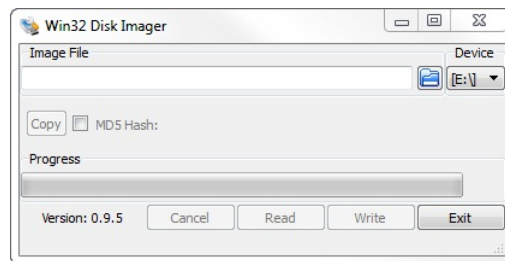
- A disk imager. This procedure uses the Win32 Disk Imager.
- The BT17800 USB image (can be downloaded from <https://www.juniper.net/support/downloads>). The software is provided as a gzipped file. You must gunzip the downloaded file before starting this procedure. See “Retrieving a BT17800 Software Image” on page 267 for more information.

1. Open Windows Explorer and click on **Computer** to see all the drives in the system.
2. Attach the USB drive to your PC.

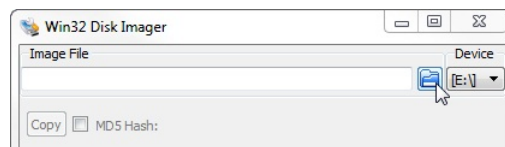
The newly attached drive should appear in the window with a new drive letter assigned.

3. Launch a disk imaging application (for example, Win32 Disk Imager). A disk imaging application is used to restore a drive image to a drive.

For example:



4. Select the USB image file by clicking on the Browse icon.

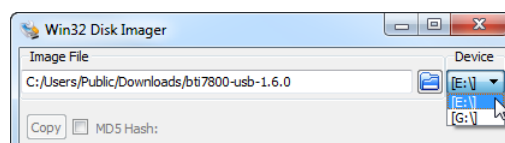


In the resulting dialog, navigate to the location where the USB image resides, select it, and click **Open**.



NOTE: By default, this program only shows *.img and *.IMG files. To show all files, change the filter to show *.*.

5. Select the target USB drive in the Device drop-down menu.





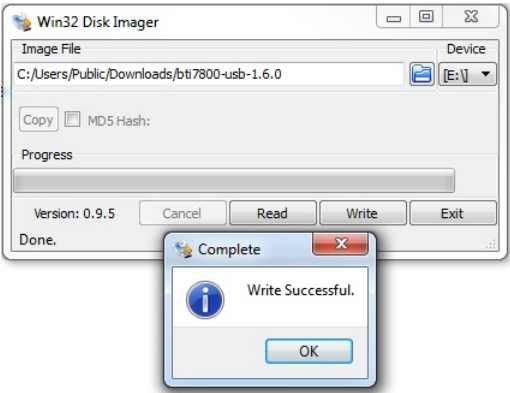
CAUTION: The imaging program erases all data on the target USB drive. Ensure you specify the correct USB drive in this command. In this example, the USB drive is E. Your USB drive assignment might be different.

6. Write the image to the USB drive by clicking on **Write**.

For example:



7. When the process completes, a **Write Successful** message appears. Click **OK**.



8. Eject the USB drive.

You have created a system repair drive that can be used to boot a BTI7800 CMM from the USB port.

BTI7800 Port Usage

Table 44: BTI7800 Port Usage

Application	Description	BTI7800 port numbers	Remote server/host port numbers
		Protocol Role: client	Protocol Role: server
FTP	For NE software upgrades, log file rotation, and other file transfer applications.	TCP:ephemeral	TCP:20,21

Table 44: BTI7800 Port Usage (continued)

Application	Description	BTI7800 port numbers	Remote server/host port numbers
SFTP, SCP	For NE software upgrades, log file rotation, and other file transfer applications.	TCP:ephemeral	TCP:22
DNS	Domain name service, used by the BTI7800 to resolve domain names.	UDP:ephemeral	UDP:53
NTP	For NTP time synchronization.	UDP:123	UDP:123
SNMP	For SNMP traps to management systems.	UDP:ephemeral	UDP:162
SYSLOG	For access to the syslog server.	UDP:ephemeral	UDP:514
RADIUS	For authentication and authorization when logging in to the BTI7800. This is only required if a RADIUS server is used.	UDP:ephemeral	UDP:1812
TACACS+	For authentication and authorization when logging in to the BTI7800. This is only required if a TACACS+ server is used.	TCP:ephemeral	TCP:49
		Protocol Role: server	Protocol Role: client
CLI over SSH	For access to the CLI.	TCP:22	TCP:ephemeral
NETCONF	For NETCONF access from management systems.	TCP:2022	TCP:ephemeral
SSH	For direct access to the NE shell.	TCP:2024	TCP:ephemeral
TL1 over Telnet	For access to TL1.	TCP:3083	TCP:ephemeral
SNMP	For SNMP access from management systems.	UDP:161	UDP:ephemeral
Traceroute	For traceroute messages.	UDP:33434-33436	UDP:ephemeral

DWDM 50-GHz Wavelength Plan

The DWDM 50-GHz wavelength plan is aligned with the ITU C-Band grid.

