6500 Reconfigurable Line System

6500 RLS Alarms and Module Replacement

Release 4.0

323-2051-530 - Standard Issue 2
May 2025
Copyright© 2019-2025 Ciena® Corporation. All rights reserved.

LEGAL NOTICES

THIS DOCUMENT CONTAINS CONFIDENTIAL AND TRADE SECRET INFORMATION OF CIENA CORPORATION AND ITS RECEIPT OR POSSESSION DOES NOT CONVEY ANY RIGHTS TO REPRODUCE OR DISCLOSE ITS CONTENTS, OR TO MANUFACTURE, USE, OR SELL ANYTHING THAT IT MAY DESCRIBE. REPRODUCTION, DISCLOSURE, OR USE IN WHOLE OR IN PART WITHOUT THE SPECIFIC WRITTEN AUTHORIZATION OF CIENA CORPORATION IS STRICTLY FORBIDDEN.

EVERY EFFORT HAS BEEN MADE TO ENSURE THAT THE INFORMATION IN THIS DOCUMENT IS COMPLETE AND ACCURATE AT THE TIME OF PUBLISHING; HOWEVER, THE INFORMATION CONTAINED IN THIS DOCUMENT IS SUBJECT TO CHANGE.

While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing CIENA PROVIDES THIS DOCUMENT “AS IS” WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice. For the most up-to-date technical publications, visit www.ciena.com.

GAI Use Restriction. Unless expressly authorized in writing by Ciena on a case-by-case basis, you may not enter or use any Ciena Documentation in any Generative AI system, or include such information in the data for training such a system.

Copyright© 2019-2025 Ciena® Corporation. All Rights Reserved

Use or disclosure of data contained in this document is subject to the Legal Notices and restrictions in this section and, unless governed by a valid license agreement signed between you and Ciena, the Licensing Agreement that follows.

The material contained in this document is also protected by copyright laws of the United States of America and other countries. It may not be reproduced or distributed in any form by any means, altered in any fashion, or stored in a data base or retrieval system, without express written permission of the Ciena Corporation.

Security

Ciena® cannot be responsible for unauthorized use of equipment and will not make allowance or credit for unauthorized use or access.

Contacting Ciena

Corporate Headquarters	410-694-5700 or 800-921-1144	*www.ciena.com*
Customer Technical Support/Warranty		*www.ciena.com/support/*
Sales and General Information	North America: 1-800-207-3714 International: +44 20 7012 5555	E-mail: sales@ciena.com
In North America	410-694-5700 or 800-207-3714	E-mail: sales@ciena.com
In Europe	+44-207-012-5500 (UK)	E-mail: sales@ciena.com
In Asia	+81-3-3248-4680 (Japan)	E-mail: sales@ciena.com
In India	+91-22-42419600	E-mail: sales@ciena.com
In Latin America	011-5255-1719-0220 (Mexico City)	E-mail: sales@ciena.com
Training		E-mail: learning@ciena.com

For additional office locations and phone numbers, please visit the Ciena web site at www.ciena.com.

READ THIS LICENSE AGREEMENT ("LICENSE") CAREFULLY BEFORE INSTALLING OR USING CIENA SOFTWARE OR DOCUMENTATION. THIS LICENSE IS AN AGREEMENT BETWEEN YOU AND CIENA COMMUNICATIONS, INC. (OR, AS APPLICABLE, SUCH OTHER CIENA CORPORATION AFFILIATE LICENSOR) ("CIENA") GOVERNING YOUR RIGHTS TO USE THE SOFTWARE. BY INSTALLING OR USING THE SOFTWARE, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS LICENSE AND AGREE TO BE BOUND BY IT.

1. License Grant. Ciena may provide "Software" to you either (1) embedded within or running on a hardware product (together with Software, "Product") or (2) as a standalone application, and Software includes upgrades acquired by you from Ciena or a Ciena authorized reseller. The terms of this License apply to your use of the Software and associated documentation whether such has been provided by Ciena, an affiliate of Ciena, or by means of an authorized reseller or distributor. Subject to these terms, and payment of all applicable License fees including any usage-based fees, Ciena grants you, as end user, a non-exclusive, non-transferable, personal License to use the Software only in object code form, subject to any applicable authorized use, activation requirements, usage levels, scope of functionality and release level of the Software, as set forth in the applicable quote accepted by Buyer upon Buyer's issuance of an acceptable purchase order ("Order"), and in accordance with the detailed ordering information in the Ciena's generally available, applicable, Product documentation as of the date of such Order. Unless the context does not permit, Software also includes associated documentation. Where an Order is for a (a) perpetual license, you may use the Software and associated documentation for as long as you use the Product for internal business use, or a (b) subscription license, you may only use the Software and associated documentation during the subscription term. A subscription license includes Software upgrades and/or technical support Services during the subscription term (that are not included in a perpetual license), in accordance with the Order and as further described in the applicable Ciena's service description as of the date of the applicable Order. Prior to the expiration of each subscription term, Ciena will send you a quote for the annual renewal fee(s). To renew the subscription Software license(s) for additional subscription terms, you issue an Order in advance of the then-current expiration date of such subscription term.

2. Open Source and Third-Party Licenses. If any Software is subject to an open-source license that provides the end user with rights that are broader than this License, then such rights shall take precedence. Ciena warrants that using Software in accordance with its documentation will not subject you to any obligation to disclose, distribute or license your own software that interacts with Software.

3. Title. You are granted no title or ownership rights in or to the Software. Unless specifically authorized by Ciena in writing, you are not authorized to create any derivative works based upon the Software. Title to the Software, including any copies or derivative works based thereon, and to all copyrights, patents, trade secrets and other intellectual property rights in or to the Software, are and shall remain the property of Ciena and/or its licensors. Ciena's licensors are third party beneficiaries of this License. Ciena reserves to itself and its licensors all rights in the Software not expressly granted to you.

4. Confidentiality. The Software contains trade secrets of Ciena. Such trade secrets include, without limitation, the design, structure and logic of individual Software programs, their interactions with other portions of the Software, internal and external interfaces, and the programming techniques employed. The Software and related technical and commercial information, and other information received in connection with the purchase and use of the Software that a reasonable person would recognize as being confidential, are all confidential information of Ciena ("Confidential Information").

5. Obligations. You shall:

i) Hold the Software and Confidential Information in strict confidence for the benefit of Ciena using your best efforts to protect the Software and Confidential Information from unauthorized disclosure or use, and treat the Software and Confidential Information with the same degree of care as you do your own similar information, but no less than reasonable care;
ii) Keep a current record of the location of each copy of the Software you make;
iii) Use the Software only in accordance with the authorized usage level;
iv) Preserve intact any copyright, trademark, logo, legend or other notice of ownership on any original or copies of the Software, and affix to each copy of the Software you make, in the same form and location, a reproduction of the copyright notices, trademarks, and all other proprietary legends and/or logos appearing on the original copy of the Software delivered to you; and
v) Issue instructions to your authorized personnel to whom Software is disclosed, advising them of the confidential nature of the Software and provide them with a summary of the requirements of this License.

Copyright© 2019-2025 Ciena® Corporation

6. Restrictions. You shall not:

i) Use the Software or Confidential Information a) for any purpose other than your own internal business purposes; and b) other than as expressly permitted by this License;
ii) Allow anyone other than your authorized personnel who need to use the Software in connection with your rights or obligations under this License to have access to the Software;
iii) Make any copies of the Software except such limited number of copies, in machine readable form only, as may be reasonably necessary for execution in accordance with the authorized usage level or for archival purposes only;
iv) Make any modifications, enhancements, adaptations, derivative works, or translations to or of the Software;
v) Reverse engineer, disassemble, reverse translate, decompile, or in any other manner decode the Software;
vi) Make full or partial copies of the associated documentation or other printed or machine-readable matter provided with the Software unless it was supplied by Ciena in a form intended for reproduction;
vii) Export or re-export the Software and/or the associated documentation from the country in which it was received from Ciena or its authorized reseller unless authorized by Ciena in writing; or
viii) Publish the results of any benchmark tests run on the Software.

7. Audit: Upon Ciena's reasonable request you shall permit Ciena to audit the use of the Software to ensure compliance with this License.

8. U.S. Government Use. The Software is provided to the Government only with restricted rights and limited rights. Use, duplication, or disclosure by the Government is subject to restrictions set forth in FAR Sections 52-227-14 and 52-227-19 or DFARS Section 52.227-7013(C)(1)(ii), as applicable. The Software and any accompanying technical data (collectively “Materials”) are commercial within the meaning of applicable Federal acquisition regulations. The Materials were developed fully at private expense. U.S. Government use of the Materials is restricted by this License, and all other U.S. Government use is prohibited. In accordance with FAR 12.212 and DFAR Supplement 227.7202, the Software is commercial computer software and the use of the Software is further restricted by this License.

9. Term of License. This License is effective until the applicable subscription term expires or the License is terminated. You may terminate this License by giving written notice to Ciena. This License will terminate immediately if (i) you breach any term or condition of this License or (ii) you become insolvent, cease to carry on business in the ordinary course, have a receiver appointed, enter into liquidation or bankruptcy, or any analogous process in your home country. Termination shall be without prejudice to any other rights or remedies Ciena may have. Upon any termination of this License, you shall destroy and erase all copies of the Software in your possession or control, and forward written certification to Ciena that all such copies of Software have been destroyed or erased. Your obligations to hold the Confidential Information in confidence, as provided in this License, shall survive the termination of this License.

10. Compliance with laws. You agree to comply with all laws related to your installation and use of the Software. Software is subject to U.S. export control laws and may be subject to export or import regulations in other countries. If Ciena authorizes you to import or export the Software in writing, you shall obtain all necessary licenses or permits and comply with all applicable laws.

11. Limitation of Liability. ANY LIABILITY OF CIENA SHALL BE LIMITED IN THE AGGREGATE TO THE AMOUNTS PAID BY YOU TO CIENA OR ITS AUTHORIZED RESELLER FOR THE SOFTWARE. THIS LIMITATION APPLIES TO ALL CAUSES OF ACTION, INCLUDING WITHOUT LIMITATION BREACH OF CONTRACT, BREACH OF WARRANTY, NEGLIGENCE, STRICT LIABILITY, MISREPRESENTATION AND OTHER TORTS. THE LIMITATIONS OF LIABILITY DESCRIBED IN THIS SECTION ALSO APPLY TO ANY LICENSOR OF CIENA. NEITHER CIENA NOR ANY OF ITS LICENSORS SHALL BE LIABLE FOR ANY INJURY, LOSS OR DAMAGE, WHETHER INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL INCLUDING WITHOUT LIMITATION ANY LOST PROFITS, CONTRACTS, DATA OR PROGRAMS, AND THE COST OF RECOVERING SUCH DATA OR PROGRAMS, EVEN IF INFORMED OF THE POSSIBILITY OF SUCH DAMAGES IN ADVANCE.

12. General. Ciena may assign this License to an affiliate or to a purchaser of the intellectual property rights in the Software. You shall not assign or transfer this License or any rights hereunder, and any attempt to do so will be void. This License shall be governed by the laws of the State of New York without regard to conflict of laws provisions. The U.N. Convention on Contracts for the International Sale of Goods shall not apply hereto. This License constitutes the complete and exclusive agreement between the parties relating to the license for the Software and supersedes all proposals, communications, purchase orders, and prior agreements, verbal or written, between the parties. If any portion hereof is found to be void or unenforceable, the remaining provisions shall remain in full force and effect.

Copyright© 2019-2025 Ciena® Corporation

Contents

CHAPTER 1

About this document 1

Publication History 1
Updated RLS equipment descriptions 4
Documentation roadmap 9

CHAPTER 2

Alarms 11

Overview 11
- Node Essentials for alarms 12
- Alarm History 13
- Alarm Filtering 13
- Alarm Correlation 14
- Attribute Editing 18
- Alarms with more than one severity level 19
- Alarm physical reference 20
- Visual alarm indicators 20
- LEDs 21
- Lamp Test 23
- Lamp Flash 24
- Telemetry / External Alarms 25
- Restart 26
- Automatic Line Shut Off (ALSO) 26
- Associated procedures 27
- Alarm parameters 27

List of procedures 27
- Retrieving the data for the active alarm object 32
- Showing the data for the alarm counts object 34
- Retrieving alarm history 35
- RPC the data for add-notes and clear-notes object 36
- Restarting an interface module or the CTM 37
- Locating a reflective event 41
- Tracing and clearing the OTDR high reflection 44
- Amplifier in Clamped State 50
- ASE Mode Active 53
- ASE Replacement Active 54

Copyright© 2019-2025 Ciena® Corporation

Automatic Power Reduction Active 56
Automatic Shutoff 60
Automatic Shutoff Compromised 61
Automatic Shutoff Disabled 63
Autoprovisioning Mismatch 65
Bad Ethernet Connection or Port Failure 67
BGP Peer Loss 68
Boot Fail Fault 69
Call Record/s Mismatch 70
Capacity Change Inhibited 71
Capacity Change Pending 73
Certificate Expired 75
Certificate Will Expire in Less Than 90 Days 76
Circuit Pack Fail 77
Circuit Pack Mismatch 80
Circuit Pack Missing 82
Circuit Pack Unknown 85
Configuration Mismatch 87
Connection Validation Data Mismatch 88
Connection Validation Data Missing 89
Controller Inactive 90
Connection Validation Focus Mode Enabled 92
Corrupt Inventory Fault 93
Database Recovery Failed 95
Database Restore In Progress 96
Data Mismatch 97
Disk Usage - 75% 99
Disk Usage - 90% 100
Disk Full 101
Entitlement Enforcement Disabled 102
Equipment Configuration Mismatch 103
External License Server Comms Failed 104
External License Server Time Out Of Sync 105
Fiber Break Detected 106
Fiber Type Unknown 111
Firmware Mismatch 112
Forced Shutoff 113
Forced Switch Active 115
Forced Switch Active - Remote 116
Guest OS Failure 117
Hardware Subsystem Failure 118
High Fiber Loss 119
High Temperature 124
High Temperature Warning 127
Incomplete Software Package Lineup 130
Input Loss Of Signal 131
Intercard Suspected 135
Internal Management Comms Suspected Fault 140
ISIS Level1/Level2 Adjacency Loss 142
Lan Port Down 143

Copyright© 2019-2025 Ciena® Corporation

Latch Open 144
License Violation 145
Link Down 147
Lockout Active 148
Lockout Active - Remote 149
Log Collection In Progress 150
Loopback Active - Facility 151
Loss of Signal 152
Low Fiber Loss 156
Low Optical Return Loss 158
Low Optical Return Loss Input 161
Low Optical Return Loss Output 165
Low Voltage 168
MAA Dropped From Area 170
Manual Switch Active 171
Neighbor Mismatch 172
Node Unreachable 173
NTP Time Offset Exceeded 175
NTP Server Not Provisioned 176
NTP Server Unreachable 177
Optical Line Failed 179
Optical Power Degrade Low/High 183
Optical Power Out of Range Low/High 186
OSPFv2 Adjacency Loss 188
OSPFv3 Adjacency Loss 189
OSRP Connection Mismatch 190
OSRP Line Degraded 191
OSRP Line Operationally Blocked 193
OSRP Link Configuration Mismatch 195
OSRP Link Down 196
OSRP Node Is Not Up 198
OSRP Node Operationally Blocked 199
OTDR File Transfer Failed 200
OTDR High Loss Detected 201
OTDR High Reflection Detected 206
OTDR Trace In Progress 209
Permanent Snc-Group Unavailable 210
Power Failure Fault 212
Preferred IP Not Available 215
Protection Switch Complete Revertive 216
Protection Switch Complete 217
Provisioning Incompatible 219
Provisioning Incomplete 221
Provisioning Mismatch 222
RADIUS Server(s) Unavailable 224
Raman Activation Inhibited 225
Remote Node Unreachable 227
Remote Switch Mismatch 229
reset-to-factory-default Check In Progress 230
reset-to-factory Factory Release Check Failed 231

Copyright© 2019-2025 Ciena® Corporation

Section Calibration In-Progress 232
Section Degraded 234
Secure Erase Completed 236
Secure Erase Failed 237
Secure Erase In Progress 238
Shutoff Threshold Crossed 239
SID Fault 242
Slot Empty 244
Snc Datapath Fault 246
Snc Unavailable 248
Snc-Group Not Mesh-Protected 250
Snc-Group Not on Home Path 251
Snc-Group Unavailable 253
Software Deliver Failed 255
Software Release Unknown 256
Software Service Inactive 257
Software Subsystem Failure 258
Spectral loading degraded 260
Syslog Server(s) Unavailable 261
TACACS Server(s) Unavailable 262
Target Unachievable 263
Telemetry - External Alarm 278
Upgrade Failed 279
Upgrade In Progress 281
User Intrusion Attempt 282
Wait To Restore 283
Wait To Restore - Remote 284

CHAPTER 3

Module replacement **285**

Overview 285
List of procedures 285
Reseating a module 287
Replacing an R2, R4, R6-300, or R8-300 shelf 291
Replacing a Control and Timing Module (CTM) 298
Replacing a CTM front panel on an R2 shelf 305
Reconfiguring a CTM with 8GB DDR memory (RAM) to a CTM with 16GB DDR memory 308
Replacing an Access Panel in an R2 shelf 314
Replacing an Access Panel in an R4 shelf 318
Replacing an Access Panel in an R6-300 shelf 324
Replacing an Access Panel in an R8-300 shelf 328
Replacing a pluggable module 333
Replacing a shelf fan module 336
Replacing a shelf air filter in R2 or R4 shelf 343
Replacing a shelf air filter in an R6-300 or R8-300 shelf 349
Replacing a DC Power Input Module 353
Replacing an AC Power Input Module 359
Replacing a DLM, TLM C-Band module 365

Copyright© 2019-2025 Ciena® Corporation

Replacing a CMD, CCMD, or SSM module 370
Replacing a CFIM, UCS, or MonCS in an OMC2 chassis 378
Replacing the WSS 32x1 C-Band Module 381
Replacing a Fiber Interconnect Module Type 4 (FIM4)/FIM4A 384
Replacing an RLA module 386
Replacing LRU module 394
Replacing an SRA module 398
Replacing a DLE or DLA module 409
Replacing an OMC2 Chassis 417
Replacing a Trunk Protection Switch module 420

Copyright© 2019-2025 Ciena® Corporation

Copyright© 2019-2025 Ciena® Corporation

CHAPTER 1
About this document

This document provides alarm clearing and module replacement information for 6500 Reconfigurable Line System (RLS).

Publication History

This technical publication contains information on how to clear alarms and replace the related equipment for 6500 Reconfigurable Line System (RLS).

Issue 2

This document is up-issued for various corrections.

Issue 1

Issue 1 of this document includes information on the following features:

New Hardware:

- 6500-R6-300 7-Slot Shelf Assembly (R6-300) (NTK803PA)
- Access Panel (NTK805PA)
- CTM (Control and Timing Module, RLS-300) (NTK810PA)
- AC Power Input Card (100-240 Vac PIM) (NTK505UN)
- Power Input Card Type 2 (Breakerless PIM, Max 30A) (NTK505UH)
- Shelf Fan Module (NTK807PA)
- Shelf Front Door w/Extended Depth (6500-R6-300) (NTK809HM)
- Filler (for CTM slot, RLS-300) (NTK809VP)
- Shelf Air Filter (6500-R6-300) (NTK807MP)
- RLA 64x1 iC&L-Band 1xSFP Module (ROADM with Line Amplifier, RLS) (RLA 64x1 iC&L-Band) (NTK862AH)

Alarm Enhancement

- Support for the following new alarms: Controller Inactive, Section Degraded, Incomplete Software Package Lineup, OSRP Line Degraded, and Firmware Mismatch

Copyright© 2019-2025 Ciena® Corporation

New and changed alarms

The following table lists the new and changed alarms since release 2.5 in this document.

> ***Note:*** The inhibited column in the table indicates the alarms that are inhibited by default. For these alarms, you have to manually enable them after an upgrade to a release that support these alarms if you want the alarms to be raised.

Table 1 New and changed alarms

Alarm Text	New/Changed	Release	Inhibited (Yes/No)
Controller Inactive	New	4.0	No
Section Degraded	New	4.0	Yes
Incomplete Software Package Lineup	New	4.0	No
OSRP Line Degraded	New	4.0	No
Firmware Mismatch	New	4.0	No
OSRP Node Operationally Blocked	Changed	3.3	Yes
Entitlement Enforcement Disabled	New	3.3	No
Software Deliver Fail	New	3.3	No
ISIS Level 1/ Level2 Adjacency Loss	New	3.3	No
Syslog Server(s) Unavailable	New	3.3	No
Forced Switch Active - Remote	New	3.1	No
Loopback Active - Facility	New	3.1	No
Lockout Active - Remote	New	3.1	No
Low Fiber Loss	New	3.1	Yes
OTDR File Transfer Failed	New	3.1	No
Preferred IP Not Available	New	3.1	No
Provisioning Mismatch	New	3.1	Yes
Spectral Loading degraded	New	3.1	No
ASE Mode Active	New	3.0	No
Forced Switch Active	New	3.0	No
Lockout Active	New	3.0	No
NTP Server Not Provisioned	New	3.0	No

Copyright© 2019-2025 Ciena® Corporation

Alarm Text	New/Changed	Release	Inhibited (Yes/No)
Software Release Unknown	New	3.0	No
Target Unachievable	Changed	3.0	No
Wait To Restore	New	3.0	No
SNC Datapath Fault	New	2.6	No
Amplifier in Clamped State	New	2.5	Yes
ASE Replacement Active	New	2.5	No
Bad Ethernet Connection or Port Failure	New	2.5	No
Database Restore In Progress	New	2.5	No
Forced Shutoff	New	2.5	Yes
Guest OS Failure	New	2.5	No
Optical Power Degrade High	New	2.5	Yes
Optical Power Degrade Low	New	2.5	Yes
Optical Power Out Of Range High	New	2.5	Yes
Optical Power Out Of Range Low	New	2.5	Yes
OSRP Connection Mismatch	New	2.5	No
Secure Erase Completed	New	2.5	No
Secure Erase In Progress	New	2.5	No
Channel Opacity Error	Deprecated	2.5	No
Delay Measurement Timeout	Deprecated	2.5	No
High Optical Power	Deprecated	2.5	No
Input Optical Overload	Deprecated	2.5	No
Loss of Signal	Deprecated	2.5	No
Output Loss Of Signal	Deprecated	2.5	No
Signal Degrade	Deprecated	2.5	No
Power Feed Failure	Deprecated (replaced with Power Failure Fault)	2.5	No
Telemetry Loss of Signal	Deprecated	2.5	No

Copyright© 2019-2025 Ciena® Corporation

Alarm Text	New/Changed	Release	Inhibited (Yes/No)
COLAN-X Port Failure	Deprecated, replaced with “Port Failure” raised against the “colan-x” resource	2.5	No
COLAN-A Port Failure	Deprecated, replaced with “Port Failure” raised against the “colan-x” resource	2.5	No
ILAN-IN1 Port Failure	Deprecated, replaced with “Port Failure” raised against the “ilan-in1” resource	2.5	No
ILAN-OUT1 Port Failure	Deprecated, replaced with “Port Failure” raised against the “ilan-out1” resource	2.5	No
ILAN-IN2 Port Failure	Deprecated, replaced with “Port Failure” raised against the “ilan-in2” resource	2.5	No
ILAN-OUT2 Port Failure	Deprecated, replaced with “Port Failure” raised against the “ilan-out2” resource	2.5	No

Updated RLS equipment descriptions

As of RLS Release 4.0, some equipment descriptions have been updated as seen in the following table.