Table 45: DWDM Wavelength Plan (50-GHz Spacing)

Frequency (THz)	Wavelength (nm)	Client Port Number (multiplexer/demultiplexer)
196.10	1528.77	C96

Table 45: DWDM Wavelength Plan (50-GHz Spacing) (continued)

Frequency (THz)	Wavelength (nm)	Client Port Number (multiplexer/demultiplexer)
196.05	1529.16	C95
196.00	1529.55	C94
195.95	1529.94	C93
195.90	1530.33	C92
195.85	1530.72	C91
195.80	1531.12	C90
195.75	1531.51	C89
195.70	1531.90	C88
195.65	1532.29	C87
195.60	1532.68	C86
195.55	1533.07	C85
195.50	1533.47	C84
195.45	1533.86	C83
195.40	1534.25	C82
195.35	1534.64	C81
195.30	1535.04	C80
195.25	1535.43	C79
195.20	1535.82	C78
195.15	1536.22	C77
195.10	1536.61	C76
195.05	1537.00	C75
195.00	1537.40	C74
194.95	1537.79	C73

Table 45: DWDM Wavelength Plan (50-GHz Spacing) (continued)

Frequency (THz)	Wavelength (nm)	Client Port Number (multiplexer/demultiplexer)
194.90	1538.19	C72
194.85	1538.58	C71
194.80	1538.98	C70
194.75	1539.37	C69
194.70	1539.77	C68
194.65	1540.16	C67
194.60	1540.56	C66
194.55	1540.95	C65
194.50	1541.35	C64
194.45	1541.75	C63
194.40	1542.14	C62
194.35	1542.54	C61
194.30	1542.94	C60
194.25	1543.33	C59
194.20	1543.73	C58
194.15	1544.13	C57
194.10	1544.53	C56
194.05	1544.92	C55
194.00	1545.32	C54
193.95	1545.72	C53
193.90	1546.12	C52
193.85	1546.52	C51
193.80	1546.92	C50

Table 45: DWDM Wavelength Plan (50-GHz Spacing) (continued)

Frequency (THz)	Wavelength (nm)	Client Port Number (multiplexer/demultiplexer)
193.75	1547.32	C49
193.70	1547.72	C48
193.65	1548.11	C47
193.60	1548.51	C46
193.55	1548.91	C45
193.50	1549.32	C44
193.45	1549.72	C43
193.40	1550.12	C42
193.35	1550.52	C41
193.30	1550.92	C40
193.25	1551.32	C39
193.20	1551.72	C38
193.15	1552.12	C37
193.10	1552.52	C36
193.05	1552.93	C35
193.00	1553.33	C34
192.95	1553.73	C33
192.90	1554.13	C32
192.85	1554.54	C31
192.80	1554.94	C30
192.75	1555.34	C29
192.70	1555.75	C28
192.65	1556.15	C27

Table 45: DWDM Wavelength Plan (50-GHz Spacing) (continued)

Frequency (THz)	Wavelength (nm)	Client Port Number (multiplexer/demultiplexer)
192.60	1556.55	C26
192.55	1556.96	C25
192.50	1557.36	C24
192.45	1557.77	C23
192.40	1558.17	C22
192.35	1558.58	C21
192.30	1558.98	C20
192.25	1559.39	C19
192.20	1559.79	C18
192.15	1560.20	C17
192.10	1560.61	C16
192.05	1561.01	C15
192.00	1561.42	C14
191.95	1561.83	C13
191.90	1562.23	C12
191.85	1562.64	C11
191.80	1563.05	C10
191.75	1563.45	C9
191.70	1563.86	C8
191.65	1564.27	C7
191.60	1564.68	C6
191.55	1565.09	C5
191.50	1565.50	C4

Table 45: DWDM Wavelength Plan (50-GHz Spacing) (continued)

Frequency (THz)	Wavelength (nm)	Client Port Number (multiplexer/demultiplexer)
191.45	1565.91	C3
191.40	1566.31	C2
191.35	1566.72	C1

Interoperability with BTI7000 Series Network Elements

BTI7800 Series network elements can be used to aggregate and transport traffic from BTI7000 Series equipment. Client traffic from a BTI7000 Series shelf can be carried seamlessly across a BTI7800 Series backbone network over 10-Gbps and 100-Gbps links. In some configurations, a client on a BTI7000 Series network element can interwork with a client on a BTI7800 Series network element.

Interoperability can be divided into two broad areas: interconnectivity and interworking.

Interconnectivity, in the context of this section, refers to direct physical connectivity between a BTI7800 Series and a BTI7000 Series network element, usually on the line (WAN) side. Interconnectivity relates to compatibility of the protocols, mappings, maintenance signals, and other attributes that govern how two network elements communicate with each other across a fiber. This is the most basic form of interoperability, the ability to connect a fiber from one type of equipment to another.

Interworking refers to logical connectivity, usually between a client on a BTI7800 Series network element and a client on a BTI7000 Series network element. Interworking relates to the compatibility of the service being offered. In addition to the attributes that govern interconnectivity, interworking includes service-level attributes such as client protection, FPSD, PMs, and other end-to-end features.

- [Interoperability with BTI7000 Series Transponders on page 283](#)
- [Interoperability with BTI7000 Series Muxponders on page 287](#)
- [Interoperability with BTI7000 Series packetVX Modules on page 289](#)

Interoperability with BTI7000 Series Transponders

The BTI7800 Series can interoperate with the BTI7000 Series dual 10-Gbps transponders (BT7A49AA and BT7A49AA-I02).

This includes both interconnectivity and interworking:

- interconnecting a BTI7800 Series device with the line side of a BTI7000 Series transponder
- interworking between a client on a BTI7800 Series device with a client on a BTI7000 Series transponder



NOTE: Client and line designations on the BTI7800 Series equipment are conceptual only. Unlike the BTI7000 Series transponders, there are no fixed client/line ports.

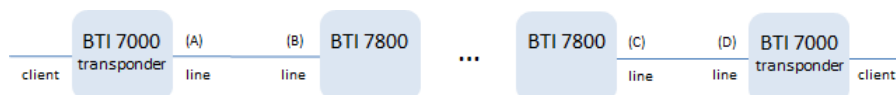


NOTE: PRBS interworking between a BTI7800 and a BTI7000 Series transponder is not supported. The BTI7000 Series transponder cannot loop back the injected BTI7800 PRBS signal.

- [Interoperability with BTI7000 Series Transponders in a Bookended Configuration on page 284](#)
- [Interworking with BTI7000 Series Transponder Clients on page 286](#)

Interoperability with BTI7000 Series Transponders in a Bookended Configuration

BTI7000 Series dual 10-Gbps transponders (BT7A49AA and BT7A49AA-IO2) can be connected to each other in a bookended configuration across BTI7800 Series equipment.



Not all protocol and line mapping combinations are supported. The main interoperability combinations supported are shown in the following table. The port designations in parentheses correspond to the reference points in the above figure.

BTI7000 Series	BTI7800 Series	BTI7800 Series	BTI7000 Series
Line Port (A)	Line Port (B)	Line Port (C)	Line Port (D)
OC192	oc192 or wanoc192 port: <ul style="list-style-type: none"> • type = sonet • mapping = asynchronous 	oc192 or wanoc192 port: <ul style="list-style-type: none"> • type = sonet • mapping = asynchronous 	OC192
OC192FEC	otu2 port: <ul style="list-style-type: none"> • type = otnOtu • fec-type = g-fec 	otu2 port: <ul style="list-style-type: none"> • type = otnOtu • fec-type = g-fec 	OC192FEC
OC192FEC	otu2 port: <ul style="list-style-type: none"> • type = otnOtu • fec-type = g-fec 	otu2 port: <ul style="list-style-type: none"> • type = otnOtu • fec-type = s-fec-i4 	OC192EFEC
OC192EFEC	otu2 port: <ul style="list-style-type: none"> • type = otnOtu • fec-type = s-fec-i4 	otu2 port: <ul style="list-style-type: none"> • type = otnOtu • fec-type = s-fec-i4 	OC192EFEC