Table 2 Updated RLS equipment descriptions

Ordering code	Previous name	New name
600-4201-009	Crate for Packs-in-Place (6500-R4 8-slot shelf)	Packaging Crate (Packs-in-Place, R4)
600-4201-028	Crate for Packs-in-Place (6500-R2 4-slot shelf)	Packaging Crate (Packs-in-Place, R2)
600-4201-032	Crate for Packs-in-Place (6500-R8-300 8-slot shelf)	Packaging Crate (Packs-in-Place, R8-300)
NTK507QA	Cooling Fan Module	Cooling Fan Module (R8-300)
NTK807DA	Shelf Fan Module	Shelf Fan Module (R2)
NTK807FA	Shelf Fan Module	Shelf Fan Module (R4)
NTK805MA	Access Panel (6500-R4)	Access Panel (R4)
NTK805MB	Access Panel Type 2 (6500-R4)	Access Panel Type 2 (R4)

Copyright© 2019-2025 Ciena® Corporation

Ordering code	Previous name	New name
NTK805NA	Access Panel (6500-R2)	Access Panel (R2)
NTK805QA	Access Panel (6500-R8-300)	Access Panel (R8-300)
NTK806DA	Front Panel for 2xCTM (6500-R2)	Front Panel (2xCTM, R2)
NTK807MD	Shelf Air Filter (6500-R2)	Shelf Air Filter (R2)
NTK807MF	Shelf Air Filter (6500-R4)	Shelf Air Filter (R4)
NTK809DA	Shelf Front Cover Kit (6500-R2)	Shelf Front Cover Kit (R2)
NTK809DB	Left-Hinged Shelf Front Cover Kit (6500-R2)	Left-Hinged Shelf Front Cover Kit (R2)
NTK809DD	Left-Hinged Shelf Front Cover Kit w/Extended Depth (6500-R2)	Left-Hinged Shelf Front Cover Kit w/ Extended Depth (R2)
NTK809FA	Shelf Front Cover Kit (6500-R4)	Shelf Front Cover Kit (R4)
NTK809FB	Left-Hinged Shelf Front Cover Kit (6500-R4)	Left-Hinged Shelf Front Cover Kit (R4)
NTK809FD	Left-Hinged Shelf Front Cover Kit w/Extended Depth (6500-R4)	Left-Hinged Shelf Front Cover Kit w/ Extended Depth (R4)
NTK809HQ	Shelf Front Door w/Extended Depth (6500-R8-300)	Shelf Front Door w/Extended Depth (R8-300)
NTK809SA	I/F Module Carrier (2xIM slots)	I/F Module Carrier (2xIM slots, R2/R4)
NTK809VA	Filler (for CTM slot)	Filler (CTM slot, R4)
NTK809VD	Filler (for CTM slot)	Filler (CTM slot, R2)
NTK809XA	Filler (for 2xIM slots)	Filler (2xIM slots, R2/R4)
NTK809YA	Filler (for IM slot in carrier)	Filler (IM slot in carrier, R2/R4)
NTK505YAE5	Filler for R8-300 CTM or IM	Filler (RLS-300 IM slot and R8-300 CTM slot)
NTK810DA	CTM (Control and Timing Module, RLS)	CTM (Control and Timing Module, R2)
NTK810DB	CTM (Control and Timing Module, RLS)	CTM (Control and Timing Module, R2)
NTK810FA	CTM (Control and Timing Module, RLS)	CTM (Control and Timing Module, R4)
NTK810FB	CTM (Control and Timing Module, RLS)	CTM (Control and Timing Module, R4)

Copyright© 2019-2025 Ciena® Corporation

Ordering code	Previous name	New name
NTK810QA	CTM (Control and Timing Module, RLS-300)	CTM (Control and Timing Module, R8-300)
NTK810QB	CTM (Control and Timing Module, RLS-300)	CTM (Control and Timing Module, R8-300)
NTYY99EM	Packs-in-Place Kit (6500-R4 8-slot shelf)	Packs-in-Place Kit (R4)
NTYY99EN	Packs-in-Place Kit (6500-R2 4-slot shelf)	Packs-in-Place Kit (R2)
NTYY99EQ	Packs-in-Place Kit (6500-R8-300 8-slot shelf)	Packs-in-Place Kit (R8-300)
NTK509PR	Shelf Bracket and Air Baffle Kit, ETSI, front or rear exhaust, 50/100 mm setback, 515 mm center-to-center, 25 mm hole pitch (6500-R8-300)	Shelf Bracket and Air Baffle Kit, ETSI, front or rear exhaust, 515 mm center-to-center, 25 mm hole pitch, 50/100 mm setback (R8-300)
NTK509PS	Shelf Bracket and Air Baffle Kit, 23-inch, rear exhaust, 100/127 mm setback, 567 mm center-to-center, EIA hole pitch (6500-R8-300)	Shelf Bracket and Air Baffle Kit, 23-inch, rear exhaust, 567 mm center-to-center, EIA hole pitch, 100/127 mm setback (R8-300)
NTK509PF	Shelf Bracket Kit, 19-inch rack, 465 mm center-to-center mounting holes, 50/100/127 mm setback, EIA hole pitch (6500-R8-300)	Shelf Bracket Kit, 19-inch rack, 465 mm center-to-center mounting holes, EIA hole pitch, 50/100/127 mm setback (R8-300)
NTK809MN	Shelf Bracket Kit, ETSI, 515 mm center-to-center, 25 mm hole pitch, 127-202/254-461 mm (5.0-8.0/10.0-18.1 inch) 2-post/4-post inter-rail depth (6500-R4)	Shelf Bracket Kit, ETSI, 515 mm center-to-center, 25 mm hole pitch, 127-202/254-461 mm (5.0-8.0/10.0-18.1 inch) 2-post/4-post inter-rail depth (R4)
NTK809MP	Shelf Bracket Kit, 23-inch, 567 mm center-to-center, EIA hole pitch, 127-202/254-461 mm (5.0-8.0/10.0-18.1 inch) 2-post/4-post inter-rail depth (6500-R4)	Shelf Bracket Kit, 23-inch, 567 mm center-to-center, EIA hole pitch, 127-202/254-461 mm (5.0-8.0/10.0-18.1 inch) 2-post/4-post inter-rail depth (R4)
NTK809MQ	Shelf Bracket Kit, 19-inch, 465 mm center-to-center, EIA hole pitch, 127-202/254-461 mm (5.0-8.0/10.0-18.1 inch) 2-post/4-post inter-rail depth (6500-R4)	Shelf Bracket Kit, 19-inch, 465 mm center-to-center, EIA hole pitch, 127-202/254-461 mm (5.0-8.0/10.0-18.1 inch) 2-post/4-post inter-rail depth (R4)

Copyright© 2019-2025 Ciena® Corporation

Ordering code	Previous name	New name
NTK809MR	Shelf Bracket Kit, ETSI, 515 mm center-to-center, 25 mm hole pitch, 127-202/254-361 mm (5.0-8.0/10.0-14.2 inch) 2-post/4-post inter-rail depth (6500-R4)	Shelf Bracket Kit, ETSI, 515 mm center-to-center, 25 mm hole pitch, 127-202/254-361 mm (5.0-8.0/10.0-14.2 inch) 2-post/4-post inter-rail depth (R4)
NTK809MS	Shelf Bracket Kit, 23-inch, 567 mm center-to-center, EIA hole pitch, 127-202/254-361 mm (5.0-8.0/10.0-14.2 inch) 2-post/4-post inter-rail depth (6500-R4)	Shelf Bracket Kit, 23-inch, 567 mm center-to-center, EIA hole pitch, 127-202/254-361 mm (5.0-8.0/10.0-14.2 inch) 2-post/4-post inter-rail depth (R4)
NTK809MT	Shelf Bracket Kit, 19-inch, 465 mm center-to-center, EIA hole pitch, 127-202/254-361 mm (5.0-8.0/10.0-14.2 inch) 2-post/4-post inter-rail depth (6500-R4)	Shelf Bracket Kit, 19-inch, 465 mm center-to-center, EIA hole pitch, 127-202/254-361 mm (5.0-8.0/10.0-14.2 inch) 2-post/4-post inter-rail depth (R4)
NTK809MU	Shelf Sliding Bracket Kit, 19/23-inch, 465/567 mm center-to-center, EIA hole pitch, 597-914 mm (23.5-36.0 inch) depth (6500-R4/R2)	Shelf Sliding Bracket Kit, 19/23-inch, 465/567 mm center-to-center, EIA hole pitch, 597-914 mm (23.5-36.0 inch) depth (R2/R4)
NTK809MW	Shelf Sliding Bracket Kit, ETSI/19/21/23-inch, 515/465/516/567 mm center-to-center, 384-603 mm (15.1-23.75 inch) depth (6500-R4/R2)	Shelf Sliding Bracket Kit, ETSI/19/21/23-inch, 515/465/516/567 mm center-to-center, 384-603 mm (15.1-23.75 inch) depth (R2/R4)
NTK809MZ	Sliding Bracket Adapter Kit (includes 4 19-inch to 21-inch/ETSI, 6500-R4/R2)	Sliding Bracket Adapter Kit (includes 4 19-inch to 21-inch/ETSI, R2/R4)
NTK809NN	Shelf Bracket Kit, ETSI, 515 mm center-to-center, 25 mm hole pitch, 127-202/254-461 mm (5.0-8.0/10.0-18.1 inch) 2-post/4-post inter-rail depth (6500-R2)	Shelf Bracket Kit, ETSI, 515 mm center-to-center, 25 mm hole pitch, 127-202/254-461 mm (5.0-8.0/10.0-18.1 inch) 2-post/4-post inter-rail depth (R2)
NTK809NP	Shelf Bracket Kit, 23-inch, 567 mm center-to-center, EIA hole pitch, 127-202/254-461 mm (5.0-8.0/10.0-18.1 inch) 2-post/4-post inter-rail depth (6500-R2)	Shelf Bracket Kit, 23-inch, 567 mm center-to-center, EIA hole pitch, 127-202/254-461 mm (5.0-8.0/10.0-18.1 inch) 2-post/4-post inter-rail depth (R2)

Copyright© 2019-2025 Ciena® Corporation

Ordering code	Previous name	New name
NTK809NQ	Shelf Bracket Kit, 19-inch, 465 mm center-to-center, EIA hole pitch, 127-202/254-461 mm (5.0-8.0/10.0-18.1 inch) 2-post/4-post inter-rail depth (6500-R2)	Shelf Bracket Kit, 19-inch, 465 mm center-to-center, EIA hole pitch, 127-202/254-461 mm (5.0-8.0/10.0-18.1 inch) 2-post/4-post inter-rail depth (R2)
NTK809NR	Shelf Bracket Kit, ETSI, 515 mm center-to-center, 25 mm hole pitch, 127-202/254-361 mm (5.0-8.0/10.0-14.2 inch) 2-post/4-post inter-rail depth (6500-R2)	Shelf Bracket Kit, ETSI, 515 mm center-to-center, 25 mm hole pitch, 127-202/254-361 mm (5.0-8.0/10.0-14.2 inch) 2-post/4-post inter-rail depth (R2)
NTK809NS	Shelf Bracket Kit, 23-inch, 567 mm center-to-center, EIA hole pitch, 127-202/254-361 mm (5.0-8.0/10.0-14.2 inch) 2-post/4-post inter-rail depth (6500-R2)	Shelf Bracket Kit, 23-inch, 567 mm center-to-center, EIA hole pitch, 127-202/254-361 mm (5.0-8.0/10.0-14.2 inch) 2-post/4-post inter-rail depth (R2)
NTK809NT	Shelf Bracket Kit, 19-inch, 465 mm center-to-center, EIA hole pitch, 127-202/254-361 mm (5.0-8.0/10.0-14.2 inch) 2-post/4-post inter-rail depth (6500-R2)	Shelf Bracket Kit, 19-inch, 465 mm center-to-center, EIA hole pitch, 127-202/254-361 mm (5.0-8.0/10.0-14.2 inch) 2-post/4-post inter-rail depth (R2)
NTZF99YK	Bracket Kit, RLS R4, includes brackets for installation in ETSI, 23-inch and 19-inch, 127-202/254-461 mm (5.0-8.0/10.0-18.1 inch) 2-post/4-post inter-rail depth	Bracket Kit, R4, includes brackets for installation in ETSI, 23-inch and 19-inch, 127-202/254-461 mm (5.0-8.0/10.0-18.1 inch) 2-post/4-post inter-rail depth
NTZF99YL	Bracket Kit, RLS R2, includes brackets for installation in ETSI, 23-inch and 19-inch, 127-202/254-461 mm (5.0-8.0/10.0-18.1 inch) 2-post/4-post inter-rail depth	Bracket Kit, R2, includes brackets for installation in ETSI, 23-inch and 19-inch, 127-202/254-461 mm (5.0-8.0/10.0-18.1 inch) 2-post/4-post inter-rail depth
NTZF99YM	Bracket Kit, RLS R4, includes brackets for installation in ETSI, 23-inch and 19-inch	Bracket Kit, R4, includes brackets for installation in ETSI, 23-inch and 19-inch
NTZF99YN	Bracket Kit, RLS R2, includes brackets for installation in ETSI, 23-inch and 19-inch	Bracket Kit, R2, includes brackets for installation in ETSI, 23-inch and 19-inch
NTZF99YQ	Bracket and Air Baffle Kit, RLS R8-300, includes brackets for installation in ETSI, 23-inch and 19-inch	Bracket and Air Baffle Kit, R8-300, includes brackets for installation in ETSI, 23-inch and 19-inch

Copyright© 2019-2025 Ciena® Corporation

Ordering code	Previous name	New name
NTZF99YU	Sliding Bracket Kit, RLS R2/R4, 19/23-inch w/adapters for 21-inch/ETSI, 597-914 mm (23.5-36.0 inch) depth	Sliding Bracket Kit, R2/R4, 19/23-inch w/adapters for 21-inch/ETSI, 597-914 mm (23.5-36.0 inch) depth
NTZF99YV	Sliding Bracket Kit, RLS R2/R4, 19/23-inch w/adapters for 21-inch/ETSI, 800-1118 mm (31.5-44.0 inch) depth	Sliding Bracket Kit, R2/R4, 19/23-inch w/adapters for 21-inch/ETSI, 800-1118 mm (31.5-44.0 inch) depth
NTZF99ZK	Bracket Kit, RLS R4, includes brackets for installation in 19-inch and 23-inch, 127-202/254-461 mm (5.0-8.0/10.0-18.1 inch) 2-post/4-post inter-rail depth	Bracket Kit, R4, includes brackets for installation in 19-inch and 23-inch, 127-202/254-461 mm (5.0-8.0/10.0-18.1 inch) 2-post/4-post inter-rail depth
NTZF99ZL	Bracket Kit, RLS R2, includes brackets for installation in 19-inch and 23-inch, 127-202/254-461 mm (5.0-8.0/10.0-18.1 inch) 2-post/4-post inter-rail depth	Bracket Kit, R2, includes brackets for installation in 19-inch and 23-inch, 127-202/254-461 mm (5.0-8.0/10.0-18.1 inch) 2-post/4-post inter-rail depth
NTZF99ZQ	Bracket and Air Baffle Kit, RLS R8-300, includes brackets for installation in 19-inch and 23-inch EIA	Bracket and Air Baffle Kit, R8-300, includes brackets for installation in 19-inch and 23-inch EIA

Documentation roadmap

The following table provides information about documentation supporting 6500 Reconfigurable Line System for Release 4.0.

Table 3 6500 RLS documentation roadmap

Documents	Description
6500 RLS OAM Communications, 323-2051-101	This document provides OAM communications information for RLS.
6500 RLS CLI Reference, 323-2051-190	This document provides a CLI description and CLI command definition for RLS.
6500 RLS Installation Guide, 323-2051-201	This document provides installation information for the 6500 RLS shelves.
6500 RLS ZTP and Manual Commissioning, 323-2051-220	This document provides Zero Touch Provisioning (ZTP) and manual commissioning information for RLS.
6500 RLS Licensing, Security, and Administration, 323-2051-300	This document provides information on RLS licensing and security and administration information for RLS.

Copyright© 2019-2025 Ciena® Corporation

Documents	**Description**
6500 RLS Equipment/Facility Provisioning and Protection, 323-2051-310	This document provides equipment, facility, and protection provisioning information for RLS.
6500 RLS Optical Control, SPLI, and OTDR, 323-2051-318	This document provides optical control, Service and Photonic Layer Interoperability (SPLI), and Optical Time Domain Reflectometry (OTDR) information for RLS.
6500 RLS L0 Control Plane, 323-2051-330	This document provides L0 Control Plane information for RLS.
6500 RLS Logs and PMs, 323-2051-520	This document provides the information to collect and manage the Logs and Performance Monitoring data for RLS.
6500 RLS Alarms and Module Replacement, 323-2051-530	This document provides alarm clearing and module replacement information for RLS.
6500 RLS SNMP, 323-2051-700	This document provides SNMP information for RLS.
6500 RLS Planning Guide, **NTRN10WA**	This document provides planning information for RLS, including: • Overview • Configurations • Interworking • NBI information (CLI, NETCONF, gRPC, REST API, OpenConfig, NBI syntax changes, SNMP) • Node Essentials overview • Shelf descriptions and technical specifications • Module descriptions, equipping rules, specifications • Pluggables • Ordering information • Operating specifications and standards compliance
Optical Connector Inspection and Cleaning, 323-1859-500	This document includes information on how to inspect and clean single fiber ferrule optical connectors and multi fiber ferrule optical connectors on an optical fiber cable, a bulkhead, and a faceplate of a module or an optical circuit pack. Also included is limited information on cleaning pluggables.
Submarine Networking Application Guide, NTRN72BA	This document provides submarine networking information for RLS.

Copyright© 2019-2025 Ciena® Corporation

CHAPTER 2
Alarms

This section covers the following topics:

- Overview
  - Node Essentials for alarms
  - Alarm History
  - Alarm Filtering
  - Alarm Correlation
  - Attribute Editing
  - Visual alarm indicators
  - LEDs
  - Lamp Test
  - Automatic Line Shut Off (ALSO)
  - Associated procedures
- List of procedures

Overview

This section describes procedures to clear the alarms in the 6500 Reconfigurable Line System (RLS) shelf.

A complete list of alarms is provided in this document. Refer to the "List of procedures" to determine whether you must perform a specific or a generic alarm clearing procedure to clear the alarm.

Before you perform a procedure, read and understand the safety guidelines that you must follow for personal safety and to operate the equipment correctly.

Ciena documentation contains precautionary messages and safety procedures that refer to specific tasks or conditions. You must read and follow all precautionary messages before you start to work on the equipment.

Copyright© 2019-2025 Ciena® Corporation

RLS will raise alarms to notify the user about issues that require intervention to correct.

Facility alarms have a fixed debounce timer to avoid alarm toggling.

- The time delay between the condition occurring and the alarm being raised is 2.5 seconds by default.
- The time delay between the condition being removed and the alarm being cleared is 10 seconds.

All alarms will include the following information:

- Resource against which the alarm is raised
- Alarm sequence number/identifier
- Time (date and time)
- Text of the alarm
- A uni-directional or bi-directional indication
- A near-end or far-end indication
- Severity (Critical, Major, Minor, Warning)
- Service impact (service affecting, non-service affecting)
- An additional information field (provides further details about the alarm if required)

Equipment alarms do not have debounce timers.

RLS supports retrieval of the active alarms and event history, which includes previously raised alarms using CLI or NETCONF, gRPC or REST. RLS also supports alarm streaming using NETCONF, gRPC/gNMI or REST.

RLS supports retrieval of historical alarms using CLI or NETCONF, gRPC or REST. The historical alarm list can be up to 5000 alarms that can survive the CTM restart. Alarm filtering and search are also supported.

RLS will support transient conditions as alarm notifications. Transient conditions will have the same record format as active alarms except

- Object id & user-notes fields will not be available
- clear-time field will not be used
- Severity of the alarm will be “transient-condition

Node Essentials for alarms

The alarm clearing procedures in this section are CLI based. The web-based RLS Node Essentials can be used to perform similar functionalities.

Copyright© 2019-2025 Ciena® Corporation

For details about the Node Essentials, refer to the *6500 RLS Planning Guide*, NTRN10WA. For details about accessing the Node Essentials, refer to *Licensing, Security, and Administration*, 323-2051-300.

The following alarms functionalities are supported on the Node Essentials.

- Current Alarms
- Historical Alarms

Alarm History

Alarm history is the record of changes to alarm records. An alarm record is entered into the alarm history for every change made to an active alarm record which is retrievable by the users. The following capabilities are included in the alarm history:

- The alarm history survives restarts and upgrades.
- Individual alarm history records are searchable and identifiable such that a subset of the alarm history can be retrieved.
- A reason is included in each alarm history record to indicate what change was made to trigger the insertion of the record into the history.
- The alarm history records are timestamped separately from the alarms to prevent duplicates of the timestamps in the alarm record.
- The alarm history is retrieved using RPC to prevent the alarm history list being part of a global or declarative configuration retrieval.
- The alarm history records a maximum of 5000 alarm records. This number can be adjusted based on the user or customer request.

Alarm Filtering

The alarm-filtering feature will provide the following capabilities:

- retrieval can be based on any single parameter or on a group of parameters specified in a filter
- filters can be specified as a part of a retrieval, making it a “one-time use” filter
- filters can be created as objects in the system and then used in a filtered retrieve RPC by specifying the name of the filter in place of specifying a set of filter parameters
- filters can be used to access either the active alarms list or the history alarm list and either a named filter or a one-time use filter can be specified and applied to the retrieval
- in most cases parameters not specified in a filter become “all” or “don't care” items; there will be a few exceptions documented as follows

Copyright© 2019-2025 Ciena® Corporation

The list of filterable criteria that apply to both alarm records of any type is as follows:

- alarm-id
- alarm-id-range
- list of alarm severity values
- direction
- location
- alarm-state
- service-impact
- condition-type
- user-notes using a boolean flag, for example, “has-user-notes”
- additional-info using a boolean flag, “has-additional-info”
- raise-time
- raise-time range
- clear-time
- clear-time-range
- time
- time-range
- last
- list of alarm names
- list of alarm causes
- list of resources

Alarm Correlation

RLS supports alarm correlation feature to suppress all alarms related to the same cause and origin of the fault. This feature reduces the number of alarms in a system and helps to pinpoint the root cause.

This feature is enhanced to be supported for the “Target Unachievable” (TU) and “Capacity Change Pending” alarms.

Note: Ciena recommends that the alarm correlation feature is disabled for the DCI (Data Center Interconnect) configurations to avoid unexpected alarm behavior, by using the following command:

```
set slots <x> config alarm-correlation upstream-fault-
masking disabled
```


Copyright© 2019-2025 Ciena® Corporation

Alarm correlation behavior

Downstream alarms are suppressed by upstream alarm when:

- The downstream alarm is directly resulted from upstream fault where the fault causes the optical power to drop significantly beyond system's normal operation limits, such as optical line fiber cut/large pinch triggering ALSO or HFL alarm on the link or LOS alarm on adjacent OPTMON.
- There is a high probability that the downstream alarm is led by the upstream fault due to how the hardware response such as APR alarm or fiber propagation effect such as SRS impact.
- As the ambiguity increases where masking downstream alarm by certain upstream alarm from a Photonic channel point of view becomes either favorable or unfavorable depending on a case-by-case analysis. In these cases, the upstream alarm masks the downstream alarm along the channel path from Tx to Rx direction.You must fix any problem coming from upstream first and work your way following the channel path.

Alarm correlation also implies proper hold-on/hold-off criteria to prevent downstream alarm toggling when faults raise/clear.

After the CTM is restarted local alarms are raised earlier than the time it takes for upstream faults to be propagated and detected on the local shelf. Since it takes a longer time for the upstream fault to get propagated, the alarm may momentarily be raised before being masked.

Also, the active alarms on the shelf are cleared or removed in the following scenarios:

- an active CTM restart or reseated
- an active CTM protection switch
- a shelf blackout power recovery

The alarm are raised as needed when the CTM comes up after any of the aforementioned scenarios.

Treatment of "Target Unachievable" alarms

Channel TU alarms suppress downstream channel TU alarms for the same channel along the entire channel path. As long as a channel TU alarm is downstream of the other Photonic alarm, it is suppressed (regardless if it is at a local node or a downstream node).

Profile TU alarm suppression is limited within the Optical Multiplex Section (OMS) where the TU alarm is raised. It does not extend beyond the OMS boundary, For example, profile TU alarms are not suppressed by alarms in an upstream OMS.

Copyright© 2019-2025 Ciena® Corporation

Profile TU alarm suppression is done on a per spectrum band basis. An upstream profile TU alarm suppresses downstream profile TU alarms per band in the same direction. An upstream profile TU alarm on C-band ONLY suppresses downstream profile TU alarm on C-band and Upstream profile TU alarm on L-band ONLY suppresses downstream profile TU alarm on L-band.

If the fiber is faulted from RLA L-Band UPG Out port to LRU L-Band UPG In causing the L-Band Pre-Amp to become faulted (for example: “Shutoff Threshold Crossed”, “Input LOS” present), the power-profile TU alarm on the L-band RLA Line-In (or SRA line-in if SRA used) is not currently masked.

Treatment of Capacity Change Pending alarms

Since the Capacity Change Pending (CCP) condition is raised on a per CCS basis, the alarm suppression is done on a per channel level for the same channel along the channel path.

Card Level Correlation (CLC)

RLS supports alarm correlation for card alarms. For example, port-level facility alarms mask service-level facility alarms on the port, and Equipment alarms mask facility alarms associated with the equipment.

- Alarms on each circuit pack are correlated to ensure the highest priority alarm is raised, and lower priority alarms are masked.
- Alarms are masked if the associated facility state is set to disabled.
- Card level correlation is always enabled and cannot be disabled by the user.
- The user can see the masked alarm by using the CLI command display-masked-alarm.

Generally, alarm correlation occurs between alarms on a same circuit pack. This means the alarms on one circuit pack are not correlated with alarms on another circuit pack. However, some configurations support correlation between circuit packs in the same shelf. Example: For RLA/LRU, the “Forced shutoff” alarm is masked on L-band ASE or RLA when the corresponding ASE is active on the LRU.

> ***Note:*** Before you deploy and use an alarm correlation feature, you need to purchase and install a license for this feature. One license is required for each RLS shelf using alarm correlation. For more information regarding the necessary licenses for each feature, refer to *Licensing, Security, and Administration*, 323-2051-300.

ILAN and COLAN “Port Failure” alarms are masked when Access Panel is removed, replaced or the admin-state is provisioned to Disabled.

Copyright© 2019-2025 Ciena® Corporation

Shelf Level Correlation (SLC) and Network Level Correlation (NLC)

Shelf and network level faults are correlated to ensure that alarms are reported against the resource/facility closest to the fault, and alarms associated with downstream resource/facilities are masked.

- Faults caused by the absence of a provisioned service (for example, channel) are masked
- Complete (loss of optical power) faults are mask downstream faults
- Degrade (of optical power) faults do not mask complete (loss of optical power) faults

The propagation of the upstream fault information can be slower than the time it take to raise the alarm locally. When that happens, a local alarm is raised for a short period of time. This is called “alarm toggling”. The software minimizes the alarm toggling, but it can not be avoided completely.

SLC and NLC can be enabled or disabled by the user. If the feature is disabled, all alarms that were masked are raised. You can retrieve the list of active alarms that are masked by SLC/NLC alarm correlation when it is enabled, using the “display-masked-alarms” RPC command.

You can disable the effect of NLC (alarm masking) by setting slots/config/alarm-correlation/upstream-fault-masking to Disabled or Disabled-locked. “Locked” means the setting is not overwritten by the setting in shelf/upstream-fault-masking.

Some alarms cannot be masked. For example, Optical Line Failed, Automatic Shutoff, hfl (High Fiber Loss), Fiber Break Detected, Automatic Power Reduction. The “Circuit Pack Failed” alarm does not mask any alarm.

The RLS Network Level Correlation feature requires a specific feature license to use (S74-LIC-NTK800BG). One license is required for each RLS shelf using Network Level Correlation.

The NLC feature is disabled by default. You must enable NLC in NLC system parameters before upgrading the shelf software. You can disable/enable NLC feature using the following CLI Commands:

To disable NLC enter:

```
set ciena-6500r-system:system features "ALARM
CORRELATION" enabled false
```

To enable NLC enter:

```
set ciena-6500r-system:system features "ALARM
CORRELATION" enabled true
```


Copyright© 2019-2025 Ciena® Corporation

Note: There is no Node Essentials equivalent command for this release.

Service Awareness Correlation (SAC) hold-off timer

The SAC mechanism prevents alarms from raising against CCMD ports with no channel provisioned. Without the hold-off time applied, as soon as a channel is provisioned, alarm masking would cease. In certain situations, absence of the hold-off timer can result in toggling the “Shutoff Threshold Crossed” alarms on a CCMD amp. A hold-off timer on SAC, extends the masking time and eliminates the alarm toggling.

If the CCMD does not have a Mux AMP, the toggling alarm would have been the RLA/LRU switch input port LOS. For example, first visible alarm condition after the CCMD MUX input port.

- Hold-off time is five Minutes
- After a CTM restart, the SAC hold-off applied is 30 seconds, otherwise ‘real’ alarms would be masked during 5 minutes.

Attribute Editing

The following alarm template attributes can be edited.

- Severity of the alarm
- Enabling or disabling of the alarm
- Cause of the alarm

Note: Other changed-alarms parameters (condition-type, direction, location, provisionable, service-impact, type) are not supported in this release. Attempting to edit them, causes an error message.

Changes to the alarm attributes are shelf-wide and retained over a CTM restart. Editing is supported using CLI, NETCONF, gRPC and REST. You cannot retrieve the list of alarms that are active but inhibited. For example, the associated template is set to disabled.

Editing of alarm templates associated with the following are blocked:

- Preventing equipment damage (for example, high temperature)
- Protecting physical safety (for example, laser safety)

You cannot disable the alarms associated with preventing equipment damage or Protecting physical safety or change the cause field. However, the severity can be edited. The severity of the alarm can be increased from the default but cannot be decreased. For example, for a safety related alarm with a default severity of Major, you can only select Major or Critical severity.

The complete list of alarms is available using “defined-alarms” command. This is the complete list of system defined alarm templates with all user changes applied. This list can only be queried and cannot be edited.

Copyright© 2019-2025 Ciena® Corporation

Note: Use “show defined-alarms <Tab>” to get complete list of all available alarm template names.

Alarms are edited against the changed-alarms object. The user needs to specify the alarm template name they wish to change (name is available in “show defined-alarms” alarm template definition). This records the changes to the individual alarm templates. This object can be edited or retrieved.

For example: set changed-alarms clamped template-state enabled.

show defined-alarms clamped

```
   name             : clamped*    type             : high    cause            :
Amplifier in Clamped State   condition-type  : OTS-AMP-CLAMPED   location
: near-end    severity         : major    service-impact   : nsa    template-
state   : enabled    provisionable    : true
```

Editable fields on the “changed-alarms” object are:

1 Template-state

2 Severity – alarm templates provide two mutually exclusive ways to provide severity information

   a. One-severity-per-alarm (for example, normal; most alarms are done this way)

   b. Multiple severities, one template with “high” and “low” severities; this provides proper alarm-manager control of different severity levels of the same alarm (this method is rarely used).

3 Cause of the alarm

Editing an alarm-severity or the alarm cause, does not take effect until the next instance of an alarm. Editing a template-state takes effect on any and all currently active alarms.

- When the template-state is edited to “inhibited”, a “virtual” clear report will be generated and the alarm counts will be adjusted accordingly.
- When the template-state is edited to “enabled”, the original alarm will be re-raised.

Alarms that are raised or cleared while inhibited do not generate an alarm report and do not adjust the alarm counts.

Alarms with more than one severity level

Alarms that have different degrees of severity level depending on circumstances are called “multi-level” alarms. For example, a failed facility that is protected might be a minor severity since traffic is not affected whereas an outage to that same facility if there is no protection is major severity since it will result in a traffic loss. The following table lists the examples of multilevel alarms.

Copyright© 2019-2025 Ciena® Corporation

Table 4 Example of multilevel alarms

Alarm Text	Level (High/Low)		Severity		Service Impact	
Circuit Pack Mismatch	High	Low	Major	Minor	SA	NSA
Circuit Pack Missing	High	Low	Major	Minor	SA	NSA
High Fiber Loss	High	Low	Major	Minor	NSA	NSA
NTP Server Unreacable	High	Low	Major	Minor	SA	NSA
Optical Power Out of Range High	High	Low	Major	Minor	SA	NSA
Optical Power Out of Range Low	High	Low	Major	Minor	SA	NSA
OTDR High Loss Detected	High	Low	Major	Minor	SA	NSA
OTDR High Reflection Detected	High	Low	Major	Minor	SA	NSA

Alarm physical reference

When alarms are raised, the external port references in the resource field (for example:`numerical shelf, slot, sub-slot, port, sub-port`) are shown for all alarms generated at an Interface Module port.

Visual alarm indicators

At the Access Panel - Critical, Major and Minor alarm LEDs are lit if there are any corresponding severity alarms active on the chassis. A Rear Alarm LED is also provided.

In addition, Interface Module (IM), CTM, Access Panel status LEDs and port LEDs indicate alarming.

All alarms include the following information

- Alarm name
- Raise time (date and time)
- A uni-directional or bi-directional indication
- Location (near-end or far-end)
- Severity (Critical, Major, Minor, Event)
- Alarm ID
- Alarm cause

RLS supports the retrieval of the active alarms and alarm history using CLI. Notification subscribe can retrieve on-going alarm notifications using NETCONF.

Copyright© 2019-2025 Ciena® Corporation

LEDs

This section define the various LEDs and their status information based on their shape and color.

Interface Modules (IM) and CTM status LED definitions

Interface Modules (IM) and CTM status LED definitions are as follows:

Red triangle (Fail)

- Used to communicate hardware or software failure state - Card OK = LED off, Card Failed = LED on

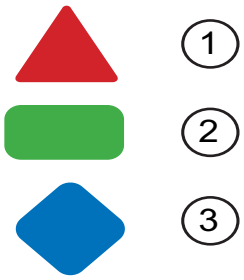
Green rectangle (Ready)

- Used to communicate hardware or software functional state (Module is healthy and available for use, does not reflect provisioning state)
- Card initializing = Blinking LED; Card active = LED on; Card failed = LED off

Blue diamond (In Use)

- Used to communicate whether CTM or IM can be extracted
- on = no pull, off = can be pulled
- Admin state of the equipment “Enabled” = LED on; Admin state of the equipment “Disabled” = LED off

Figure 1 Module LEDs



Legend

1	Fail
2	Ready
3	In Use

Interface Module port LED definitions

- LED OFF Circle: Used to communicate facility not provisioned.
- RED Circle: Used to communicate pluggable module failed.
- YELLOW Circle: Used to communicate that the facility is provisioned and the signal is failed.

Copyright© 2019-2025 Ciena® Corporation

- GREEN Circle: Used to communicate that the facility is provisioned and the signal is not failed.

Ethernet ports LED definitions

- YELLOW Square: Indicates data transfer. It will blink rapidly while data is received, and will be off if there is nothing being received.
- GREEN Square: Indicates link status. It will be on if link is established, and off if there is no link established.
- GREEN Circle: Indicates if the CTM/Craft is active. This Craft LED is only available on CTMs.
- RED Square: Not supported on the Ethernet ports.

Access Panel status LED definitions

Shelf-level alarms LEDs

- RED Circle Critical: Indicates a Critical alarm is present in the system.
- RED Circle Major: Indicates a Major alarm is present in the system.
- Orange Circle Minor: Indicates a Minor alarm is present in the system.
- Red Circle Rear Alarm: there is an alarm against the rear facing common equipment (Fan/PIM).

Access Panel port LED definitions

ILAN/ILAN2 pluggable LEDs are tri-coloured and follow the same convention as RLS IM port LEDs:

- LED OFF Circle: Used to communicate facility not provisioned.
- RED Circle: Used to communicate pluggable module failed.
- YELLOW Circle: Used to communicate that the facility is provisioned and the signal is failed.
- GREEN Circle: Used to communicate that the facility is provisioned and the signal is not failed.

Functional LED definitions and labeling

Power Input Module (PIM):

- Green power OK – Indicates that the voltage applied to the PIM is above a defined threshold. There is one LED per power input feed.

Access Panel (for R2 and R4 shelves only):

- Red Critical – Indicates a shelf level critical alarm
- Red Major – Indicates a shelf level major alarm
- Orange Minor – Indicates a shelf level minor alarm
- Red rear alarm – Indicates to user alarm (faults) are against the rear of the shelf

Copyright© 2019-2025 Ciena® Corporation

The fan modules have a triangular red LED and a rectangular green LED.

- The red LED turns on to indicate a fan module failure.
- The green LED turns on to indicate an operational fan module.

The fan module on the R8-300 shelf has the following LEDs:

- Red Critical - Indicates a shelf level critical alarm
- Red Major - Indicates a shelf level major alarm
- Orange Minor - Indicates a shelf level minor alarm

The R8-300 shelf fan module has an ACO/Lamp Test button with an ACO LED. Alarm cut-off (ACO) is not supported; only the shelf lamp test is supported.

Lamp Test

RLS supports a user-initiated Lamp Test on a per-shelf, slot or sub-slot basis. The Lamp Test button on the R8-300 shelf is supported and can be initiated as follows:

- If no Shelf LEDs are On (no Major/Minor/Critical shelf alarms are active), press the ACO Button once and hold it for 5 seconds to trigger the Lamp Test.
- If either of the Shelf LEDs (Major/Minor/Critical) are on, press the ACO Button twice and hold it for 5 seconds to trigger the Lamp test.

Lamp Test can be executed using the following CLI command:

```
action slots <slot number> lamp-test
```

When initiated on a:

- Shelf - the lamp test illuminates all supported LEDs on the chassis including CTM cards, IM cards, AP and fan cooling modules. The R2 shelf has an extra FRU Front Panel for the CTM. The LED for the corresponding CTM is illuminated during the lamp test. The power card LEDs are not included in the lamp test. The LEDs on ports that are not used, are lit during the lamp test. See the following LED behavior for special cases :
  - AP External Inventory Port supports 1 green LED and will light up during lamp test.
  - For R2 AP (NTK805NA) Telemetry port and ESI/ESO port LEDs are not supported and will not light up during lamp test.
  - For R4 AP (NTK805MA) or R8-300 AP (NTK805QA) or R6-300 (NTK805PA), Console port, Telemetry ports and ESI/ESO ports LEDs are not supported and will not light up during lamp test
  - For R4 AP Type 2 (NTK805MB), Console port and Telemetry ports LEDs are not supported and will not light up during lamp test

Copyright© 2019-2025 Ciena® Corporation

Note: The R2, R4, R6-300, and R8-300 Access Panel Telemetry and Console ports LEDs are not supported. Therefore will not light-up during usage or during the lamp test.

- Slot - the lamp test illuminates all supported LEDs on the equipment in a given slot.
- Sub-slot - the lamp test is not supported on the sub-slot. Lamp-test is only supported on a module.

The lamp test duration is 30 seconds. Multi-color LEDs cycle through red, yellow, and green during the lamp test. For tri-color LEDs, each color illuminates for 10 seconds (red -> yellow -> green). For bi-color LEDs, each color illuminates for 15 seconds (red -> yellow) or (yellow -> green) or (red -> green) as applicable.

For interface modules, the card status LEDs (Green/Blue/Red) will illuminate solid for the duration of the lamp test.

When a CCMD is undergoing a Secure Erase operation, the Lamp Test on that particular CCMD is not supported.

Lamp Flash

RLS supports a user-initiated Lamp Flash on a shelf, slot, sub-slot or port basis. Lamp Flash is available using all available NBIs. Lamp Flash can be executed using the following CLI commands:

```
action shelf lamp-flash

action slot <slot number> lamp-flash

action slot <slot number> config port <port number> lamp-
flash test-action start

action slot <slot number> config port <port number> lamp-
flash test-action stop
```

Example for CCMD8x24 in slot 5 and Channel Input port 26:

```
action slot 5 config port 26 lamp-flash test-action start

action slot 5 config port 26 lamp-flash test-action stop
```

There are two types of Lamp Flash are supported:

- Card level: only card status LEDs blink
- Port level: Card status LEDs + port led blinks green if supported. Otherwise, blinks yellow

Copyright© 2019-2025 Ciena® Corporation

When initiated on a:

- Card LED – the card lamp flash will flash all three card status LEDs on CTM or IM cards. Lamp flash will flash the Critical/Major/Minor alarm LEDs on R2 or R4 AP. All 3 external Inventory LEDs (slot 71, 72, 73) on R8-300 AP will flash. Both external Inventory LEDs (slot 71, 72) on R6-300 AP will flash.
- Sub-slot – the lamp flash will flash card LEDs as well as status LEDs on the equipment in the given sub-slot.
- Port – the lamp flash will flash card LEDs, any status LEDs associated with the equipment in the sub-slot (if applicable) and the designated port LED.

The lamp test duration is 15 minutes. Lamp Flash can be turned off by the user prior to the 15 minutes expiring. Multi-color LEDs use a single color during a Lamp Flash. For tri-color LEDs, each color illuminates for 10 seconds (red -> yellow -> green). For bi-color LEDs, each color illuminates for 15 seconds (red -> yellow) or (yellow -> green) or (red -> green) as applicable.

For tri-color LEDs (red, yellow, green) - green is used.

For bi-color LEDs;

- (red, yellow) – yellow is used
- (yellow, green) – green is used
- (red, green) – green is used

Lamp flash is not supported with the Power Modules and Fan cooling module.

Telemetry / External Alarms

The Access Panel provides a single Telemetry general purpose input that can be used to monitor (input) external equipment.

Alarm attribute editing is supported as follows:

```
set changed-alarms "alarm name" cause "alarm cause"
```

Note: There is no Node Essentials equivalent command for this release.

When an external alarm point is triggered, an associated alarm is raised against the Access Panel (slot 40).

- Alarm “name” identifies the specific telemetry input (for example, TELEMETRY IN 1, TELEMETRY IN 2.
- A default alarm “cause” is required (for example, “Telemetry – External Alarm).
- Alarm “cause” is editable by the user.

Copyright© 2019-2025 Ciena® Corporation

- Default severity (Minor)

To clear an external alarm raised against the Access Panel, verify the external equipment.

Restart

The following user-initiated restarts can be performed through CLI, NETCONF, gRPC and REST commands.

- CTM cards – cold or power-on
- IM cards – warm or cold

CTM cards:

- A restart of a CTM does not impact traffic. However, it impacts management network communications. For Duplex CTM configurations, OAM connectivity to the chassis is lost during the time required to launch applications on the secondary CTM.

  Restarts of CTM cards have a target completion of 5 minutes (OAM access is available after 5 minutes)

Interface Modules (IM) cards:

- A warm restart of the IM card does not impact traffic. However, a cold restart of the IM card impacts traffic.

  The pinhole reset button on the CTM front panel of the R2 shelf is supported. Pressing the button results in the corresponding CTM to undergo a power-on restart. A power-on restart mimics, as close as possible, the physical reseat of the CTM card.

Automatic Line Shut Off (ALSO)

RLS supports ALSO. Line facing AMP modules support ALSO bi-directional and uni-directional cuts. ALSO functions even if CTM is missing or failed.

ALSO triggers the Optical Line Failed (OLF) alarm when Line In Shutoff Threshold Crossed and OSC Loss of Signal alarms are raised. Automatic Shutoff is also triggered when OSC Continuity Check Message (CCM) RDI is active.

For unidirectional operation of the ALSO functionalities, auto-negotiation is automatically disabled on the GE OSC interface.

ALSO can be disabled by the user. You can provision the time to automatically re-enable ALSO.

Copyright© 2019-2025 Ciena® Corporation

Associated procedures

Some procedures require the user to perform procedures relating to other topics. Before performing a procedure, if necessary, ensure the information about the associated procedures is available.

All procedures assume that you have logged into the network element. Refer to “Accessing and logging in to a network element” procedure in *Licensing, Security, and Administration*, 323-2051-300.

Alarm parameters

The following table provides the alarm parameters, options and description.