BTI7000 Series	BTI7800 Series	BTI7800 Series	BTI7000 Series
Line Port (A)	Line Port (B)	Line Port (C)	Line Port (D)
STM64	stm64 or wanstm64 port: <ul style="list-style-type: none"> type = sonet mapping = asynchronous 	stm64 or wanstm64 port: <ul style="list-style-type: none"> type = sonet mapping = asynchronous 	STM64
STM64FEC	otu2 port: <ul style="list-style-type: none"> type = otnOtu fec-type = g-fec 	otu2 port: <ul style="list-style-type: none"> type = otnOtu fec-type = g-fec 	STM64FEC
STM64FEC	otu2 port: <ul style="list-style-type: none"> type = otnOtu fec-type = g-fec 	otu2 port: <ul style="list-style-type: none"> type = otnOtu fec-type = s-fec-i4 	STM64EFEC
STM64EFEC	otu2 port: <ul style="list-style-type: none"> type = otnOtu fec-type = s-fec-i4 	otu2 port: <ul style="list-style-type: none"> type = otnOtu fec-type = s-fec-i4 	STM64EFEC
10GELAN	10ge port: <ul style="list-style-type: none"> type = ethernetCsmacd 	10ge port: <ul style="list-style-type: none"> type = ethernetCsmacd 	10GELAN
10GELANFEC EPCMF (BT7A49AA)	otu2 port: <ul style="list-style-type: none"> type = otnOtu fec-type = g-fec 	otu2 port: <ul style="list-style-type: none"> type = otnOtu fec-type = g-fec 	10GELANFEC EPCMF (BT7A49AA)
10GELANFEC EPCMF (BT7A49AA)	otu2 port: <ul style="list-style-type: none"> type = otnOtu fec-type = g-fec 	otu2 port: <ul style="list-style-type: none"> type = otnOtu fec-type = s-fec-i4 	10GELANFEC EPCMF (BT7A49AA)
10GELANFEC EPCMF (BT7A49AA)	otu2 port: <ul style="list-style-type: none"> type = otnOtu fec-type = s-fec-i4 	otu2 port: <ul style="list-style-type: none"> type = otnOtu fec-type = s-fec-i4 	10GELANFEC EPCMF (BT7A49AA)
10GELANFEC EPV3 (BT7A49AA-I02)	otu2 port: <ul style="list-style-type: none"> type = otnOtu fec-type = g-fec 	otu2 port: <ul style="list-style-type: none"> type = otnOtu fec-type = g-fec 	10GELANFEC EPV3 (BT7A49AA-I02)
10GELANFEC EPV3 (BT7A49AA-I02)	otu2 port: <ul style="list-style-type: none"> type = otnOtu fec-type = g-fec 	otu2 port: <ul style="list-style-type: none"> type = otnOtu fec-type = s-fec-i4 	10GELANFEC EPV3 (BT7A49AA-I02)

BTI7000 Series	BTI7800 Series	BTI7800 Series	BTI7000 Series
Line Port (A)	Line Port (B)	Line Port (C)	Line Port (D)
10GELANEFEC EPV3 (BT7A49AA-I02)	otu2 port: <ul style="list-style-type: none"> type = otnOtu fec-type = s-fec-i4 	otu2 port: <ul style="list-style-type: none"> type = otnOtu fec-type = s-fec-i4 	10GELANEFEC EPV3 (BT7A49AA-I02)



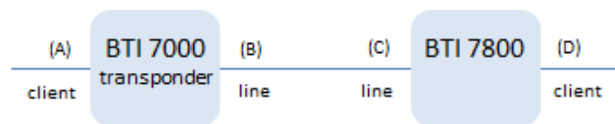
NOTE: Contact Juniper Networks Support if your interoperability configuration is not listed above.

Interworking with BTI7000 Series Transponder Clients

BTI7800 Series clients can interwork with BTI7000 Series dual 10-Gbps transponder clients (BT7A49AA and BT7A49AA-I02).



NOTE: Protection switching (client or line) is not supported in an interworking configuration.



Not all protocol and line mapping combinations are supported. The main interoperability combinations supported are shown in the following table. The port designations in parentheses correspond to the reference points in the above figure.