Table 5 Alarm parameters

Parameter	Values	Description
additional-info	string	Additional information supplied by system
cause	string	text
condition-type	condition-type	text
direction	direction	Direction indication of the alarm
id	alarm-id	Alarm instance identifier
location	N/A	Location indication of the alarm
note-time	yang:date-and-time	Time the user-note was entered
name	string	Alarm template name
note (user-notes)	string	Free text field for user supplied notes
resource	instance-identifier	Resource under alarm
raise-time	yang:date-and-time	Time alarm was raised
severity	unknown/critical/major/ minor/warning	Severity of alarm.
template-name	instance-identifier	Alarm template to select
type	high/low	Alarm template type

List of procedures

- Procedure 1, “Retrieving the data for the active alarm object”
- Procedure 2, “Showing the data for the alarm counts object”
- Procedure 3, “Retrieving alarm history”
- Procedure 4, “RPC the data for add-notes and clear-notes object”
- Procedure 5, “Restarting an interface module or the CTM”

Copyright© 2019-2025 Ciena® Corporation

- Procedure 6, “Locating a reflective event”
- Procedure 7, “Tracing and clearing the OTDR high reflection”
- Procedure 8, “Amplifier in Clamped State”
- Procedure 9, “ASE Mode Active”
- Procedure 10, “ASE Replacement Active”
- Procedure 11, “Automatic Power Reduction Active”
- Procedure 12, “Automatic Shutoff”
- Procedure 13, “Automatic Shutoff Compromised”
- Procedure 14, “Automatic Shutoff Disabled”
- Procedure 15, “Autoprovisioning Mismatch”
- Procedure 16, “Bad Ethernet Connection or Port Failure”
- Procedure 17, “BGP Peer Loss”
- Procedure 18, “Boot Fail Fault”
- Procedure 19, “Call Record/s Mismatch”
- Procedure 20, “Capacity Change Inhibited”
- Procedure 21, “Capacity Change Pending”
- Procedure 22, “Certificate Expired”
- Procedure 23, “Certificate Will Expire in Less Than 90 Days”
- Procedure 24, “Circuit Pack Fail”
- Procedure 25, “Circuit Pack Mismatch”
- Procedure 26, “Circuit Pack Missing”
- Procedure 27, “Circuit Pack Unknown”
- Procedure 28, “Configuration Mismatch”
- Procedure 29, “Connection Validation Data Mismatch”
- Procedure 30, “Connection Validation Data Missing”
- Procedure 32, “Connection Validation Focus Mode Enabled”
- Procedure 31, “Controller Inactive”
- Procedure 33, “Corrupt Inventory Fault”
- Procedure 34, “Database Recovery Failed”
- Procedure 35, “Database Restore In Progress”
- Procedure 36, “Data Mismatch”
- Procedure 37, “Disk Usage - 75%”
- Procedure 38, “Disk Usage - 90%”

Copyright© 2019-2025 Ciena® Corporation

- Procedure 39, “Disk Full”
- Procedure 40, “Entitlement Enforcement Disabled”
- Procedure 41, “Equipment Configuration Mismatch”
- Procedure 42, “External License Server Comms Failed”
- Procedure 43, “External License Server Time Out Of Sync”
- Procedure 44, “Fiber Break Detected”
- Procedure 45, “Fiber Type Unknown”
- Procedure 46, “Firmware Mismatch”
- Procedure 47, “Forced Shutoff”
- Procedure 48, “Forced Switch Active”
- Procedure 49, “Forced Switch Active - Remote”
- Procedure 50, “Guest OS Failure”
- Procedure 51, “Hardware Subsystem Failure”
- Procedure 52, “High Fiber Loss”
- Procedure 53, “High Temperature”
- Procedure 54, “High Temperature Warning”
- Procedure 55, “Incomplete Software Package Lineup”
- Procedure 56, “Input Loss Of Signal”
- Procedure 57, “Intercard Suspected”
- Procedure 58, “Internal Management Comms Suspected Fault”
- Procedure 59, “ISIS Level1/Level2 Adjacency Loss”
- Procedure 60, “Lan Port Down”
- Procedure 61, “Latch Open”
- Procedure 62, “License Violation”
- Procedure 63, “Link Down”
- Procedure 64, “Lockout Active”
- Procedure 65, “Lockout Active - Remote”
- Procedure 66, “Log Collection In Progress”
- Procedure 67, “Loopback Active - Facility”
- Procedure 68, “Loss of Signal”
- Procedure 69, “Low Fiber Loss”
- Procedure 70, “Low Optical Return Loss”
- Procedure 71, “Low Optical Return Loss Input”

Copyright© 2019-2025 Ciena® Corporation

- Procedure 72, “Low Optical Return Loss Output”
- Procedure 73, “Low Voltage”
- Procedure 74, “MAA Dropped From Area”
- Procedure 75, “Manual Switch Active”
- Procedure 76, “Neighbor Mismatch”
- Procedure 77, “Node Unreachable”
- Procedure 78, “NTP Time Offset Exceeded”
- Procedure 79, “NTP Server Not Provisioned”
- Procedure 80, “NTP Server Unreachable”
- Procedure 81, “Optical Line Failed”
- Procedure 82, “Optical Power Degrade Low/High”
- Procedure 83, “Optical Power Out of Range Low/High”
- Procedure 84, “OSPFv2 Adjacency Loss”
- Procedure 85, “OSPFv3 Adjacency Loss”
- Procedure 86, “OSRP Connection Mismatch”
- Procedure 87, “OSRP Line Degraded”
- Procedure 88, “OSRP Line Operationally Blocked”
- Procedure 89, “OSRP Link Configuration Mismatch”
- Procedure 90, “OSRP Link Down”
- Procedure 91, “OSRP Node Is Not Up”
- Procedure 92, “OSRP Node Operationally Blocked”
- Procedure 93, “OTDR File Transfer Failed”
- Procedure 94, “OTDR High Loss Detected”
- Procedure 95, “OTDR High Reflection Detected”
- Procedure 96, “OTDR Trace In Progress”
- Procedure 97, “Permanent Snc-Group Unavailable”
- Procedure 98, “Power Failure Fault”
- Procedure 99, “Preferred IP Not Available”
- Procedure 100, “Protection Switch Complete Revertive”
- Procedure 101, “Protection Switch Complete”
- Procedure 102, “Provisioning Incompatible”
- Procedure 103, “Provisioning Incomplete”
- Procedure 104, “Provisioning Mismatch”

Copyright© 2019-2025 Ciena® Corporation

- Procedure 105, “RADIUS Server(s) Unavailable”
- Procedure 106, “Raman Activation Inhibited”
- Procedure 107, “Remote Node Unreachable”
- Procedure 108, “Remote Switch Mismatch”
- Procedure 109, “reset-to-factory-default Check In Progress”
- Procedure 110, “reset-to-factory Factory Release Check Failed”
- Procedure 111, “Section Calibration In-Progress”
- Procedure 112, “Section Degraded”
- Procedure 113, “Secure Erase Completed”
- Procedure 114, “Secure Erase Failed”
- Procedure 115, “Secure Erase In Progress”
- Procedure 116, “Shutoff Threshold Crossed”
- Procedure 117, “SID Fault”
- Procedure 118, “Slot Empty”
- Procedure 119, “Snc Datapath Fault”
- Procedure 120, “Snc Unavailable”
- Procedure 121, “Snc-Group Not Mesh-Protected”
- Procedure 122, “Snc-Group Not on Home Path”
- Procedure 123, “Snc-Group Unavailable”
- Procedure 124, “Software Deliver Failed”
- Procedure 125, “Software Release Unknown”
- Procedure 126, “Software Service Inactive”
- Procedure 127, “Software Subsystem Failure”
- Procedure 128, “Spectral loading degraded”
- Procedure 129, “Syslog Server(s) Unavailable”
- Procedure 130, “TACACS Server(s) Unavailable”
- Procedure 131, “Target Unachievable”
- Procedure 132, “Telemetry - External Alarm”
- Procedure 133, “Upgrade Failed”
- Procedure 134, “Upgrade In Progress”
- Procedure 135, “User Intrusion Attempt”
- Procedure 136, “Wait To Restore”
- Procedure 137, “Wait To Restore - Remote”

Copyright© 2019-2025 Ciena® Corporation

Procedure 1 Retrieving the data for the active alarm object

Use this procedure to show the data for the active-alarm object and its children.

Steps

1 Start a CLI session. See “Accessing and logging in to a network element” in the *Licensing, Security, and Administration*, 323-2051-300.

2 Retrieve the data for the active-alarm object:

If you want to perform the procedure using	**Then** go to the
CLI commands	“CLI INTERFACE STEPS”
Node Essentials	“NODE ESSENTIALS STEPS”

CLI INTERFACE STEPS

3 This command is best run in tabular format. To enter table display mode, use the CLI command “display table”. To retrieve the data for the active-alarm object, enter:

```
show active-alarm [id] [name] resource raise-time [clear-time] cause [condition-type] [direction] [location] severity service-impact [additional-info] [user-notes...]
```

Refer to “Alarm parameters” on page 27 for applicable parameters. Go to step 6.

4 To show active-alarm user-notes using CLI commands, enter:

```
show active-alarm user-notes <note-time> note
```

NODE ESSENTIALS STEPS

5 Select **Alarms > Current alarms** from the Node Essentials navigation menu.

The Current alarms page displays the current active alarms in the alarm grid.

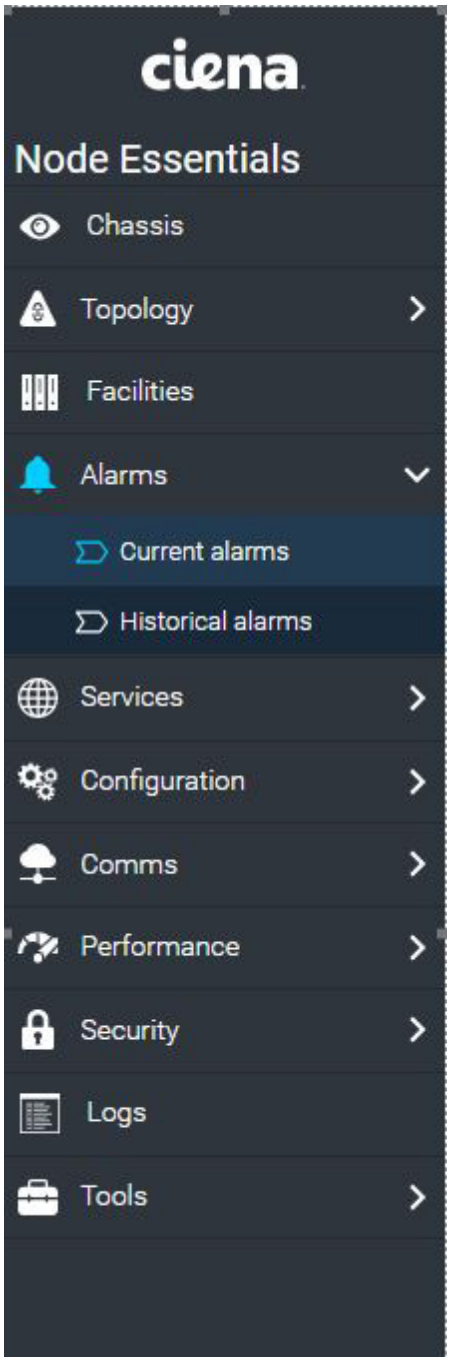
Note: The alarm timeline graph located above the alarm grid, shows the alarms raised in the past 24 hours.

6 The active-alarm user-notes in Node Essentials is accessed by selecting the **User notes** icon on the top right of the alarm grid.

You have completed the procedure.

Copyright© 2019-2025 Ciena® Corporation

Figure 2 Alarms menu



Copyright© 2019-2025 Ciena® Corporation

Procedure 2 Showing the data for the alarm counts object

Use this procedure to show alarm counts for the alarm counts object and its children.

Steps

1. Start a CLI session. See “Accessing and logging in to a network element” in the *Licensing, Security, and Administration*, 323-2051-300.
2. Retrieve the data for the alarm counts object:

If you want to perform the procedure using	**Then** go to the
CLI commands	“CLI INTERFACE STEPS”
Node Essentials	“NODE ESSENTIALS STEPS”

CLI INTERFACE STEPS

3. To show the data for the alarm-counts object and its children, enter:

```
show alarm-counts [critical] [major] [minor] [warning]
```

Refer to “Alarm parameters” on page 27 for applicable parameters.

NODE ESSENTIALS STEPS

4. Select **Current Alarms** from the application bar in Node Essentials.

The summary of the number of alarms displays on the top right of the screen.

You have completed the procedure.

Copyright© 2019-2025 Ciena® Corporation

Procedure 3 Retrieving alarm history

Use this procedure to show the alarm history. User with limited access can also perform this procedure.

Steps

1. Start a CLI or Node Essentials session. See “Accessing and logging in to a network element” in the *Licensing, Security, and Administration*, 323-2051-300.
2. Retrieve the historical alarm detail:

If you want to perform the procedure using	**Then** go to the
CLI commands	“CLI INTERFACE STEPS”
Node Essentials	“NODE ESSENTIALS STEPS”

CLI INTERFACE STEPS

3. Use this command to view alarm history:

```
show alarm-history [id]
```

4. Use this command to view the alarm history in tabular format:

```
show alarm-history --display table
```

Refer to “Alarm parameters” on page 27 for applicable parameters.

NODE ESSENTIALS STEPS

5. Select **Alarms > Historical alarms** from the Node Essentials navigation menu.

   The Historical alarms page displays the alarm history in the alarm grid.

6. Filter the alarm history by using the search option on the top left of the alarm grid.

   You have completed the procedure.

Copyright© 2019-2025 Ciena® Corporation

Procedure 4 RPC the data for add-notes and clear-notes object

Use this procedure to Remote Procedure Call (RPC) the data for the add-notes and clear-notes object and its children.

Steps

1. Start a CLI session. See “Accessing and logging in to a network element” procedure in the *Licensing Security, and Administration*, 323-2051-300.
2. RPC the data for the add-notes and clear-notes object:

If you want to perform the procedure using	**Then** go to the
CLI commands	“CLI INTERFACE STEPS”
Node Essentials	“NODE ESSENTIALS STEPS”

CLI INTERFACE STEPS

3. To RPC the data for the add-notes object, enter:

```
add-notes id <clear-note> user-notes <Value>
```

Refer to “Alarm parameters” on page 27 for applicable parameters.

4. To RPC the data for the clear-notes object and its children enter:

```
clear-notes id <Value>
```

Refer to “Alarm parameters” on page 27 for applicable parameters.

NODE ESSENTIALS STEPS

5. The active-alarm user-notes in Node Essentials is accessed by selecting the **User notes** icon on the top right of the alarm grid.

   A **Notes** window opens.

6. Type a user notes object in the **Notes** window and click save to add the notes. When you click user notes icon, if there is already notes for that alarm, it will show notes. You can click on **Clear** to clear the notes.

   Note: The user notes do not survive restarts, upgrades, or module replacement. An added note in the Node Essential is visible, however after a restart it is lost since a new alarm record raises and the original note associated with the first alarm record is lost.

Copyright© 2019-2025 Ciena® Corporation

Procedure 5 Restarting an interface module or the CTM

Requirements

To perform this procedure, you must use an account with at least an Admin user access level.

Overview

CAUTION
Risk of traffic loss
A cold restart on an unprotected module causes traffic loss. A cold restart on an active protected module causes a protection switch that impacts traffic.

As cold restarts can be traffic affecting, you must only perform a cold restart to restore functionality when all other trouble clearing procedures have been performed. Before performing a cold restart, if possible, change the admin state of the module to “Disabled” and unless it contains unprotected services, contact your next level of support or your Ciena support group for assistance.

Use this procedure to initialize an interface module in a warm or cold restart mode.

Use this procedure to initialize a CTM in a cold restart mode. CTM warm restarts are not supported in this release. If the user enters the CLI command to perform a warm restart on the CTM, the system will automatically switch to cold restart.

You can perform a “power-on restart” on a CTM in R4 or R8-300 shelves as follows:

```
restart resource “slots <SlotName>” restart-type <warm |
cold | power-on>
```

Consider the following:

- A loss of connectivity to the CTM occurs when you restart one or both CTMs. You must wait up to 10 minutes before logging back in.
- In duplex operation, if the Access Panel fails, the primary CTM restarts resulting in a switch-over.
- In duplex operation, CTM switchovers initiated via the “protection-switch” command are blocked
  - If the mate CTM has an admin state of disabled
  - If the mate CTM has a CP Failed alarm

Copyright© 2019-2025 Ciena® Corporation

- In duplex operation, CTM switchovers initiated via a CTM restart are not blocked
  - If the mate CTM has an admin state of disabled
  - If the mate CTM has a CP Failed alarm

  It is recommended to use the “protection switch” command instead of cold restarting the active CTM to perform a switch from active CTM.

  It is also recommended to clear any alarms on the inactive CTM before performing a switch from active CTM.
- After a CTM restart is performed on a remote network element (RNE), the first login attempt to the RNE will fail. An “Operation Failed” error message appears and you need to log back in a second time to establish the connection to the RNE.
- The power-on restart on the CTM has a target completion of five minutes. After a power-on restart the system can experience a DCN/CLI outage for approximately 10 minutes. In a simplex CTM system after a power-on restart the microservices need to be shut down, the CTM undergoes a graceful cold restart, then the CTM does a power-on restart.
- When CTM/IM is restarted, the restart event shows up under “Show alarm-history”.
- After a shelf power cycle, where all IMs and CTMs restart at the same time, there is a possibility that slot-mgr misses a restart notification. As a result, some restart complete events might be missing after a shelf power cycle.
- After a CTM restart is performed, an “OTDR File Transfer Failed” alarm can be raised. The alarm is raised with a delay, because the system retries the file transfer with increasing waiting times (for example; 1, 2, 5 minutes). When the file transfer fails 3 consecutive times, the “OTDR File Transfer Failed” alarm is raised.

Impact of module restart

A CTM restart results in a switch-over (Duplex CTM).

Impact on PM counts

For Photonic modules, current and previous bin PM statistics are stored on the CTM. Therefore, a restart of the CTM clears untimed, current and previous bin PM counts for Photonic modules provisioned on the shelf.

Steps

1 Select the network element in the navigation tree.

Copyright© 2019-2025 Ciena® Corporation

2

If you want to perform a	**Then** go to
cold restart on the module or CTM	step 3
warm restart on the module	step 9

3 Perform a cold restart on the module or CTM:

If you want to perform the procedure using	**Then** go to the
CLI commands	“CLI INTERFACE STEPS”
Node Essentials	“NODE ESSENTIALS STEPS”

CLI INTERFACE STEPS

4 Perform a cold restart on the module or CTM. Enter:

```
restart resource "slots <SlotNum>" restart-type <cold>
```

During a cold restart of the CTM module in place, the LEDs go through the following sequence:

- the module LED flashes
- the Green LED flashes
- the Green LED turns solid and if the CTM module is “Enabled”, the Blue LED turns on

5 Go to step 14.

NODE ESSENTIALS STEPS

6 Select **Facilities** from the Node Essentials navigation menu.

The Facilities menu opens.

7 From the **Equipment** grid, select the module you want to restart by row selector and click on the **Card restart** icon on the top. Choose **COLD** restart in the restart dialog that opens.

8 Go to step 14.

9 Perform a warm restart on the module:

If you want to perform the procedure using	**Then** go to the
CLI commands	“CLI INTERFACE STEPS”
Node Essentials	“NODE ESSENTIALS STEPS”

CLI INTERFACE STEPS

10 Perform a warm restart on the module you want to restart. Enter

```
restart resource "slots <SlotNum>" restart-type <warm>
```

11 Go to step 14.

NODE ESSENTIALS STEPS

12 Select **Facilities** from the Node Essentials navigation menu.

The Facilities menu opens.

Copyright© 2019-2025 Ciena® Corporation

13 From the **Equipment** grid, select the module you want to restart by row selector and click on the **Card restart** icon on the top. Choose **WARM** restart in the restart dialog that opens.

14 Change the equipment state of the module to “Enabled”. Refer to *Equipment/ Facility Provisioning and Protection*, 323-2051-310.

15 Change the facility states to “Enabled” for all facilities on the module. Refer to *Equipment/Facility Provisioning and Protection*, 323-2051-310.

Copyright© 2019-2025 Ciena® Corporation

Procedure 6 Locating a reflective event

Use this procedure to locate connector losses or a reflective event at a line amplifier site.

Requirements

To perform this procedure, you must:

- observe all safety requirements described in *6500 RLS Shelf Installation Guide,* 323-2051-201
- have a network diagram that identifies all connection points at the site of the alarmed module that can be cleaned
- have the appropriate personal grounding device to dissipate electrostatic charges
- have a mandrel or screwdriver

Overview

In this procedure you will attempt to isolate the connector losses by starting at the connector that is farthest from the alarmed amplifier and then working back towards the alarmed amplifier.

CAUTION
Risk of equipment damage
This procedure involves wrapping optical fiber around a mandrel to create optical power attenuations. Winding the fiber too tightly will damage optical fibers and the optical power attenuations can generate additional alarms on the system. Do not perform this action on the fiber connected to the LINE-IN port of a RAMMAN amplifier.

Steps

1

CAUTION
Risk of damage to module
Wear an antistatic wrist strap to protect the equipment from static damage.

Connect the wrist strap to the ESD jack on the shelf or module.

2 Review the network diagram, and locate the connector that is farthest from the alarmed amplifier within the site.

3 Wind the optical fiber patchcord that is attached to the connector, identified in step 2, four turns around a 15-mm mandrel. You can use a screwdriver handle or other similar sized cylinder in place of a mandrel.

Copyright© 2019-2025 Ciena® Corporation

This step checks for high reflection (low return loss) by causing attenuation of the optical power in the direction back towards the amplifier output.

4

If the original alarm	**Then**
does not clear, and there are more optical fiber patchcords before the alarmed amplifier	the reflective event is closer to the alarmed amplifier. Go to step 5.
does not clear, and there are no more optical fiber patchcords before the alarmed amplifier at this site (you are now at the output of the alarmed amplifier)	If you were sent from another procedure, return to the step in the procedure that referred you to this procedure. Otherwise, contact your next level of support or your Ciena support group.
clears	Go to step 6.

5 Locate the next farthest connector from the alarmed amplifier and go to the step 3.

6 Place the admin state of all facilities on the alarmed amplifier to “Disabled”. Refer to the *Equipment/Facility Provisioning and Protection*, 323-2051-310.

7

CAUTION
Risk of laser radiation exposure
Do not look directly into the optical beam. Invisible light can severely damage your eyes.

CAUTION
Risk of damage to module
Never disconnect an optical fiber that is connected to an active or powered up optical amplifier. To disconnect or reconnect an optical fiber, make sure the optical amplifier is “Disabled”, then disconnect or reconnect the fiber.

CAUTION
Risk of damage to module
Wear an antistatic wrist strap to protect the equipment from static damage. Connect the wrist strap to the ESD jack on the shelf or module.

Clean and then reconnect the output fibers and connectors at the amplifier. Refer to *Optical Connector Inspection and Cleaning*, 323-1859-500.

8 Change the admin state of the amplifier back to “Enabled”.

Copyright© 2019-2025 Ciena® Corporation

9

If the original alarm	**Then**
clears	the procedure is complete
does not clear	return to the step in the procedure that referred you to this procedure or contact your next level of support or your Ciena support group

Copyright© 2019-2025 Ciena® Corporation

Procedure 7 Tracing and clearing the OTDR high reflection

Use this procedure to trace and clear OTDR high reflection.

Requirements

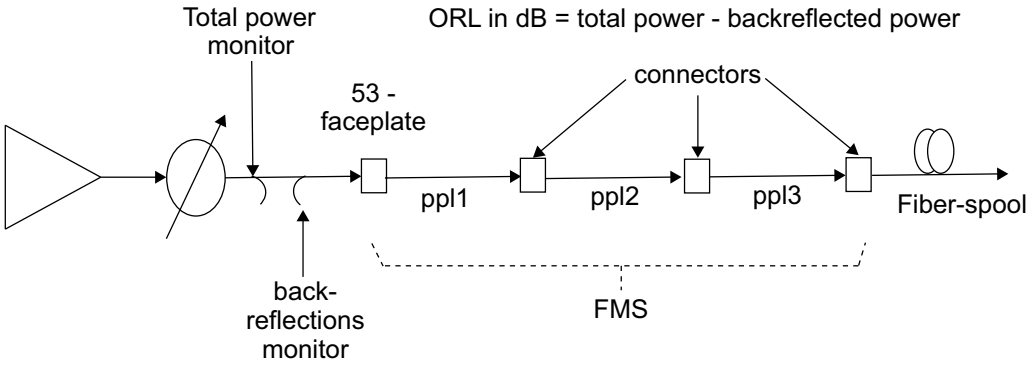
To perform this procedure, you must:

- observe all safety requirements described in *6500 RLS Shelf Installation Guide,* 323-2051-201
- have a network diagram that identifies all connection points at the site of the alarmed module that can be cleaned
- have the appropriate personal grounding device to dissipate electrostatic charges

Note: Before tracing ORL issues, make sure 0dBm <= amp out-current-power <= 10dBm.

See Figure 3, “Tracing ORL Example” for an example of tracing ORL.

Figure 3 Tracing ORL Example



Legend

1	Total power monitor	5	backreflections monitor
2	ORL in dB = total power - backreflected power	6	FMS
3	53-faceplate	7	Fiber-spool
4	connectors		

Copyright© 2019-2025 Ciena® Corporation

CAUTION
Risk of equipment damage
This procedure involves wrapping optical fiber around a mandrel to create optical power attenuations. Winding the fiber too tightly will damage optical fibers and the optical power attenuations can generate additional alarms on the system.

CAUTION
Risk of laser radiation exposure
Do not look directly into the optical beam. Invisible light can severely damage your eyes.

CAUTION
Risk of damage to module
Never disconnect an optical fiber that is connected to an active or powered up optical amplifier. To disconnect or reconnect an optical fiber, make sure the optical amplifier is “Disabled”, then disconnect or reconnect the fiber.

CAUTION
Risk of equipment damage
Electrostatic discharge (ESD) can damage electrostatic sensitive devices. You must use antistatic protection while unpacking and installing all Field-Replaceable Units (FRU) and cables.

Overview

In this procedure you will attempt to locate and clear the optical return losses by bending or creating small loops on the fiber to locate the ORL. Review the following figures. If there is a Raman card (SRA) present, tracking ORL techniques are similar, where ORL tracing is done patch by patch.

Copyright© 2019-2025 Ciena® Corporation

Figure 4 Tracing ORL from faceplate connector

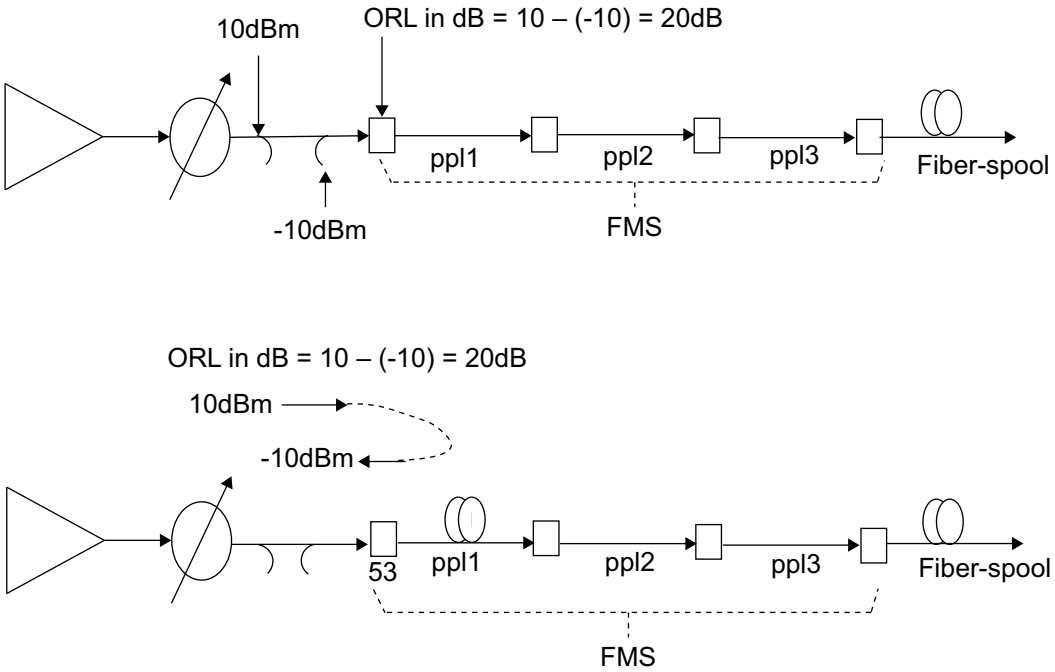
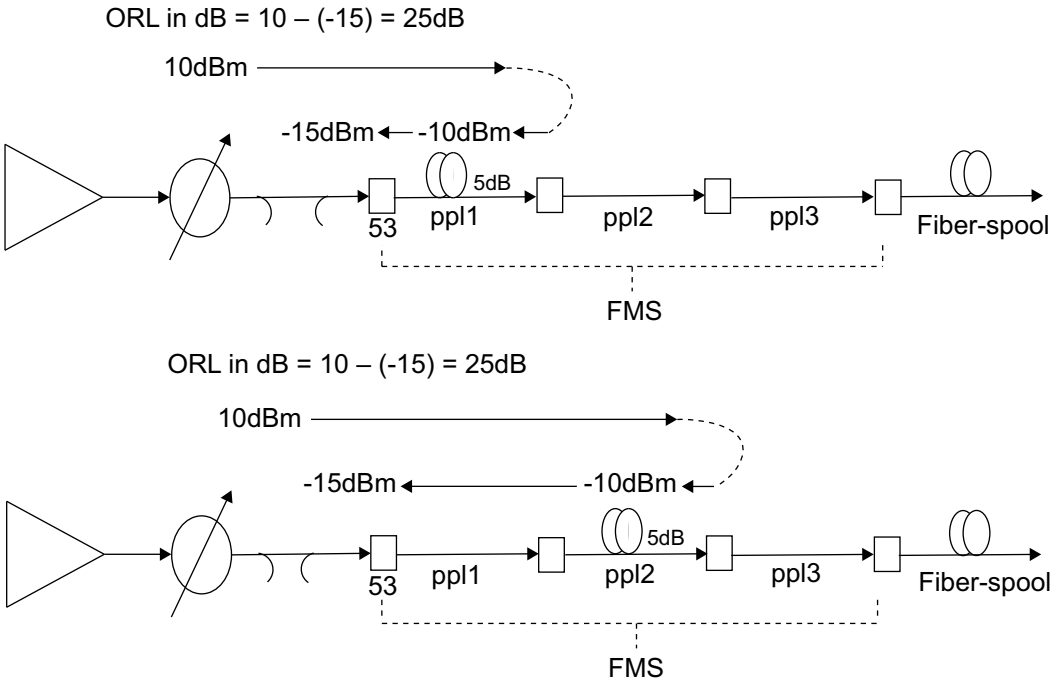


Figure 5 Tracing ORL from downstream patch panel connector



Copyright© 2019-2025 Ciena® Corporation

Figure 6 Tracing ORL Issues with Raman in Place

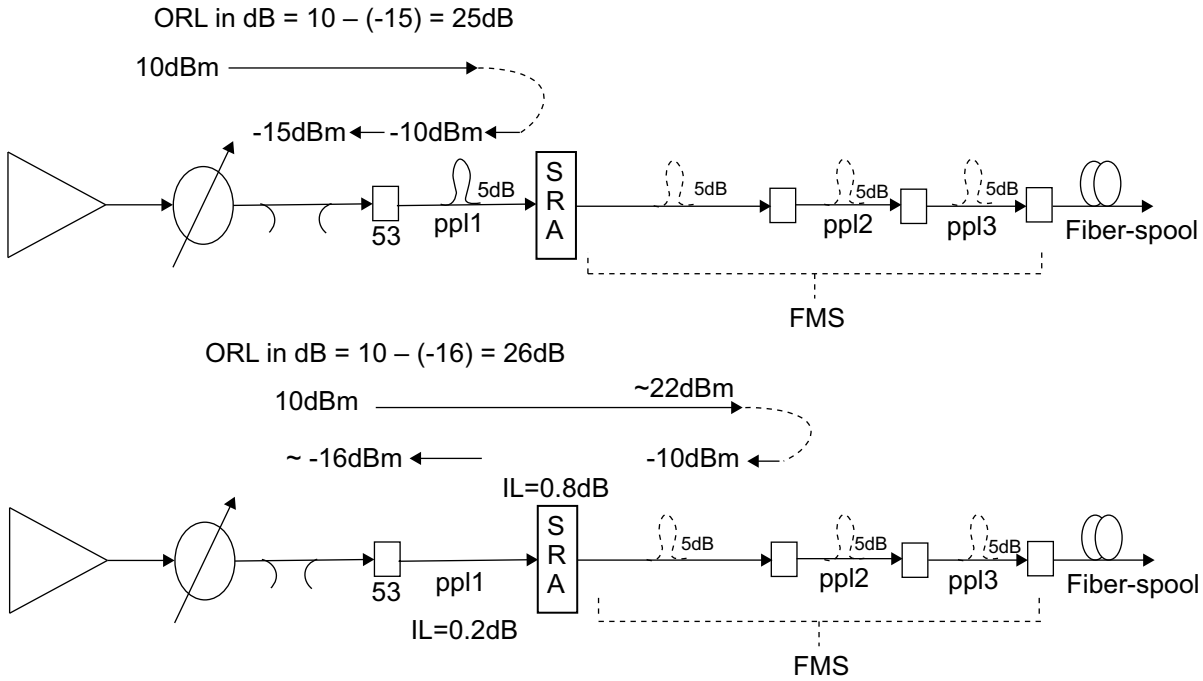
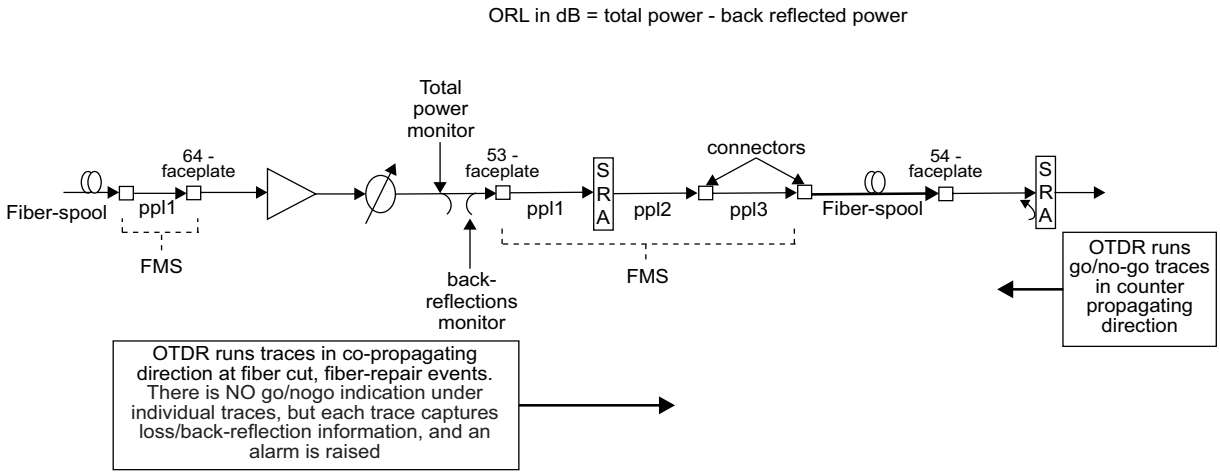


Figure 7 ORL Detection vs OTDR Traces



The admin state of the OTDR facility can be enabled or disabled by the user. Refer to “provisioning OTDR facilities” in *Optical Control, SPLI, and OTDR*, 323-2051-318 for more information.

- enabled (default): allows OTDR trace to be run on the specified OTDR facility.

Copyright© 2019-2025 Ciena® Corporation

- disabled: prevents OTDR trace from running on the specified OTDR facility.

  Note 1: Typically an OTDR facility remains at the default setting (enabled); however, for cases where the user does not want the OTDR trace to run, Ciena recommends the user provision the admin-state to disabled instead of deleting the OTDR facility.

  Note 2: Supported for RLS Release 2.6 and later. Applies to greenfield deployments and brownfield upgrade to RLS Release 2.6. No user intervention is required after upgrade.

  Note 3: Previously, it was required/recommended to delete an OTDR facility to disable it. This is no longer required/recommended.

Steps

1. Connect the wrist strap to the ESD jack on the shelf or module.
2. Review the network diagram, and locate the connector at the first fiber-patch of the alarmed amplifier.
3. Create a small bend or loop at the first fiber-patch by winding the optical fiber patchcord that is attached to the connector, identified in step 2, four turns around a 15-mm mandrel. You can use a screwdriver handle or other similar sized cylinder in place of a mandrel.
4.

If the ORL value	**Then**
remains unchanged	it means, the reflection is primarily happening on the faceplate connector. See Figure 4, “Tracing ORL from faceplate connector”. Go to step 5.
increases	it means, the reflection is coming from a downstream patch panel connector. See Figure 5, “Tracing ORL from downstream patch panel connector”. Go to step 8.

5. Clean the fiber connectors, or replace the patch fiber. Refer to *Optical Connector Inspection and Cleaning*, 323-1859-500.
6. Reconnect the fiber, re-run the OTDR traces and measure ORL again without having any extra bend.
7. Repeat the above steps until the ORL > 25dB. You have completed this procedure.
8. Clear the fiber-bend, and create a new one on the next patch fiber.
9.

If the ORL value	**Then**
increases	it means, the reflection is coming from a further downstream patch panel connector. Go to step 10.
remains unchanged	Go to step 11.

Copyright© 2019-2025 Ciena® Corporation

10 Continue the process until a patch panel is found where extra bend does not make noticeable change to the reflected power. For example, ORL value remains unchanged.

11 Clean up the fiber connectors, or replace the patch fiber.

12 Reconnect the fiber and measure ORL again without having any extra bend.

13 Repeat the above steps until the ORL >= 25 dB. When the ORL >= 25 dB, you have completed this procedure.

Copyright© 2019-2025 Ciena® Corporation

Procedure 8 Amplifier in Clamped State

Requirements

To perform this procedure, you must use an account with at least an Admin user access level.

Probable cause

This alarm is raised for all RLS modules with gain-clamp capable EDFA when delta between the target-gain and the measured-gain is greater than 1dB. This is because the input power to the amplifier is higher than expected.

The alarm is raised on CCMD8x24, CCMD16 modules if the channel input powers are too high.

The alarm is raised on RLA booster amplifiers if the channel powers are coming in too high from upstream.

The alarm is raised on DLE CLS bypass line-amplifiers and RLA/LRU pre-amplifiers in submarine networks if the span loss has improved (including fiber cleaning operations during circuit pack replacements).

The alarm is raised on DLE/DLA line-amplifiers and RLA/LRU pre-amplifiers in terrestrial networks if there is a significant improvement in span loss causing the amplifier to reach minimum-gain.

The alarm hold-off for this alarm is 150 seconds.

Impact

Major, non-service-affecting (M, NSA)

Steps

Alarm raised on CCMD16/CCMD8x24

1. Clear any “Optical Power Degrade Low/High” or “Optical Power Out of Range Low/High” alarms on channel-in ports of the card raising the “Amplifier in Clamped State” alarm. If the alarm is not clear, proceed to next step.
2. Verify the inventory OPTMONs facility of each channel-in port that currently has a channel added to ensure the added channels are not coming into the card with high power. If the current-power is >0.5dB, take corrective action to lower the modem Tx power.

Copyright© 2019-2025 Ciena® Corporation

a. to get the expected input power, first get the tx-proxy total-target-tx-power for the port and then subtract the expected-physical-loss from the link (if any) between transponder and CCMD ch-in port

- show slots <slot> config tx-proxy <ch-in port) total-target-tx-power

- show link <link name> expected-physical-loss

- link whose "to" port is the CCMD channel-in port being verified

- if there is no link provisioned, expected-physical-loss is 0

b. to get the measured input power;

- show slots <slot> inventory optmons <ch-in port> current-power low-pwr-threshold

If the alarm is not clear, proceed to next step.

3 Verify that the ports without added channels don't have any unexpected incident power by verifying the inventory OPTMON current-power is below the low-pwr-threshold. If the current-power is not below the low-pwr-threshold, take corrective action to remove the unexpected power. If not cleared proceed to next step (Note that this step does not apply to CCMD8x24).

```
show slots <slot> inventory optmons <ch-in port> current-
power low-pwr-threshold
```

4 If the alarm does not clear, contact your next level of support or your Ciena support group.

Alarm raised on RLA Booster Amp

5 If the channels are coming in with high power from upstream, verify ccs-instance channel-controller's channel input powers are not too high for the ccs-instance associated with clamped booster amp

*show ccs-instance <ccs> channel-controller * channel-power input*

if measured-power is >0.5dB above the expected-power troubleshoot and correct for the unexpected higher power

Alarm raised on RLA/LRU pre-amp or at DLA/DLE line-amp

6 If the amplifier raising the alarm is at the end of a submarine link:

a. there is no active span-loss control for a submarine link, if the clamped amp is not at min-gain for its provisioned gain-range (high/low), then lower the target-gain to meet the measured gain. To do so, edit both target-gain and baseline-target-gain to achieve the measured-gain.

b. check if the amp is at the minimum gain or not:

show slots <slot> config amps <amp> gain-mode target-gain target-gain-ranges

c. if amp is at minimum gain, contact Ciena

d. if not at minimum gain, get the measured gain from the amp

show slots <slot> inventory amps <amp> gain

Copyright© 2019-2025 Ciena® Corporation

e. set the target-gain and baseline-target-gain to the measured-gain value to remove the clamp condition

set slots <slots> config amps <amp> target-gain <measured-gain value> baseline-target-gain <measured-gain value>

7 If the amplifier raising the alarm is at the end of a terrestrial span:

a. if the clamped amp target-gain is at minimum-gain for its provisioned gain-range (high/low), then a large pinch may have been released since previous calibration.

show slots <slot> config amps <amp> gain-mode target-gain target-gain-ranges

b. if the amp is at minimum-gain, compare the logical-line-fiber measured with the baseline loss for the preceding link to verify the span loss has changed since last calibration.

- if the current measured-loss is the intended operating point for the span, a full section calibration should be run during the next maintenance window to operate the section at the new setpoint. A re-calibration is required because there has been a significant change in physical condition since last calibration.

- if the current measured-loss is not the intended operating point (for example, an external loss element is supposed to be on the line but has been removed mistakenly), take corrective action to restore the span to the previous baseline setpoint.

c. If the amp is not at minimum-gain, verify the span compensation is enabled:

- on preceding line-fiber link, verify pinch-compensation is enabled. If it is not enabled, set it to enabled.

- on local device-controller, verify amp and voa device-controllers are running (admin-state = true). If admin-state is not true, set it to true.

8 If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 9 ASE Mode Active

Requirements

To perform this procedure, you must use an account with at least an Admin user access level.

Probable cause

This alarm is raised when the ASE mode is active on the amplifier. The “ASE” mode can be set to active during the installation to check line out fiber connectivity and APR / ORL detection. The “ASE” mode must be changed back to “gain/gainclamp” mode. Otherwise device controller will change it at calibration time. The ASE alarm is raised when the amp is operating in one of these ASE modes:

- ASE Enable Constant Output Power
- ASE Enable Constant Drive Current
- ASE Safe

Impact

Minor, non-service-affecting (m, NSA)

Steps

1. Set back the AMP to gainclamp mode for regular operation. Enter the following CLI command:

   ```
   set slots <x> amps Booster-Cband mode gainclamp
   ```

   Note: There is no Node Essential equivalent command for this release.

2. If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 10 ASE Replacement Active

Requirements

To perform this procedure, you must use an account with at least an Admin user access level.

Probable cause

This alarm is raised when a fault causes the traffic to switch to the Amplified Spontaneous Emission (ASE) mode.

The alarm is raised when one or multiple channels of a section-mux CCS instance are replaced with local ASE source where the “operational-state” is set to “ase” for the faulted channel(s).

The “ASE Replacement Active” alarm is not masked by any local or upstream alarm.

> ***Note:*** When you replace a module or insert a new module in an RLS shelf, an auto-software upgrade occurs for the specific module. In these cases, the auto-software upgrade raises “ASE Replacement Active” alarm and causes a cold restart, which is traffic-affecting.

Examples to help diagnose the fault

Use the following examples to filter the channels to help diagnose and clear the faults.

Copyright© 2019-2025 Ciena® Corporation

Figure 8 Showing the operational state

```
SITE-1201# show ccs-instance SECTION-MUX-PFG-1 channel-controller * operational-state
ccs-instance  channel-controller
+-------------------------------------+
| center-frequency | operational-state |
+-------------------------------------+
| 191350.000       | in-service        |
| 191587.500       | in-service        |
| 191662.500       | in-service        |
| 191737.500       | in-service        |
| 191812.500       | in-service        |
| 191887.500       | in-service        |
| 191962.500       | in-service        |
| 192037.500       | in-service        |
| 192112.500       | in-service        |
| 192187.500       | in-service        |
| 192262.500       | in-service        |
| 192337.500       | in-service        |
| 192412.500       | in-service        |
| 195112.500       | in-service        |
| 195187.500       | ase               |
| 195262.500       | in-service        |
| 195337.500       | in-service        |
| 195412.500       | in-service        |
```

Use grep ase command to filter the particular instances.

Figure 9 grep ase CLI command

```
SITE-1201# show ccs-instance SECTION-MUX-PFG-1 channel-controller * operational-state | grep ase
| 195187.500       | ase               |
| 195487.500       | ase               |
| 195562.500       | ase               |
| 195637.500       | ase               |
| 195712.500       | ase               |
| 195787.500       | ase               |
```

Impact

Warning, service-affecting (W, SA)

Steps

1. Verify upstream for faults on that channel or on the entire band (for example, LOS for single channel, OLF for all channels).
2. Ensure that none of the channels of a section-mux CCS instance have “operational-state” set to “ase”.
3. If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 11 Automatic Power Reduction Active

Requirements

To perform this procedure, you must:

- use an account with at least an Admin user access level.
- observe all safety requirements described in the “Observing product and personnel safety guidelines” section in *6500 RLS Shelf* Installation Guide, 323-2051-201
- have the Engineering Documentation Package (EDP)
- have a fiber cleaning kit
- have a replacement module

Probable cause

The APR alarm is raised against an AMP facility. The APR condition is caused by a reflection somewhere downstream from the AMP facility. This reflection can be caused by:

- dirty optical connectors
- improper optical cable mating
- a disconnected optical fiber at the amplifier output
- an optical fiber cut
- a degraded optical fiber
- a disconnected or missing termination

When the ORL reading is not valid because the power into the backward reflective monitor tap is too low and cannot be measured accurately, the ORL PM reading(s) report “OOR”. The true ORL reading(s) cannot be determined in this case.

Note 1: This alarm indicates a condition on the output port of an amplifier; however, the alarm is raised against the input port of the corresponding DLM or TLM module. Therefore, ensure you troubleshoot the appropriate port.

Note 2: This alarm can be raised on CCMD16 module after commissioning since there is no power in the opposite direction. The alarm is raised for safety reasons. Once a channel is added, the alarm will clear. In this case there is no action to be taken before the first capacity change.

This alarm is also raised against the CCMD8x24 when the Demux OPTMON has no power, which indicates there is no physical fiber connected between the CCMD and RLA.

Copyright© 2019-2025 Ciena® Corporation

This alarm is raised momentary on a CCMD Mux amplifier during a channel delete or restoration event. For this case no further action is required.

ATTENTION

The MuxAmp configuration disables the Automatic Power Reduction (APR) function. Certain C-band amplifier modules used in a MuxAmp configuration with one or more wavelengths in the IEC 60825-1 Class 1M range may have a Class 1 Hazard level label but should have a Class 1M Hazard Level label because APR is disabled.

Modules that were originally manufactured with a Hazard Level 1 warning label can be re-labeled with the Level 1M label kit (part number 415-2818-001).

For more information and the procedure to apply the Level 1M label on these modules, see the section on observing product and personnel safety guidelines in *6500 RLS Shelf Installation Guide*, 323-2051-201.

Impact

Major

Steps

1

If this alarm	**Then**
was raised as a result of maintenance or SLAT that has not been completed	no action is required. The alarm clears when the maintenance activity or Commissioning is completed. The procedure is complete.
is unexpected	go to step 2

2 Confirm that the amplifier's provisioning matches what is defined in the EDP. Refer to the *Equipment/Facility Provisioning and Protection*, 323-2051-310. Edit the power level values as required.

3

If the original alarm has	**Then**
cleared	the procedure is complete
not cleared	go to step 4

4 If the APR alarm is raised on the CCMD8x24 Mux AMP, verify the corresponding Demux OPTMON for the same degree as the Mux AMP. If the Demux OPTMON is in an LOS state, the APR alarm is raised on the Mux AMP. Trace the power or physical fiber connection in the drop direction to determine the cause of the Demux OPTMON LOS condition.

5 Ensure that all LC connectors located after the amplifier output are properly mated. Verify this on both ends of the connector-mating receptacles.

Copyright© 2019-2025 Ciena® Corporation

6

If the original alarm has	**Then**
cleared	the procedure is complete
not cleared	go to step 7

7 Ensure that the termination plugs are present and are mated properly on unused ports.

8

If the original alarm has	**Then**
cleared	the procedure is complete
not cleared	go to step 9

9

CAUTION
Risk of laser radiation exposure
Do not look directly into the optical beam. Invisible light can severely damage your eyes.

CAUTION
Risk of damage to modules
Never disconnect an optical fiber that is connected to an active or powered up optical amplifier. To disconnect or reconnect an optical fiber, make sure the optical amplifier is “Disabled”, then disconnect or reconnect the fiber.

CAUTION
Risk of damage to modules
Wear an antistatic wrist strap to protect the equipment from static damage. Connect the wrist strap to the ESD jack on the shelf or module.

10 Place the alarmed AMP facility to “Disabled”:

If you want to perform the procedure using	**Then** go to the
CLI commands	“CLI INTERFACE STEPS”
Node Essentials	“NODE ESSENTIALS STEPS”

CLI INTERFACE STEPS

11 To place the alarmed AMP facility to “Disabled”. Enter the following command:

```
set slots <name> config amps <name> [admin-state
<Disabled>]
```

12 Go to step 20.

NODE ESSENTIALS STEPS

13 Select **Facilities** from the Node Essentials navigation menu.

The Facilities menu opens.