BTI7000 Series		BTI7800 Series	
Client Port (A)	Line Port (B)	Line Port (C)	Client Port (D)
OC192	OC192	oc192 or wanoc192 port: <ul style="list-style-type: none"> type = sonet mapping = asynchronous 	oc192 or wanoc192 port: <ul style="list-style-type: none"> type = sonet mapping = asynchronous
OC192	OC192FEC	otu2 port: <ul style="list-style-type: none"> type = otnOtu fec-type = g-fec 	oc192 or wanoc192 port: <ul style="list-style-type: none"> type = sonet mapping = bit-synchronous
OC192	OC192EFEC	otu2 port: <ul style="list-style-type: none"> type = otnOtu fec-type = s-fec-i4 	oc192 or wanoc192 port: <ul style="list-style-type: none"> type = sonet mapping = bit-synchronous

BTI7000 Series		BTI7800 Series	
Client Port (A)	Line Port (B)	Line Port (C)	Client Port (D)
STM64	STM64	stm64 or wanstm64 port: <ul style="list-style-type: none"> type = sonet mapping = asynchronous 	stm64 or wanstm64 port: <ul style="list-style-type: none"> type = sonet mapping = asynchronous
STM64	STM64FEC	otu2 port: <ul style="list-style-type: none"> type = otnOtu fec-type = g-fec 	stm64 or wanstm64 port: <ul style="list-style-type: none"> type = sonet mapping = bit-synchronous
STM64	STM64EFEC	otu2 port: <ul style="list-style-type: none"> type = otnOtu fec-type = s-fec-i4 	stm64 or wanstm64 port: <ul style="list-style-type: none"> type = sonet mapping = bit-synchronous
10GELAN	10GELAN	10ge port: <ul style="list-style-type: none"> type = ethernetCsmacd 	10ge port: <ul style="list-style-type: none"> type = ethernetCsmacd signaling-mode = standard
10GELAN	10GELANFEC EPCMF (BT7A49AA)	otu2 port: <ul style="list-style-type: none"> type = otnOtu fec-type = g-fec 	10ge port: <ul style="list-style-type: none"> type = ethernetCsmacd signaling-mode = legacy
10GELAN	10GELANEFEC EPCMF (BT7A49AA)	otu2 port: <ul style="list-style-type: none"> type = otnOtu fec-type = s-fec-i4 	10ge port: <ul style="list-style-type: none"> type = ethernetCsmacd signaling-mode = legacy
10GELAN	10GELANFEC EPV3 (BT7A49AA-I02)	otu2 port: <ul style="list-style-type: none"> type = otnOtu fec-type = g-fec 	10ge port: <ul style="list-style-type: none"> type = ethernetCsmacd signaling-mode = standard
10GELAN	10GELANEFEC EPV3 (BT7A49AA-I02)	otu2 port: <ul style="list-style-type: none"> type = otnOtu fec-type = s-fec-i4 	10ge port: <ul style="list-style-type: none"> type = ethernetCsmacd signaling-mode = standard



NOTE: Contact Juniper Networks Support if your interoperability configuration is not listed above.

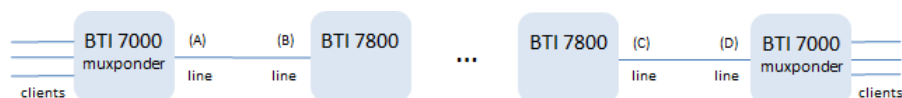
Interoperability with BTI7000 Series Muxponders

The BTI7800 Series can be used to transport the multiplexed signal from BTI7000 Series 10-Gbps muxponders (BT7A48AA, BT7A48BA, BT7A48DA) in a bookended configuration.

Interworking between a client on the BTI7000 Series muxponder and a client on the BTI7800 Series is not currently supported.



NOTE: Client and line designations on the BTI7800 Series equipment are conceptual only. Unlike the BTI7000 Series muxponders, there are no fixed client/line ports.



Not all protocol and line mapping combinations are supported. The main interoperability combinations supported are shown in the following table. The port designations in parentheses correspond to the reference points in the above figure.