Copyright© 2019-2025 Ciena® Corporation

14 From the **Equipment** grid, select the module with the alarmed AMP facility.

The bottom part of screen becomes populated.

15 Select AMP facility from Facility navigator.

The AMP Facilities grid opens.

16 Select the alarmed AMP facility by Row selector from the AMP Facilities grid.

17 Click the **Pencil** icon.

The related Edit AMP dialog opens.

18 Edit the Admin state of the AMP facility to Disabled.

19 Click **Confirm**.

20

> **CAUTION**
> **Risk of traffic loss**
> Only disconnect the output fiber of the alarmed optical amplifier. It is not necessary to disconnect any other output fibers, which could affect service. Disconnecting the output fiber will impact traffic in both directions, as this triggers Automatic Line Shut Off (ALSO).

Disconnect the output fiber of the alarmed optical amplifier, clean the output fiber and connectors at the amplifier, then reconnect the fiber.

21 Place the AMP facility back to “Enabled”.

22

If the original alarm has	**Then**
cleared	the procedure is complete
not cleared	go to step 23

23 You may have to clean a specific connector or connectors that may not be immediately connected to the alarmed amplifier output. For information on isolating connector losses, complete Procedure 6, “Locating a reflective event”.

24 If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 12 Automatic Shutoff

Requirements

To perform this procedure, you must use an account with at least an Admin user access level.

Probable cause

This alarm is raised against an AMP facility when an ALSO condition is triggered, and is raised against any amplifier that has been shut off. An ALSO condition is cleared when the OSC receives a clean signal.

For DLE modules this alarm is raised against a DGFF amp facility.

> ***Note:*** This alarm indicates a condition on the output port of an amplifier; however, the alarm is raised against the input port of the corresponding DLM or TLM module. Therefore, ensure you troubleshoot the appropriate port.

CAUTION

Risk of radiation exposure

If light is used to test the broken fiber (for example, with a light source or an OTDR), certain Automatic Line Shut Off (ALSO) and Input loss of signal alarms can clear. When the shelf detects light, the alarms clear and the amplifier facility is powered up. This is an expected behavior because a shelf cannot distinguish between a light source from an optical test set and a light source from a shelf. Ensure the adjacent optical amplifiers are “Disabled” when performing fiber repairs.

Impact

Major, service-affecting (M, SA)

Steps

1. Complete the “Optical Line Failed” on page 179 alarm clearing procedure.
2. If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 13 Automatic Shutoff Compromised

Requirements

To perform this procedure, you must:

- observe all safety requirements described in the “Observing product and personnel safety guidelines” section in *6500 RLS Shelf* Installation Guide, 323-2051-201
- have the Engineering Documentation Package (EDP)
- have a fiber cleaning kit

Probable cause

This alarm is raised when the Rx/Tx fibers of the OSC on a DLM, TLM, DLE, TLE, DLA, or RLA module are crossed at one or both ends of a Photonic span.

The alarm is also raised when the Tx power on the SFP is below the threshold, the OSC tx to OSC In fiber is pinched, defective or has a dirty connector, or if the OSC transmitter is disabled.

Note: When this alarm is active, the Automatic Line Shutoff (ALSO) feature is disabled.

CAUTION

Risk of laser radiation exposure

During this procedure the fiber plant does not have to be disrupted and the system remains a Class 1(IEC)/Class I (FDA) product.

If the fiber downstream of the OSC becomes disconnected accidentally while the “Automatic Shutoff Disabled” alarm is active, the radiation at the exposed fiber can be at hazard level 1M (IEC 60825-2). In this situation, you must take all safety precautions appropriate to hazard level 1M (IEC 60825-2). The ORL-based APR safety mechanism remains active.

Impact

Major, non-service-affecting (M, NSA)

Steps

1. Ensure that the OSC fibers are correctly connected at both ends of their spans.
2. If the alarm does not clear, ensure that the transmitter is enabled. Check for and clean any dirty fibers. Refer to *Optical Connector Inspection and Cleaning*, 323-1859-500.

Copyright© 2019-2025 Ciena® Corporation

3 If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 14 Automatic Shutoff Disabled

Requirements

To perform this procedure, you must use an account with at least an Admin user access level.

Probable cause

This alarm is raised on an AMP facility when you set the ALSO Disabled parameter to True for the AMP facility. The AMP facility is placed in this mode for certain maintenance actions such as:

- recovering from ALSO in certain configurations
- checking for ORL at SLAT time
- nodal continuity testing

CAUTION

Risk of laser radiation exposure

During this procedure the fiber plant does not have to be disrupted and the system remains a Class 1(IEC)/Class I (FDA) product.

If the fiber downstream from the AMP Line A output connector becomes disconnected accidentally while the “Automatic Shutoff Disabled” alarm is active, the radiation at the exposed fiber can be at hazard level 1M (IEC 60825-2). In this situation, you must take all safety precautions appropriate to hazard level 1M (IEC 60825-2). The ORL-based APR safety mechanism remains active.

Impact

Major, service-affecting (M, SA)

Steps

1. Make sure that the maintenance work is complete.
2. Ensure there is proper OSC established across the line. When there is proper OSC is established, the system recovers and the alarm clears.
3. Immediately after the maintenance work is complete, enable Auto Shutoff. Refer to the *Equipment/Facility Provisioning and Protection*, 323-2051-310.
4. Select the AMP facilities. Set the ALSO Disabled parameter to False for the AMP facility.

   This action clears the Automatic Shutoff Disabled alarm.
5. Provision the Shutoff Threshold to be above -60 dBm. Refer to “Provisioning AMP facilities” procedure in the *Equipment/Facility Provisioning and Protection*, 323-2051-310.

Copyright© 2019-2025 Ciena® Corporation

6 If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 15 Autoprovisioning Mismatch

Requirements

To perform this procedure, you must:

- observe all safety requirements described in the “Observing product and personnel safety guidelines” section in *6500 RLS Shelf Installation Guide*, 323-2051-201
- if necessary, obtain a replacement module or a filler card

Probable cause

This alarm is raised when a module is installed in an unprovisioned slot that does not support that module. There is no effect on shelf operations.

When auto equipping is disabled, this alarm is not raised if you install a module in an unprovisioned slot that does not support that module.

CAUTION
Risk of damage to module
Wear an antistatic wrist strap to protect the equipment from static damage. Connect the wrist strap to the ESD jack on the shelf or module.

Impact

Minor, non-service-affecting (m, NSA)

Steps

1 Identify the module raising the alarm:

If you want to perform the procedure using	**Then** go to
CLI commands	step 2
Node Essentials	See the Node Essential steps in “Retrieving the data for the active alarm object” on page 32. Then go to step 3.

2 To identify the module raising the alarm using CLI commands, enter:

```
show active-alarm [id] [name] resource raise-time [clear-time] cause [condition-type] [direction] [location] severity service-impact [additional-info] [user-notes...]
```

Refer to “Alarm parameters” on page 27 for applicable parameters.

3 Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.

Copyright© 2019-2025 Ciena® Corporation

4

If	**Then** go to
the module in the alarmed slot is a spare module you want to store in that slot	step 5
otherwise	step 7

5 Disable auto equipping for the alarmed slot.

6 Reseat the module in the same slot. Refer to Procedure 138, “Reseating a module” in “Module replacement” section in this document. Go to step 8.

7 Remove the module in the alarmed slot and replace it with a module that is supported in the slot, a module of the correct equipment type, or a filler card. Refer to the “Module replacement” procedures in this document.

8 If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 16 Bad Ethernet Connection or Port Failure

Requirements

To perform this procedure, you must:

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *6500 RLS Shelf Installation Guide*, 323-2051-201
- have an antistatic wrist strap to dissipate electrostatic charges
- have the fiber connection information (that is, how the optical modules on each network element connect to other network elements)
- use an account with at least a level 3 UPC

Probable cause

This alarm is raised when a cable or fiber is disconnected from the port or a fault on the interface is detected.

Impact

Minor, non-service-affecting (m, NSA)

Steps

1. Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
2. Ensure that cables or fibers between the subtending equipment and the COLAN, ILAN, ILAN1 or WSC ports are properly connected and are not damaged.
3. Ensure that the subtending client equipment is correctly provisioned, functioning, and transmitting a valid signal.
4. If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 17 BGP Peer Loss

Requirements

To perform this procedure, you must use an account with at least an Admin user access level.

Probable cause

This alarm is raised when the Border Gateway Protocol (BGP) peer is provisioned and the TCP session with the BGP peer cannot be established.

Impact

Major, Service affecting (M, SA)

Steps

1. Ensure the TCP session between the BGP peer is established.
2. If the alarm does not clear and you want to remove the BGP to clear the alarm, then delete the BGP Peer using the following command:

   ```
   > delete network-instances network-instance network-
   instance <string> protocols protocol BGP,<string>
   bgpneighbors neighbor <IP address>
   ```

   Note: There is no Node Essentials equivalent command for this release.
3. If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 18 Boot Fail Fault

Requirements

To perform this procedure, you must use an account with at least an Admin user access level.

Probable cause

This alarm is raised when the when a module has a software failure that cannot be recovered on its own or when a module fails to boot up after few attempts.

Impact

Major, non-service-affecting (M, NSA)

Steps

1. Perform a warm restart on the module that is raising the alarm. Refer to the Procedure 5, “Restarting an interface module or the CTM” section of this document.
2. **CAUTION**
   Risk of traffic loss
   A cold restart on an unprotected module causes a traffic loss. A cold restart on an active protected module causes a protection switch that impacts traffic.

   If the alarm does not clear, perform a cold restart on the alarmed module. Refer to Procedure 5, “Restarting an interface module or the CTM” in this document.
3. If the alarm does not clear, reseat the module. Refer to Procedure 138, “Reseating a module” in “Module replacement” section in this document.
4. If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 19 Call Record/s Mismatch

Requirements

To perform this procedure, you must use an account with at least an Admin user access level.

Probable cause

This alarm is raised when call records mismatch is identified on a remote node of the OSRPLINE or when a loopback is detected on an AMP between 2 peer ROADM sites.

Impact

Major, non-service-affecting (M, NSA)

Steps

1. If the alarm is raised due to Loopback detected on an AMP between 2 peer ROADM sites, the alarm will be cleared once loopback clears.
2. Identify the node that raised the alarm.

   ```
   show active-alarm <id> [name] [resource] [raise-time]
   [raise-time] [cause] [condition-type] [direction]
   [location] [severity] [service-impact] [additional-info]
   [user-notes...]
   ```
3. On the alarmed node, retrieve the OSRP Lines and select the OSRP Line on which the alarm is raised. Refer to “Displaying OSRP network topology” procedure in *6500 RLS Equipment/Facility Provisioning and Protection*, 323-2051-310.
4. Edit the OSRP Line and change “PSNC Mismatch Action” from “Keep” to “Release”. Refer to “Provisioning an OSRP line” procedure in *6500 RLS Equipment/Facility Provisioning and Protection*, 323-2051-310.
5. Once the alarm clears, change the “PSNC Mismatch Action” from “Release” back to “Keep”.
6. If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 20 Capacity Change Inhibited

Requirements

To perform this procedure, you must log into the CLI of the nodes with admin or higher privilege level. For login information, See “Accessing and logging in to a network element” in *Licensing, Security, and Administration*, 323-2051-300.

Probable cause

This alarm is raised when the channel controller is disabled blocking the subsequent capacity changes. While the section-calibration is in progress, the channel-controller instances are blocked for the capacity changes until the section is fully calibrated.

This alarm is raised when:

- The ccs-instance mode is set by the system to a value other than “traffic-with-ase” or “traffic-without-ase”, after calibration or recalibration.
- The ccs-instance mode is set by a user to a value other than “traffic-with-ase” or “traffic-without-ase”.

The alarm clears when the ccs-instance mode is set by the system or user to “traffic-with-ase” or “traffic-without-ase”.

The alarm is not raised during the calibration or recalibration, where it is expected that the ccs-instance mode may change, or until a first successful calibration.

Impact

Warning, non-service-affecting (W,NSA)

Steps

1 If the ccs-instance corresponds to a functional group of type Section Demux, Channel Mux, or Channel Demux, set the ccs-instance mode to “traffic-without-ase” as follows.

```
set ccs-instance <ccs_instance_name> config mode traffic-without-ase
```

Note: There is no Node Essentials equivalent command for this release.

2 If the ccs-instance corresponds to a functional group of type Section Mux, the ccs-instance mode would typically be traffic-with-ase (unless set otherwise by user). As such, set the ccs-instance mode to “traffic-with-ase” as follows.

```
set ccs-instance <ccs_instance_name> config mode traffic-with-ase
```

Note: There is no Node Essentials equivalent command for this release.

Copyright© 2019-2025 Ciena® Corporation

3 If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 21 Capacity Change Pending

Requirements

To perform this procedure, you must log into the CLI of the nodes with admin or higher privilege level. For login information, See “Accessing and logging in to a network element” in *Licensing, Security, and Administration*, 323-2051-300.

Probable cause

This warning is raised when channels are added and the indicating condition are preventing the channel to be added successfully. This warning is raised if channel stays in Wait For Power (WFP) state for longer than 15 min.

Since “Capacity Change Pending” diagnostic is raised on a per channel controller basis, the alarm masking is as a per channel level for the same channel along the channel path.

> ***Note:*** In case of active CTM switchover, this alarm re-appears after 15 min, because WFP channel condition has to persist for at least 15 min on the controller.

Impact

Warning, non-service-affecting (W, NSA)

Steps

1 Verify the operational-state. If it is “waiting for Power”, that means scaled power data is not available to Channel Controller (CCS) or the scaled measured power is below the add-threshold-offset. Review the Controller’s additional info for more information.

2 Verify if expected-power is available for both input and output. Enter:

```
show ccs-instance <PFG> channel-controller <center-freq>
```

Note: There is no Node Essentials equivalent command for this release.

If the expected-power is	**Then**
available	Power Profile provisioning is good and the scaled power profile data is available to CCS.
not available	go to step 3

3 Verify the power profile provisioning first on the switch ports, and line out for section-mux location, or OCM baseline for pre-amp out and switch out ports for section-demux or channel-mux/demux locations. Enter:

```
show slots # config pwr-profile <profile-name>
```

Note: There is no Node Essentials equivalent command for this release.

4 Verify if measured-power is available for both input and output.

Copyright© 2019-2025 Ciena® Corporation

5 If not available at input, trace the power data optically first.

6 If locally added from CCMD, trace power from Channel Mux Tx port to all the way up to RLA Mux switch in port. Enter:

```
get-port-trail-power port "slots # config port #" center-frequency <center-freq>
```

Note: There is no Node Essentials equivalent command for this release.

7 Ensure channel power at Tx port meeting the target as expected.

8 Use get-channel-data rpc for the CCMD MC BW (start and stop frequency) to ensure all pixels are set correctly on the CCMD8x24.

a. Start and stop frequency of mc or nmc can be found from mc/nmc provisioning.

b. From get-channel-data rpc , confirm config vs inventory lines up.

c. If config vs inventory does not line up, then call Ciena Support for further instruction on clean-up the issue.

9 Ensure the CCMD8x24 mux AMP is not in the Shutoff state. Note, an APR condition for channel Mux AMP in RLS is normal in dark conditions.

10 Verify the CCMD common-out power matches RLA Mux Switch Input, or the delta between their power is reflected properly on link fiber loss.

11 If channels are added from an express demux location,

a. Check if any fiber break detected alarm present for the demux to mux degree fiber link. If present, that needs to be fixed first.

b. If channel is indicating operational-state="waiting-for-power" and additional-info="Loss of signal detected", then the total power must be checked at upstream demux switch out port if that is clearing the low-optical-power threshold for the given OPTMON facility. If not, then the LOP threshold must be manually adjusted to a lower value to proceed with a channel add action.

See example in "Channel add troubleshooting, capacity change pending in "Overview" section of *6500 RLS Optical Control, SPLI, and OTDR*, 323-2051-318.

12 If not, ensure the channel is in-service at upstream section-demux. and pwr-profiles are setup correctly.

13 Ensure channel power is visible at section-demux switch-out location under nmcmon-<switchoutPort>. Check RLA demux wss settings using get-channel-data rpc.

14 If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 22 Certificate Expired

Requirements

To perform this procedure, you must use an account with an at least a Super user access level.

Probable cause

This alarm is raised when a TLS validation certificate has expired.

Impact

Major, non-service-affecting (M, NSA)

Steps

1. Upload a new TLS validation certificate to the RLS shelf. Refer to “Uploading a TLS validation certificate” procedure in *Licensing, Security, and Administration*, 323-2051-300.

Copyright© 2019-2025 Ciena® Corporation

Procedure 23 Certificate Will Expire in Less Than 90 Days

Requirements

To perform this procedure, you must use an account with at least a Super user access level.

Probable cause

This alarm is raised 90 days before a TLS validation certificate expires.

Impact

Minor, non-service-affecting (m, NSA)

Steps

1. Upload a new TLS validation certificate to the RLS shelf. Refer to “Uploading a TLS validation certificate” procedure in *Licensing, Security, and Administration*, 323-2051-300.

Copyright© 2019-2025 Ciena® Corporation

Procedure 24 Circuit Pack Fail

Requirements

To perform this procedure, you must:

- observe all safety requirements described in the “Observing product and personnel safety guidelines” section in *6500 RLS Shelf Installation Guide, 323-2051-201*
- have a replacement module for the failed module
- have an Electrostatic Device (ESD) ground strap

Probable cause

This alarm is raised in the following situations:

- the module or SFP has a hardware failure
- the CTM detects a major failure on another module or SFP
- when a wrong fiber or incorrect transponder modem source is connected to a module. For example, inserting a fiber originating from an L-band modem into a C-band CCMD.

Both the alarm and LED alarm indicators can report the failure at the same time. If not, verify that a CTM problem does not exist. The status LED comes on (red indicates a failure) after a module is inserted until it is completely booted. The module is not failed in this case. This LED must clear one minute after insertion.

When a Circuit Pack Failed alarm is raised, some hardware may not be operational. This can cause inaccuracies in the PM counts for facilities on this module.

Impact

Major, non-service-affecting (M, NSA) (for CTM, PIM)

Critical, service-affecting (C, SA) (for AP, FAN, IM)

Steps

1 Determine the time since the “Circuit Pack Failed” alarm was raised. Design expert data is automatically saved after a “Circuit Pack Failed” condition. This will take 5 minutes for the interface modules and 10 minutes for the CTM. It is recommended that modules or SFPs are not replaced during this time after the “Circuit Pack Failed” alarm has raised. The design expert data is not captured if you do not wait.

2 Identify the module raising the alarm.

Copyright© 2019-2025 Ciena® Corporation

If you want to perform the procedure using	**Then** go to the
CLI commands	step 3
Node Essentials	See the Node Essential steps in "Retrieving the data for the active alarm object" on page 32. Then go to step 5.

3 To identify the module raising the alarm, enter:

```
show active-alarm <id> [name] [resource] [raise-time]
[raise-time] [cause] [condition-type] [direction]
[location] [severity] [service-impact] [additional-info]
[user-notes...]
```

Refer to "Alarm parameters" on page 27 for applicable parameters.

4 Perform a diagnose equipment CLI command to evaluate alarm on the effected module. See the example below:

```
rls# action slots <slot|all> diagnose-equipment
```

The command have the following options:

```
<all> re-evaluate circuit pack failed alarm on all
equipment on the shelf
```

```
<slot> re-evaluate circuit pack failed alarm on a
particular slot on the shelf
```

If Diagnose Equipment is successful and the slot is in "ok" status, the alarm for that slot clears.

5 If the failure is against the CTM, it may not be possible to log into the network element to determine the active alarms.

6 Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.

7 If the failure is against the fan module, go to step 10.

8 Reseat the faulty module or SFP. Refer to "Reseating a module" procedure in this document.

9 Replace the faulty module or SFP. Refer to appropriate module replacement procedures in the "Module replacement" section.

10 If the failure is against the fan module, check whether the identified fan module has failed, or is not compatible with the shelf or its equipped Power Input Module. The fan status is indicated by the LEDs on the Access Panel "Rear Alarm" LED and the LEDs on the fan modules. A "Rear alarm" red LED

Copyright© 2019-2025 Ciena® Corporation

indicates if there are any alarms against the shelf fan modules and/or PIMs. If the LED is lit requiring the user to service the rear of the shelf to clear the alarm. The LEDs on the fan module behave as follows:

- A green LED is lit when the module is working properly.
- A red LED is lit when the fan fails but is receiving power.
- No LEDs are lit if the fan control circuit is damaged or if the fan is not receiving power because it is not compatible with the shelf or its Power Input Modules.

Treat a fan with no LEDs lit as a failed fan.

11

If the fan module	**Then** go to
has failed	step 12
is missing	step 14

12 Verify that the fan module is fully inserted and make any necessary adjustments.

13

If the original alarm has	**Then**
cleared	this procedure is completed
not cleared	go to step 14

14 Install the missing fan module(s) or replace the failed fan module(s). Refer to the Procedure 148, “Replacing a shelf fan module” of this document.

Ensure you use the correct fan type.

15 Retrieve all alarms and ensure the system is restored to its original state.

If the original alarm has	**Then** go to
cleared	step 16
not cleared	step 18

16 Verify the shelf inventory. To display the inventory, refer to “Provisioning a slot” procedure in *Equipment/Facility Provisioning and Protection*, 323-2051-310.

17 Ensure that the new module is displayed in the equipment inventory.

18 If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 25 Circuit Pack Mismatch

Requirements

To perform this procedure, observe all safety requirements described in the "Observing product and personnel safety guidelines" section in *6500 RLS Shelf Installation Guide*, 323-2051-201.

Probable cause

This alarm is raised when a module or SFP is equipped in or inserted into a slot provisioned for:

- a module or SFP of another type
- a module or SFP of the same type that supports additional features (in this case, the module or SFP have different/mismatched PECs)

During provisioning, a slot is assigned a specific facility and module type. The assignments are recorded in the provisioning database.

Insertion of the CTM with 16G DDR Memory (RAM) (NTK810DB) in an R2 shelf while the shelf is running a pre-Release 2.1 software load will result in a Circuit Pack Mismatch alarm.

This alarm can also be raised after an SPF replacement or when an incompatible SFP is inserted in the slot. The alarm clears when you re-provision the slot.

This alarm is also raised if the module is not inserted properly in the slot. User can reseat the module to clear this alarm.

Impact

Major, service-affecting (M, SA)

Note: An equipment protection switch occurs if protection is available. If the module is unprotected, shelf functions can be disrupted.

Steps

1 Verify the shelf inventory and compare the slot assignments and physical PECs listed with the actual modules in the shelf until you identify the mismatched module.

To display the inventory, use the following command:

```
show slots <x> inventory circuit-pack
```

To display the equipment provisioned, use the following command:

```
show slots <x> config circuit-pack
```

For more information, refer to *Equipment/Facility Provisioning and Protection*, 323-2051-310.

Copyright© 2019-2025 Ciena® Corporation

2 Identify any mismatches between the physical PEC and provisioned PEC. A mismatch can indicate a PEC provisioning error or an incorrect module is installed.

Mismatched modules can be the same circuit pack type, but have different PECs. In these cases, ensure PECs match. Refer to the probable cause section for this alarm.

3 Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.

4 Identify the slot where the mismatch module located and reseat the mismatch module in the same slot. Verify if the alarm is cleared. If the alarm is not cleared then go to next step.

5 Identify the slot where the mismatch module located and replace the mismatched module with an appropriate module. Refer to the "Module replacement" procedure section in this document.

6

If the original alarm has	**Then**
cleared	the procedure is complete
not cleared	go to step 7

7 Identify the module raising the alarm.

If you want to perform the procedure using	**Then** go to the
CLI commands	step 8
Node Essentials	See the Node Essential steps in "Retrieving the data for the active alarm object" on page 32. Then, go to step 9.