BTI7000 Series	BTI7800 Series	BTI7800 Series	BTI7000 Series
Line Port (A)	Line Port (B)	Line Port (C)	Line Port (D)
<ul style="list-style-type: none"> protocol = OC192 line mapping = none 	oc192 or wanoc192 port: <ul style="list-style-type: none"> type = sonet mapping = asynchronous 	oc192 or wanoc192 port: <ul style="list-style-type: none"> type = sonet mapping = asynchronous 	<ul style="list-style-type: none"> protocol = OC192 line mapping = none
<ul style="list-style-type: none"> protocol = OC192 line mapping = none 	oc192 or wanoc192 port: <ul style="list-style-type: none"> type = sonet mapping = bit-synchronous 	otu2 port: <ul style="list-style-type: none"> type = otnOtu fec-type = g-fec 	<ul style="list-style-type: none"> protocol = OC192 line mapping = OTU2
<ul style="list-style-type: none"> protocol = OC192 line mapping = OTU2 or ODU1-OTU2 	otu2 port: <ul style="list-style-type: none"> type = otnOtu fec-type = g-fec 	otu2 port: <ul style="list-style-type: none"> type = otnOtu fec-type = g-fec 	<ul style="list-style-type: none"> protocol = OC192 line mapping = OTU2 or ODU1-OTU2
<ul style="list-style-type: none"> protocol = STM64 line mapping = none 	stm64 or wanstm64 port: <ul style="list-style-type: none"> type = sonet mapping = asynchronous 	stm64 or wanstm64 port: <ul style="list-style-type: none"> type = sonet mapping = asynchronous 	<ul style="list-style-type: none"> protocol = STM64 line mapping = none
<ul style="list-style-type: none"> protocol = STM64 line mapping = none 	stm64 or wanstm64 port: <ul style="list-style-type: none"> type = sonet mapping = bit-synchronous 	otu2 port: <ul style="list-style-type: none"> type = otnOtu fec-type = g-fec 	<ul style="list-style-type: none"> protocol = STM64 line mapping = OTU2
<ul style="list-style-type: none"> protocol = STM64 line mapping = OTU2 or ODU1-OTU2 	otu2 port: <ul style="list-style-type: none"> type = otnOtu fec-type = g-fec 	otu2 port: <ul style="list-style-type: none"> type = otnOtu fec-type = g-fec 	<ul style="list-style-type: none"> protocol = STM64 line mapping = OTU2 or ODU1-OTU2



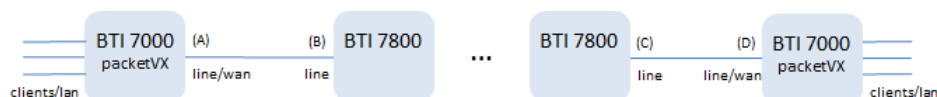
NOTE: Contact Juniper Networks Support if your interoperability configuration is not listed above.

Interoperability with BTI7000 Series packetVX Modules

The BTI7800 Series can be used to transport the Ethernet traffic from BTI7000 Series packetVX modules in a bookended configuration. Interworking between a client on the BTI7000 Series packetVX and a client on the BTI7800 Series is not currently supported.



NOTE: Client (lan) and line (wan) designations are conceptual only. There are no fixed client/line ports on either the BTI7800 Series or the packetVX modules.



Not all protocol and line mapping combinations are supported. The main interoperability combinations supported are shown in the following table. The port designations in parentheses correspond to the reference points in the above figure.

BTI7000 Series	BTI7800 Series	BTI7800 Series	BTI7000 Series
Line Port (A)	Line Port (B)	Line Port (C)	Line Port (D)
tenGigabitEthernet port: • line-mapping = 10ge-lanphy	10ge port: • type = ethernetCsmacd	10ge port: • type = ethernetCsmacd	tenGigabitEthernet port: • line-mapping = 10ge-lanphy
tenGigabitEthernet port: • line mapping = otu2-gfp1 • error-correction = FEC	otu2 port: • type = otnOtu • fec-type = g-fec	otu2 port: • type = otnOtu • fec-type = g-fec	tenGigabitEthernet port: • line mapping = otu2-gfp1 • error-correction = FEC
tenGigabitEthernet port: • line mapping = otu2-gfp1 • error-correction = FEC	otu2 port: • type = otnOtu • fec-type = g-fec	otu2 port: • type = otnOtu • fec-type = s-fec-i4	tenGigabitEthernet port: • line mapping = otu2-gfp1 • error-correction = EFEC
tenGigabitEthernet port: • line mapping = otu2-gfp1 • error-correction = EFEC	otu2 port: • type = otnOtu • fec-type = s-fec-i4	otu2 port: • type = otnOtu • fec-type = s-fec-i4	tenGigabitEthernet port: • line mapping = otu2-gfp1 • error-correction = EFEC



NOTE: Contact Juniper Networks Support if your interoperability configuration is not listed above.