8 Identify the module raising the alarm, enter:

```
show active-alarm <id> [name] [resource] [raise-time]
[raise-time] [cause] [condition-type] [direction]
[location] [severity] [service-impact] [additional-info]
[user-notes...]
```

Refer to "Alarm parameters" on page 27 for applicable parameters.

9 Replace the module you identified in step 8. Refer to the "Module replacement" section in this document. Select the appropriate procedure from the "Module replacement procedures list" table.

If the alarm clears, the module you identified in step 8 is damaged.

10 If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 26 Circuit Pack Missing

Requirements

To perform this procedure, you must:

- observe all safety requirements described in the “Observing product and personnel safety guidelines” section in *6500 RLS Shelf Installation Guide*, 323-2051-201
- obtain replacement modules

Probable cause

This alarm is raised when a slot is provisioned and the following occurs:

- no module or SFP is in the designated slot
- module or SFP failure makes it undetectable
- the access panel or PIM has been removed from the system
- a provisioned passive module is disconnected from the shelf Access Panel External Slot port
- the fan module is not fully engaged with the backplane

Impact

Major, service-affecting (M, SA)

Steps

1 Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.

2 Identify the module raising the alarm.

If you want to perform the procedure using	**Then** go to the
CLI commands	step 3
Node Essentials	See the Node Essential steps in “Retrieving the data for the active alarm object” on page 32. Then go to step 4.

3 Identify the module raising the alarm, enter:

```
show active-alarm <id> [name] [resource] [raise-time]
[raise-time] [cause] [condition-type] [direction]
[location] [severity] [service-impact] [additional-info]
[user-notes...]
```

Refer to “Alarm parameters” on page 27 for applicable parameters.

Copyright© 2019-2025 Ciena® Corporation

4

If	**Then** go to
an equipment connected to External Slots is reported missing	step 7
any other module is reported missing	step 5

5

If	**Then**
the slot is empty	insert a module of the correct type into the slot. Go to step 6.
a module of the correct type is in the slot	go to step 8.

6 Wait 30 seconds and retrieve all alarms to determine if the original alarm has cleared.

If the original alarm has	**Then**
cleared	the procedure is complete
not cleared	go to step 8

7 Verify that the cable between the shelf External Slot Inventory port and the external peripheral is connected and is not damaged.

Go to step 12.

8

If the module	**Then** go to
is still carrying traffic and providing all services	the next step
is not carrying traffic and providing all services	step 12

9 Reseat the previously active CTM. Refer to the Procedure 138, “Reseating a module” in “Module replacement” section in this document. When the CTM has finished booting, initiate a switch back to the originally active CTM. After the system recovers, check if the alarm has cleared.

If the original alarm has	**Then**
cleared	the procedure is complete
not cleared	go to step 10

10 Ensure that the fan module is fully engaged with the backplane. Refer to Procedure 148, “Replacing a shelf fan module”, step 10 to step 14.

11 If the alarm does not clear, replace the original CTM. Refer to the Procedure 140, “Replacing a Control and Timing Module (CTM)”. Initiate a switch back to the newly inserted CTM. After the system recovers, check if the alarm has cleared.

If the original alarm has	**Then**
cleared	the procedure is complete
not cleared	go to step 12

Copyright© 2019-2025 Ciena® Corporation

12 If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 27 Circuit Pack Unknown

Requirements

To perform this procedure, you must observe all safety requirements described in the “Observing product and personnel safety guidelines” section in *6500 RLS Shelf Installation Guide*, 323-2051-201.

Probable cause

This alarm is raised in the following situations:

- when an unsupported module or SFP is inserted into the shelf
- when the inventory information cannot be properly read from the module or SFP
- module or SFP is provisioned and present, but is unable to get inventory PEC or inventory PEC is invalid/unsupported module or SFP
- when a CTM with 16G DDR Memory (RAM) (NTK810DB) is inserted in an R2 shelf while the shelf is running a pre-Release 2.1 software load

Impact

Minor, non-service-affecting (m, NSA)

Steps

1 Identify the module raising the alarm.

If you want to perform the procedure using	**Then** go to the
CLI commands	step 2
Node Essentials	See the Node Essential steps in “Retrieving the data for the active alarm object” on page 32. Then go to step 3.

2 To identify the module raising the alarm, enter:

```
show active-alarm <id> [name] [resource] [raise-time]
[raise-time] [cause] [condition-type] [direction]
[location] [severity] [service-impact] [additional-info]
[user-notes...]
```

Refer “Alarm parameters” on page 27 to for applicable parameters.

3 Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.

4 Ensure that the module reporting the alarm is supported for the software release running on the shelf.

Copyright© 2019-2025 Ciena® Corporation

If the module is	**Then**
not supported by the software release	the module cannot be equipped in the shelf. Remove it. Go to step 5.
supported by the software release	go to step 6

5 Wait 30 seconds, and retrieve all alarms. When the module is removed, a “Circuit Pack Mismatch” or “Slot Empty” alarm can be raised.

If the original alarm has	**Then**
cleared	the procedure is complete
not cleared	go to step 6

6 Compare the module raising the alarm with the supported modules for each slot on the shelf. Refer to the “Module descriptions, equipping rules, specifications” section in *6500 RLS Planning Guide*, NTRN10WA.

If the module raising the alarm is in	**Then**
an unsupported slot	go to step 9
a supported slot	the module may be damaged. Go to step 8.

7 Replace the module raising the alarm with a module supported in that slot. Refer to the “Module replacement” section in this document.

Go to step 9.

8 Replace the module with an identical module.

9 Wait 30 seconds and retrieve all alarms.

If the original alarm	**Then**
is cleared	the procedure is complete. If you replaced a module in step 8, the module you replaced is damaged.
is not cleared	contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 28 Configuration Mismatch

Requirements

To perform this procedure, you must use an account with at least an Admin user access level.

Probable cause

This alarm is raised if the admin weight or bundle id is different on both sides of a Optical Signaling and Routing Protocol (OSRP) link.

Impact

Minor, Non-service-affecting (m, NSA)

Steps

1. Log into Node Essentials, launch the OSRP Provisioning application and click on Links Tab to determine if both ends of the OSRP link have the same admin weight and bundle id assigned.
2. If different, provision the OSRP link to have the same admin weight and bundle id assigned.
3. If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 29 Connection Validation Data Mismatch

Probable cause

This alarm is raised when expected-nbr-ids and expected-port-id in the configuration connection validation data did not match the actual-nbr-ids and actual-port-id in the inventory connection validation data on the Rx ports of the MPO sub-fiber.

> ***Note:*** After a module restart, the module's inventory CV ports rx actual-port-id shows “Pending” until the port is scanned in the first subsequent CV RX cycle. Once all RX ports are scanned, the alarm clears. It can take up to 75 minutes to scan the port after a module restart.

Impact

Warning, non-service-affecting (W, NSA)

Steps

1. Verify that links are provisioned to represent both the physical and logical paths between the MPO ports on the active modules. Refer to *Optical Control, SPLI, and OTDR*, 323-2051-318 for more information.
   a. Check what the configured expected-port-id field is of the alarming resource using the following command:

      ```
      show slots <#> cv ports rx <port-subfiber>
      ```

      Note: There is no Node Essentials equivalent command for this release.

   b. Compare this with what the slot inventory is displaying with the following command:

      ```
      show slots <#> cv ports rx <port-subfiber>
      ```

      Note: There is no Node Essentials equivalent command for this release.
2. Verify if all the MPO cables are connected correctly.
3. If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 30 Connection Validation Data Missing

Probable cause

This alarm is raised when the connection validation (CV) data used for validation of fiber interconnections is missing.

The alarm is raised when the CV expected data is not received due to a misprovisioned link or CV data, a dirty, defective or missing LC loopback plug or MPO.

This alarm is also raised momentary when you switch back from CV mode Focus to Full mode. The alarm stays active (up to 20 minutes) until the CV cycle goes through all ports.

This alarm is also raised momentary when the CCMD card or any other card with CV also when you perform the cold restart operation on the card.

Impact

Warning, non-service-affecting (W, NSA)

Steps

1. Verify that fibers are installed on the LC/MPO port. Use loopback connectors if fibers are missing on the port.
2. Verify if all the MPO cables are connected correctly. Manually provision CV associations between each interconnected MPO Tx port and MPO Rx port.
3. **CAUTION**
   Risk of traffic loss
   The following steps will impact traffic. If possible, re-route the traffic to minimize the traffic loss.

   Perform the following steps during a maintenance window.

   a. Disconnect and clean the suspected MPO fiber or the LC loopback connector. Clean the connector and fiber end using an appropriate fiber cleaner.
   b. Re-insert the fiber. Wait at least 30 minutes for the alarm to clear.
4. If the alarm does not clear, clean the LC loopback fibers/connectors.
5. If the alarm does not clear, replace the suspected MPO fiber.
6. Ensure that the CV data and link provisioning of the system is correct. Refer to “Retrieving, provisioning and deleting connection validation port sequences” procedure in *6500 RLS Optical Control, SPLI, and OTDR*, 323-2051-318.
7. If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 31 Controller Inactive

Requirements

To perform this procedure you must use an account with an at least an Admin user access level.

Probable cause

This alarm is raised by different controller instances such as device-controller and channel-controllers to indicate that the controller is not actively running due to an administrative action.

For more detail on this alarm, refer to the RLS Optical Control, SPLI, and OTDR, 323-2051-318.

Impact

Warning, non-service-affecting (W, NSA)

Steps

1

If the alarm is raised by	**Then** go to
device-controller	step 2
CCS (Channel-Control-SVC)	step 6

2

If the alarm is raised due to	**Then** go to
admin-state disabled	step 3
span loss compensation disabled	step 4
controller not in operational state in a calibrated system	step 5

3 Set the device-controller instance admin-state to Enabled.

```
set device-controller <PFG name, controller type> admin-state Enabled
```

For example, set device-controller LINE-PFG-1-MUX, booster admin-state Enabled.

Go to step 10.

4 If the alarm is raised due to span loss compensation that is disabled on the line-fiber link facility. Eventually, disables the span loss compensation in the downstream amp-controller. In such case, enable the pinch-compensation on the upstream shelf as follows:

a. go to the upstream shelf.

b. enable the pinch-compensation on the line out link.

```
set link PFG-1-MUX-LINEOUT pinch-compensation enabled
```

Go to step 10.

Copyright© 2019-2025 Ciena® Corporation

5

CAUTION
Risk of traffic loss
Recalibration causes traffic loss.

Confirm there are no faults on the line (for example, fiber break, APR, ...) and trigger recalibration.

Note: For any configuration, C+L-Band or C-Band only, a single alarm is raised by the parent instance for all child controllers. This alarm is not supported in DCI configurations.

Go to step 10.

6

If the alarm is raised due to	**Then** go to
admin-state disabled	step 7
channel controller disabled	step 8

7 Set the admin-state to Enabled:

```
set ccs-instance <PFG name> config admin-state Enabled
```

For example, set ccs-instance SECTION-PFG-1-MUX-L/SECTION-PFG-1-MUX config admin-state Enabled.

Go to step 10.

8 Find the closed-loop condition per channel controller using the following command:

```
show ccs-instance SECTION-PFG-1-MUX channel-controller *
config closed-loop
```

9 Set the closed-loop to enabled:

```
set ccs-instance <PFG name> channel-controller <fc>
config closed-loop Enabled
```

For example, set ccs-instance SECTION-PFG-1-MUX channel-controller 189362.500 config closed-loop Enabled.

10 If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 32 Connection Validation Focus Mode Enabled

Requirements

To perform this procedure you must use an account with at least an Admin user access level.

Probable cause

This alarm is raised against the target-port provisioned under the cv-shelf-config when the Connection Validation (CV) mode is set to focus.

Impact

Warning, non-service-affecting (W, NSA)

Steps

1. Set the cv-shelf-config mode full.

   ```
   set cv-shelf-config mode full
   ```

   Note: There is no Node Essentials equivalent command for this release.

2. If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 33 Corrupt Inventory Fault

Requirements

To perform this procedure, you must:

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *6500 RLS Shelf Installation Guide*, 323-2051-201
- have an antistatic wrist strap to dissipate electrostatic charges

Probable cause

This alarm is raised against the shelf, cooling unit, Access Panel, Power Input Card, R2 CTM front panel, or external equipment connected to the remote inventory ports on the access panel when the inventory data cannot be retrieved from the specified equipment when the equipment is:

- not recognized by the NE
- not fully inserted
- defective
- connected using a defective cable

Impact

Major, non-service-affecting (M, NSA)

Steps

1 **DANGER**
Risk of eye injury
Wear eye protection such as safety goggles or safety glasses with side guards when you work with fan modules, air filters or in proximity to the shelf air exhaust.

Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.

2 Verify that the alarmed unit is fully inserted.

3 Verify that the cable between the shelf External Slot Inventory port and the external peripheral is connected and not damaged.

4 If applicable, perform a restart of the alarmed unit. Refer to Procedure 5, “Restarting an interface module or the CTM”.

5 If the alarm did not clear, reseat the alarmed unit, or disconnect and reconnect the cable connecting the alarmed module (the cable between the shelf External Slot Inventory port and the external peripheral). Refer to Procedure 138, “Reseating a module”.

6 If the alarm did not clear, replace the alarmed unit. Refer to the equipment replacement procedures in this document.

Copyright© 2019-2025 Ciena® Corporation

7 If the alarm does not clear, it could be due to a problem with a module. Contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 34 Database Recovery Failed

Requirements

To perform this procedure, you must use an account with at least an Admin user access level.

Probable cause

This alarm is raised when the database is failed during the database recovery operation.

Impact

Major, non-service-affecting (M, NSA)

Steps

1. If there is a valid backup available, perform a complete database restore. Refer to the “Backup and Restore” procedures in *6500 RLS Licensing, Security, and Administration*, 323-2051-300.
2. If the alarm is not cleared or a valid database is not available, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 35 Database Restore In Progress

Requirements

To perform this procedure, you must use an account with at least an Admin user access level.

Probable cause

This alarm is raised when the provisioning data is being restored to a shelf.

Impact

Minor, non-service-affecting (m, NSA) alarm

Steps

1. Wait until the currently ongoing database restore successfully completes. Refer to the “Backup and Restore” procedures in *6500 RLS Licensing, Security, and Administration*, 323-2051-300.
2. To clear the alarm and abort the database restore action, Cancel the Backup and Restore operation. Canceling recovers the system and cleans up any backup files left in invalid states.
3. You can also clear the alarm by committing the internal provisioning database. Refer to “Restoring and committing the internal provisioning database” in *6500 RLS Licensing, Security, and Administration*, 323-2051-300.
4. If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 36 Data Mismatch

Requirements

To perform this procedure, you must use an account with at least an Admin user access level.

Probable cause

This alarm is raised when tx-proxy config parameters do not match tx-proxy inventory parameters. Consider the following:

> ***Note:*** The alarm is not raised if pre-MCP 6.2 Wave Line Synchronizer (WLS) is managing the channels.WLS supports the discovery of transponder parameters as of MCP 6.2, and the alarm can be raised in this case. The minimum recommended load is MCP 6.2-P02.When WLS populates tx-proxy in the inventory of the RLS ingress port for the Photonic service (for example, CCMD Channel Input, or RLA12x1 Switch Input in the case of TDA), the RLS software compares inventory and config and raise the “Data Mismatch” alarm if there are inconsistencies between the two.The “Data Mismatch” alarm can be incorrectly raised in earlier RLS releases 2.3 through 3.0 (contact Ciena support group for further information) when managed by MCP 6.2 or later.

The default value of tx-proxy tuning-mode parameter is set to fast. If you have Waveserver WL3 transponders connected to RLS 2.3 or higher, it is required to manually provision tuning-mode parameter in tx-proxy to **accelerated**. This alarm is raised when tuning-mode is not provisioned to **accelerated** and SPLI is managing that connection. To clear the alarm, update tuning mode to accelerated.

This alarm is also raised if the user is managing the WL5n PTP on the transponder using SPLI or the WLS and the `Tx-proxy link optimization mode` is not same as `provisioned tuning mode`.

Impact

Minor, non-service-affecting (m, NSA)

Steps

1 Compare the tx-proxy or rx-proxy config/inventory (for example, CenterFreq, TransmissionMode, LinkOptimizationMode, TuningMode, LaserCentering, CcdaEnabled, and Blanking) using the following commands:

```
show slots <CCMD slot #> config tx-proxy <port> //
“provisioned” data
```

```
show slots <CCMD slot #> inventory tx-proxy <port> //
“discovered” data
```

```
show slots <CCMD slot #> config rx-proxy <port>
```


Copyright© 2019-2025 Ciena® Corporation

```
show slots <CCMD slot #> inventory rx-proxy <port>
```

Note: There is no equivalent Node Essentials menu items of this command in this release.

2 Verify if connection to transponder shelf is reliable.

```
RLS11# show transponders host
host-name : ciena-pro-neighbors:neighbors TERM5-5
connection-state : reliable
```

Note: There is no equivalent Node Essentials menu items of this command in this release.

3 If the connection state is unreliable, “Node Unreachable” alarm is raised. Refer to “Node Unreachable” alarm clearing procedure to clear the alarm.

4 If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 37 Disk Usage - 75%

Requirements

To perform this procedure, you must use an account with at least an Admin user access level.

Probable cause

This alarm is raised when the disk is 75% full on the CTM or Access Panel, and clears when there is at least 30% free space. This alarm is for information only and does not affect the operation of the shelf. It is recommended that you attempt to clear this alarm to prevent possible future problems if the disk becomes too full.

Impact

Minor, non-service-affecting (m, NSA)

Steps

1. Contact your next level of support or your Ciena support group to delete any loads that you do not require on the disk.

Copyright© 2019-2025 Ciena® Corporation

Procedure 38 Disk Usage - 90%

Requirements

To perform this procedure, you must use an account with at least an Admin user access level.

Probable cause

This alarm is raised when the disk is 90% full on the CTM or Access Panel, and clears when there is at least 15% free space. This alarm is for information only and does not affect the operation of the shelf. It is recommended that you attempt to clear this warning to prevent possible future problems if the disk becomes too full.

Impact

Major, non-service-affecting (M, NSA)

Steps

1. Contact your next level of support or your Ciena support group to delete any loads that you do not require on the disk.

Copyright© 2019-2025 Ciena® Corporation

Procedure 39 Disk Full

Requirements

To perform this procedure, you must use an account with at least an Admin user access level.

Probable cause

This alarm is raised when the disk is full on the CTM or Access Panel.

Impact

Major, Service-affecting (M, SA)

Steps

1. Contact your next level of support or your Ciena support group to delete any loads that you do not require on the disk.

Copyright© 2019-2025 Ciena® Corporation

Procedure 40 Entitlement Enforcement Disabled

Requirements

To perform this procedure, a user must have an account with at least admin access privileges.

Probable cause

This alarm is raised in the following situations:

- a shelf has recovered from commissioning mode and no licensing model has yet been provisioned.
- License client registration-id is configured but the license client registration-secret is not yet configured
- The license operational-state is in 'commissioning' mode in this condition.

Impact

Warning, non-service-affecting (W, NSA)

Steps

1. Activate a license file or configure a license server on the RLS node. Refer to “Licensing” chapter in *Licensing, Security, and Administration*, 323-2051-300 for more information.
2. If the alarm does not clear, contact your next level of support or Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 41 Equipment Configuration Mismatch

Requirements

To perform this procedure, you must observe all safety requirements described in *6500 RLS Shelf Installation Guide*, 323-2051-201.

Probable cause

This alarm applies to Power Input Modules (PIM)s when a mixture of two different PIM PECs is detected.

This alarm also applies to CTMs in slot 41 and 42 when a mixture of two different CTM PECs (NTK810FA/NTK810FB) or (NTK810DA/NTK810DB) or (NTK810QA/NTK810QB) is detected.

Impact

Major, non-service-affecting (M, NSA)

Steps

1 **DANGER**
Risk of eye injury
Wear eye protection such as safety goggles or safety glasses with side guards when you work with fan modules, air filters or in proximity to the shelf air exhaust.

Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.

2 Ensure the shelf is equipped with two Power Input Modules or CTMs of the same type.

3 If the Power Input Module or CTMs are not the same type, determine which Power Input Module or CTM is not expected. Replace the Power Input Module or CTM that is not expected in the shelf. Ensure that the equipped Power Input Modules or CTMs are compatible with the shelf, and that all equipped Power Input Modules have the same amperage capacity. Refer to Procedure 151, “Replacing a DC Power Input Module” or Procedure 140, “Replacing a Control and Timing Module (CTM)” in this document.

4 After the expected Power Module or CTM replacement is completed, the “Circuit Pack Mismatch” alarm can be raised against the replaced module. Refer to Procedure 25, “Circuit Pack Mismatch” to clear the alarm.

5 If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 42 External License Server Comms Failed

Requirements

To perform this procedure you must use an account with at least an Admin user access level.

Probable cause

Once a license server is configured, there is a periodic (every 15 minutes) health check and license sync up between the license server and the RLS shelf. This alarm is raised when the health check fails. The alarm is reported within 30 min of the detection of the health check failure. The alarm will be cleared when the health check succeeds in the next 15 min periodic attempt.

Impact

Minor, non-service-affecting (m, NSA) when the primary server is down, but the backup server is up, or the backup server is down and the primary server is up

Major, non-service-affecting (M, NSA) when both servers or the only server is down

Steps

1. Log into the RLS shelf raising the alarm. Refer to “Accessing and logging in to a network element procedure in *Licensing, Security, and Administration*, 323-2051-300 for more information.
2. Verify the network connection between the shelf and the license server.
3. Verify the additional-info text in the alarm to find out whether it is the primary, backup, or both servers.
4. Verify that the license server is provisioned and are not down. using ping, verify the external license server IP from the RLS shelf where the alarm has raised.
5. If the alarm does not clear, contact your next level of support or Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 43 External License Server Time Out Of Sync

Requirements

To perform this procedure you must use an account with at least an Admin user access level.

Overview

This alarm is raised when the RLS shelf system time is changed and the time difference between the RLS shelf and the license server is more than 24 hours. The alarm is raised within 30 minutes after a health check (which detects this time difference). The alarm clears when the RLS shelf system time is changed to be within the 24 hours from the license server system time. When this alarm is active, no licenses can be acquired/released from/to the license server.

Impact

Major, non-service-affecting (M, NSA)

Steps

1. Log into the RLS shelf raising the alarm. Refer to “Accessing and logging in to a network element procedure in *Licensing, Security, and Administration*, 323-2051-300 for more information.
2. Verify the TOD setting on the node and ensure that the difference between the RLS shelf and the license server is not more than 24 hours.
3. If the alarm does not clear, contact your next level of support or Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 44 Fiber Break Detected

Requirements

To perform this procedure, you must:

- log into the CLI of the nodes with admin or higher privilege level. For login information, see “Accessing and logging in to a network element” procedure in *Licensing, Security, and Administration*, 323-2051-300 for more information.
- observe all safety requirements described in *Installation – 6500 RLS Shelf,* 323-2051-201
- have an antistatic wrist strap to dissipate electrostatic charges
- have a fiber cleaning kit
- have a power meter and a power source

Probable cause

This alarm is raised when there is a physical fiber disconnection or when a large pinch is causing an LOS on the end port. In either case, the physical fiber needs to be repaired once the alarm is raised.

To detect a fiber-disconnect, the application verifies if a valid power is reported at the transmitting-end (from-port) of the fiber-link and the receiving-end (to-port) port is below LOS.

For “Fiber Break Detected” alarm to be raised, the following condition has to remain valid for 30 to 35 seconds.

- The “from” port of a given link has to have power > LOS threshold and the “to” port of the link has to have power < LOS threshold.

For a given bi-directional fiber connection, on a layer 0 restoration system, once a fiber break detected from one end, restoration is expected to trigger and that may not allow enough time to detect fiber break condition on the reverse direction due to lack of power (if all channels are restored from the that link). In this case, “Connection Validation Missing” alarm is also expected on the disconnected MPO port.

> ***Note:*** The “Fiber Break Detected” alarm is not supported on half-links where either the “to” port or “from” port is missing from link provisioning. The alarm is also not reported if link-type = line-fiber, for which “Optical Line Fail” alarm is reported on fiber-disconnect. The alarm is also not reported for a fiber break between a passive CMD module's common ports and an RLA switch port, as CMD passive modules do not provide power measurements.

Copyright© 2019-2025 Ciena® Corporation

When the alarm is active, channels at downstream section-mux are replaced with ASE.

If the nodes are Layer 0 Control Plane (L0CP) enabled, then the fiber break detection condition brings the associated OSRPLINK down and triggers restoration on existing traffic. The OSRPLINK continues to remain down until the alarm condition is.

When the fiber is pulled and then CTM is restarted after MR completed for all the channels, the error condition diagnostic is re-evaluated. In this case, fiber loss/scale finds that both switch-out and switch-in are in LOS state and the “Fiber Break Detected” alarm is not raised. Following the CTM restart, control plane may find the route available and can trigger restoration or revert which eventually fails and raises the alarm again. The behavior is as follows:

- Fiber break on inter-degree connections can happen
- All channels are restored
- CTM restarted
- If all above are true, following CTM restart, “Fiber Break Detected” alarm clears.
- If CV compatible config and CV runs over the next 16 minutes window, the “Connection Validation Missing” alarm will be raised.

  Note: If attenuation is too high and Fiber-break-detected conditions are showing true in link diagnostics, in this situation link diagnostics will not show measured-physical-loss and actual-measured-loss.

CAUTION

Risk of radiation exposure

If light is used to test the broken fiber (for example, with a light source or an OTDR), certain Automatic Line Shut Off (ALSO) and Input Loss Of Signal alarms can clear. When the shelf detects light, the alarms clear and the amplifier facility is powered up. This is an expected behavior because a shelf cannot distinguish between a light source from an optical test set and a light source from a shelf.

Ensure the adjacent optical amplifiers are “Disabled” when performing fiber repairs.

Impact

Major, service-affecting (M, SA)

Copyright© 2019-2025 Ciena® Corporation

Steps

1

CAUTION
Risk of laser radiation exposure
Do not look directly into the optical beam. Invisible light can severely damage your eyes.

CAUTION
Risk of damage to modules
Never disconnect an optical fiber that is connected to an active or powered-up optical amplifier. To disconnect or reconnect an optical fiber, ensure the optical amplifier is “Disabled”, then disconnect or reconnect the fiber.

CAUTION
Risk of damage to modules
Wear an antistatic wrist strap to protect the equipment from static damage. Connect the wrist strap to the ESD jack on the shelf or module.

Verify the fiber condition and clean it (for example, replace the jumper or remove the pinches).

2 If the link is in-between two different nodes, then check if there is proper communication between “From” and “To” nodes.

a. In CLI, “show nodes” indicates if the nodes are visible to each other and if the communication is up.

b. If the communication remains down (is-up = false), then a good communication needs to be established before clearing the alarm.

Note: See the “Node Unreachable” on page 173 alarm clearing procedure.

3 If comms are up, check if both “From” and “To” ports cleared the LOS, in which case a valid measured-physical-loss should be reported on the link and the alarm should be cleared.

Note: Even if there is communication issue between two nodes, following fiber re-connection or clean-up, a downstream section-mux will still recover channels from ASE. However, for control plane enabled node, the OSRPLINK will continue to remain down.

4 If the alarm is not clear after reconnection of the “To” port and it is in LOS clear, choose your next step:

If	**Then** go to
both the from and to-end modules have CV (connection-validation) capability	step 5
one of the modules do not have CV capability	step 6

Copyright© 2019-2025 Ciena® Corporation

5 If both the from and to-end modules have CV capability (such as RLA/LRU32x1 or CCMD8x24), then a valid measured loss can be reported by CV application following fiber reconnection and the alarm clears. In this case, no additional user action is required. CV measured loss can be refreshed faster by provisioning focused-mode to inspect specific MPO port connections. Go to step 25.

6 If one of the modules do not have CV capability (such as RLA12x1 C-band circuit pack or CCMD16), then following the fiber reconnection, it needs to be manually validated by injecting light to clear the alarm.

7 For manual validation, create a “TEST” channel at section-demux to set light on the demux switch port using upstream line system ASE where no channel existed. This will light up the fiber link. See the following examples:

If you want to perform the procedure using	**Then** go to the
CLI commands	“CLI INTERFACE STEPS”
Node Essentials	“NODE ESSENTIALS STEPS”

CLI INTERFACE STEPS

8 To create a “TEST” channel at section-demux, enter the following commands:

```
set mc-path TEST-DEMUX-193912.5-s1 min-freq 193875 max-
freq 193950 high-freq-deadband 6.25 low-freq-deadband
6.25 to "slots 1 config port 43" from "slots 1 config port
54" user-label "193912.5 MC slot 1 TEST"
```

```
set nmc-path TEST-DEMUX-193912.5-s1  to "slots 1 config
port 43" from  "slots 1 config port 54" center-freq
193912.5 spectral-width 62.5 nmc-network-id 193912.5fc
```

9 Go to step 18.

NODE ESSENTIALS STEPS

10 Select **Services** and then Media channel path from the Node Essentials navigation menu.

The Media channel path menu opens.

11 From the Media channel path grid, click on create icon.

The Create media channel path dialog opens.

12 Enter values for Name, Label, Minimum frequency, and Maximum frequency. Low frequency deadband and High frequency deadband are already defaulted at 6.25GHz. Select “from” and “to” port from Originating and Terminating end point.

13 Click **Confirm**.

14 Select **Services** and then Media channel path from the Node Essentials navigation menu.

The Network Media channel path menu opens.

15 From the Media channel path grid, click on create icon.

The Create NMC path dialog opens.

Copyright© 2019-2025 Ciena® Corporation

16 Enter values for Name, User label, Center frequency, Spectral width and NMC network ID. Select from and to port from Originating and Terminating end point.

17 Click **Confirm**.

18 Validate the measured-physical-loss from the fiber link and ensure the measured loss <= expected physical loss.

19 Delete the “TEST” channel (for example: delete nmc-path TEST-DEMUX-193912.5-s1 or delete mc-path TEST-DEMUX-193912.5-s1).

20 If the alarm is toggling and one of the modules (RLA, LRU or CCMD) has CV capability, then ensure at least 8x ports are defined under CV tx port-sequence or all ports from the CV port-sequence are removed that, in default, scans all ports. Port count lower than 8x can lead to transient alarms getting raised and cleared.

Figure 10 Example of CV port sequence with port count < 8x

```
NODE01# show slots 1 config cv config tx
  slots:
  - name   : 1
    config:
      cv:
        config:
          tx:
            admin-state   : Enabled
            port-sequence:
            - port   : ciena-6500r-ports:port 21-3
            - port   : ciena-6500r-ports:port 21-4
            - port   : ciena-6500r-ports:port 21-5
            - port   : ciena-6500r-ports:port 21-6
```

NODE ESSENTIALS STEPS

21 Select **Facilities** from the Node Essentials navigation menu.

The Facilities menu opens.

22 From the Equipment grid, select the module which you want to check CV port sequence.

The bottom part of screen becomes populated.

23 Select Connection validation facility from Facility navigator.

The Connection validation details opens.

24 Browse Port Sequence for Tx or Rx in its details.

25 If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 45 Fiber Type Unknown

Requirements

To perform this procedure, use an account with at least an Admin user access level.

Probable cause

This alarm is raised against a line-fiber link-type when the fiber type is not provisioned (for example: left at default “unknown”).

Impact

Major, non-service-affecting (M, NSA)

Steps

1. Provision the Fiber Type value to the fiber type used. Refer to *Optical Control, SPLI, and OTDR*, 323-2051-318.
2. If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 46 Firmware Mismatch

Requirements

To perform this procedure, a user must have an account with at least admin access privileges.

Probable cause

This alarm is raised on a module or CTM where the FPGA image is incorrect.

This alarm is masked by Circuit Pack Fail, Upgrade Fail, or Intercard Suspected alarms.

Impact

Major, non-service-affecting (M, NSA)

Steps

1. Identify the module that is raising the alarm.
2. Perform a one-step or multi-step upgrade on the identified module.
3. If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 47 Forced Shutoff

Requirements

To perform this procedure, you must use an account with at least an Admin user access level.

Probable cause

This alarm is raised by control applications when software sets the force shutoff on an EDFA due to upstream fiber faults or loss of communication/ topology with another node in the section.

Note: The “Forced Shutoff” alarm can be masked when the booster AMP forced-shutoff is enabled. If Automatic Line Shut Off (ALSO) is not disabled explicitly, setting the forced-shutoff enabled will cause ALSO to be enabled where there is no OSC.This alarm does not mask the ALSO related alarms (OLF + AS alarm) because they are safety alarms.

Impact

Major, service-affecting (M, SA)

Steps

1 Check if oms egress FDI (forward defect indicator) flag is set. Enter the following CLI command:

```
show oms-egress
```

```
Example:
```

```
SITE-01# oms-egress: - name : LINE-PFG-1-DEMUX fdi : true
band-specific: - band : BAND-C fdi : true - band : BAND-
L fdi : true
```

Note: There is no Node Essentials equivalent command for this release.

2 If the FDI flag set to true, the fault condition is still present in upstream within the OMS. Clear the fault condition.

The FDI flag and the forced-shutoff condition are automatically cleared.

3 Check if a “Node Unreachable” alarm is raised in the section. This alarm needs to be cleared in order for FDI to be updated. Refer to “Node Unreachable” alarm clearing procedure for more details.

WARNING

If there is line-fault such as Optical Line Failed (OLF), and then recovered later, the section level Fault-Detection-Indicator (FDI) may not be able to recover if full section comms visibility is not available. Therefore it is important that any alarms such as Node Unreachable or OSPF Adjacency Loss are resolved to ensure the system can respond accordingly to photonic faults.

Copyright© 2019-2025 Ciena® Corporation

4 Verify if the EDFA is turned off manually during some MW operation. In such case, FDI flag is set to false. Disable forced shutoff condition manually on the AMP facility.

5 Verify the booster AMP state if the “Optical Line Failed” (OLF) alarm is active.

6 Place the alarmed AMP facility to “Disabled”:

If you want to perform the procedure using	**Then** go to the
CLI commands	“CLI INTERFACE STEPS”
Node Essentials	“NODE ESSENTIALS STEPS”

CLI INTERFACE STEPS

7 To disable forced shutoff condition manually on the AMP facility, enter the following CLI command:

```
set slots <x> amps Pre-AMP-Cband forced-shutoff Disabled
```

8 Go to step 16.

NODE ESSENTIALS STEPS

9 Select **Facilities** from the Node Essentials navigation menu.

The Facilities menu opens.

10 From the **Equipment** grid, select the module with the alarmed AMP facility.

The bottom part of screen becomes populated.

11 Select AMP facility from Facility navigator.

The AMP Facilities grid opens.

12 Select the alarmed AMP facility by Row selector from the AMP Facilities grid.

13 Click the **Pencil** icon.

The related Edit AMP dialog opens.

14 Edit the AMP facility Forced shutoff to Disabled.

15 Click **Confirm**.

16 If Raman is present in the section and Raman OTS RDI/FDI is set to true, the FDI can be raised. If the FDI is raised, check the Raman inventory diagnostic to verify the OTS RDI/FDI value.

17 If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 48 Forced Switch Active

Requirements

To perform this procedure, you must use an account with at least an Admin user access level.

Probable cause

This alarm is raised when a forced switch action has been set on a path.

Impact

Minor, non-service-affecting (m, NSA)

Steps

1. No action is required if a user is performing a test or maintenance operation. This alarm is a reminder not to leave a potentially service-affecting condition on the system.
2. Release the forced switch. Refer to the “Releasing a Manual switch, Forced switch, or Lockout” procedure in *Equipment/Facility Provisioning and Protection*, 323-2051-310. See the example below:

   ```
   protection-switch resource "slots 4 config protection-group 1 switch 2" switch-action release
   ```

3. If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 49 Forced Switch Active - Remote

Requirements

To perform this procedure, you must use an account with at least an Admin user access level.

Probable cause

This alarm is raised when a forced switch is active on the remote TPS.

Note: This alarm is only applicable for DCI TPS configurations.

Impact

Minor, non-service-affecting (m, NSA)

Steps

1. No action is required if a user is performing a test or maintenance operation. This alarm is a reminder not to leave a potentially service-affecting condition on the system.
2. Release the forced switch on the remote TPS. Refer to the “Releasing a Manual switch, Forced switch, or Lockout” procedure in *Equipment/Facility Provisioning and Protection*, 323-2051-310. See the example below:

   ```
   protection-switch resource "slots 4 config protection-
   group 1 switch 2" switch-action release
   ```
3. If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 50 Guest OS Failure

Requirements

To perform this procedure, you must:

- observe all safety requirements described in *6500 RLS Shelf Installation Guide,* 323-2051-201
- ensure that you have all the documentation referenced in this procedure
- ensure that all alarms are enabled; see the alarm provisioning and alarm profiles procedures in this chapter
- use an account with admin privileges or higher

CAUTION
Risk of traffic loss
You will lose all traffic while reseating an unprotected module. If possible, ensure that the module you are reseating is protected.

CAUTION
Risk of equipment damage
Electrostatic discharge (ESD) can damage electrostatic sensitive devices. You must use antistatic protection while unpacking and installing all Field-Replaceable Units (FRU) and cables.

Probable cause

This alarm is raised when the Guest OS fails either due to an internal error or an error with the user scripts.

Impact

Minor

Steps

1. Disable the guest OS to clear the alarm.
2. If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 51 Hardware Subsystem Failure

Requirements

To perform this procedure, you must:

- use an account with at least an Admin user access level
- observe all safety requirements described in the “Observing product and personnel safety guidelines” section in *6500 RLS Shelf Installation Guide*, 323-2051-201

Probable cause

This alarm is raised when:

- a module has a hardware failure that cannot be recovered on its own
- a module fails to boot up
- Connection Validation Transmitter fails on a CCMD card

Impact

Minor, non-service-affecting (M, NSA)

Steps

1 Perform a diagnose equipment CLI command to evaluate alarm on the effected module. See the example below:

```
rls# action slots <slot|all> diagnose-equipment
```

The command have the following options:

```
<all> re-evaluate circuit pack failed alarm on all
equipment on the shelf
```

```
<slot> re-evaluate circuit pack failed alarm on a
particular slot on the shelf
```

If Diagnose Equipment is successful and the slot is in “ok” status, the alarm for that slot clears.

2 If the alarm did not clear, perform a protection switch on the module. Refer to the “Protection configurations and CTM redundancy” procedure in *Equipment/Facility Provisioning and Protection*, 323-2051-310.

3 If the alarm does not clear, reseat the module. Refer to Procedure 138, “Reseating a module” in the “Module replacement” section in this document.

4 Replace the alarmed module. Refer to the appropriate procedure in the “Module replacement” section of this document, to clear this alarm.

5 If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 52 High Fiber Loss

Requirements

To perform this procedure, you must:

- use an account with at least an Admin user access level
- observe all safety requirements described in *6500 RLS Shelf Installation Guide,* 323-2051-201
- have a fiber cleaning kit (for Photonic configurations, LC cleaning kits are needed). See the *Optical Connector Inspection and Cleaning*, 323-1859-500.
- obtain a fiber patchcord, if required

Probable cause

The “High Fiber Loss” alarm is raised when the measured loss between near-end and the far-end is greater than either of the provisioned loss thresholds.

A 0.5 dB hysteresis is also applied for the alarm to clear, which prevents the alarm from clearing until the measured loss has gone below the threshold(s) by more than 0.5 dB.

The alarm with **minor** severity:

- is raised when: (Measured-physical-loss - Expected-physical-loss) >= high-fiber-loss-minor-threshold
- and clears when: (Measured-physical-loss - Expected-physical-loss) < high-fiber-loss-minor-threshold - hysteresis (0.5 dB)

The alarm with **major** severity:

- is raised when: (Measured-physical-loss - Expected-physical-loss) >= high-fiber-loss-major-threshold
- and clears when: (Measured-physical-loss - Expected-physical-loss) < high-fiber-loss-major-threshold - hysteresis (0.5 dB)

Note: For spans that include the SRA module, the actual measured loss is equivalent to the measured physical loss minus the reported RAMAN gain, as the SRA provides Raman amplification. If the SRA is not present, the actual measured loss and measured physical loss are equal.

Refer to “Link Parameters” table in *Optical Control, SPLI, and OTDR*, 323-2051-318.

Copyright© 2019-2025 Ciena® Corporation

This alarm is also raised when upgrading from a pre-fix release to a post fix release and the pumps are toggled (can be due to ALSO and recovery as well), the Raman gain may change depending on how the gain was calculated when it turned on before. If the old gain was sourced from TG and instead of PD1, the gain can increase by 1-2 dB but closer towards the provisioned gain.

Note 1: If the alarm is detected on the LRU to RLA fiber link, check the L-band ASE status under the RLA to confirm that forced shutoff is “Enabled”. If the forced shutoff is “Disabled” (that means the RLA upgrade L-band ASE is ON), and the LRU reverse OPTMON (41-reverse or 51-reverse) is in LOS, it means the LRU to RLA link fiber is in disconnected state, and any link loss measurement provided on that state for the LRU to RLA fiber link will not be reliable at that state.

Note 2: The expected-physical-loss is system derived and must not be changed manually.

Impact

Major, service-affecting (M, SA)

Minor, non-service-affecting (m, NSA)

Note 1: When the measured-physical-loss is greater than the channel add threshold (default of 4.0 dB) on any of the ROADM intra-site fiber links including (1) CCMD to RLA/LRU in the add direction, (2) RLA to RLA or (3) LRU to LRU, the channel add action will fail. A capacity change pending alarm will be visible in such case.

Note 2: If the network is L0 control plane managed, then that will cause L0CP managed channels to fail to recover when trying to restore using the path with the excessive fiber loss.

Steps

1 Use the active “High Fiber Loss” alarm to identify the link the alarm is raised on.

2 Verify the current “measured-physical-loss” on the alarmed link and compare it to the “expected-physical-loss” actual current loss shown in the response:

If you want to perform the procedure using	**Then** go to the
CLI commands	“CLI INTERFACE STEPS”
Node Essentials	“NODE ESSENTIALS STEPS”

CLI INTERFACE STEPS

3 To display the expected-physical-loss, measured-physical-loss and expected-line-fiber-loss, along with provisioned high fiber loss thresholds, enter the following command accordingly:

Copyright© 2019-2025 Ciena® Corporation

```
show link <LinkName> [measured-physical-loss] [expected-
physical-loss] [expected-line-fiber-loss] [high-fiber-
loss-minor-threshold] [high-fiber-loss-major-threshold]
```

4 Go to step 7.

NODE ESSENTIALS STEPS

5 From the **Topology** menu, click on the **Links** to display the Links grid.

6 Use the Row selector in the Links grid to select the link you want to display the information.

7 Confirm that the provisioned expected-line-fiber-loss, for a line span, or the actual-measured-loss on the other link types (fiber, logical) is as expected. Change the expected-line-fiber-loss if needed. Refer to *Equipment/Facility Provisioning and Protection*, 323-2051-310.

8

CAUTION
Risk of traffic loss
Only disconnect the fibers involved in the “High Fiber Loss” alarm. Disconnecting the fibers can impact traffic.

CAUTION
Risk of damage to modules
Wear an antistatic wrist strap to protect the equipment from static damage. Connect the wrist strap to the ESD jack on the shelf or module.

Check the fibers involved in the “High Fiber Loss” alarm (all fibers between the port where the alarm is raised and the port specified as the provisioned name on the “to” port of the link).

a. verify that the fibers are connected (fully inserted and clicked-in) and not crossed, looped back, or misconnected

b. check and clean any dirty fibers. Refer to *Optical Connector Inspection and Cleaning*, 323-1859-500.

c. confirm the provisioned “expected-line-fiber-loss” and edit if needed

d. If applicable, verify that the MPO cable for the subfiber that has the alarm and the far-end of the MPO cable are connected properly

9

If the subfiber adjacency has a far-end address that points to	**Then** go to
the same card	step 10
otherwise	step 13

10 Determine which MPO/LC loopback connector is used for the subfiber on the FIM.

11 Determine the far-end MPO adjacency from the local subfiber adjacency far-end address. Check that the MPO cable is connected properly. Determine the far-end of this MPO cable by looking at the MPO adjacency far-end address.

12 Check that the MPO cable is connected properly.

Copyright© 2019-2025 Ciena® Corporation

13 If the alarm does not clear 10 minutes after insertion of the fiber or the MPO/LC loopback connector, clean the cables.

> **CAUTION**
> **Risk of traffic loss**
> Ensure to switch any traffic that is on any of the other subfibers, away from the ROADM.

14 If the RLA or CCMD subfiber loopbacks to itself, clean the associated loopback connector at the FIM.

> **CAUTION**
> **Risk of traffic loss**
> Ensure to switch any traffic that is on the MPO cables. The traffic will be lost when you clean the cables.

15 If the alarm does not clear 10 minutes after insertion of the loopback connector, clean the MPO cables between the RLA (or CCMD) and the FIM on both ends.

16 If the RLA subfiber goes to another RLA or CCMD, clean the MPO cables between the RLA and the FIM or the MPO cables between the CCMD and the FIM. Clean the MPO cable of the newly installed circuit pack first.

17 Verify that the actual fibering matches the provisioned fibering.

18 If the alarm is raised on the CMD48, clean the jumper fibers on the dark fiber or the Manual loopback path fiber as follows.

> **CAUTION**
> **Risk of traffic loss**
> Ensure to switch traffic that is on any of the subfibers.

19 If the loss value is greater than the default value but below the maximum possible loss for either MPO logical links or logical link fiber type as specified in *6500 RLS Shelf Installation Guide*, 323-2051-201, then excess loss may need to be provisioned to compensate for the extra loss.

20 Excess Loss provisioning: if there are lossy elements (patch panels and multiple connectors are typical examples of lossy elements) between the two ports, the loss of the element itself should be provisioned in the Excess Loss field. Refer to *Equipment/Facility Provisioning and Protection*, 323-2051-310.

21 If the loss threshold was adjusted and the excess loss added where necessary and the alarm is still present, contact your next level of support or your Ciena support group.

22 For connections between a transponder Tx port and the CMD48 or CCMD8x24 Channel In port, verify that the derived total power on the Tx-proxy facility of the circuit pack has been copied to the transponder.

Copyright© 2019-2025 Ciena® Corporation

23 For CCMD8x24, verify the current power reported on the corresponding OTPMON facility of the channel-in port matches the provisioned Tx power on the transponder.

24 If the High Fiber Loss alarm is toggling and one of the modules (RLA, LRU or CCMD) has CV capability, then ensure at least 8x ports are defined under CV tx port-sequence or all ports from the CV port-sequence are removed that, in default, scans all ports. Port count lower than 8x can lead to transient alarms getting raised and cleared. See the example below.

Figure 11 Example of CV port sequence with port count < 8x

```
NODE01# show slots 1 config cv config tx
  slots:
  - name   : 1
    config:
      cv:
        config:
          tx:
            admin-state   : Enabled
            port-sequence:
            - port   : ciena-6500r-ports:port 21-3
            - port   : ciena-6500r-ports:port 21-4
            - port   : ciena-6500r-ports:port 21-5
            - port   : ciena-6500r-ports:port 21-6
```

NODE ESSENTIALS STEPS

25 Select **Facilities** from the Node Essentials navigation menu.

The Facilities menu opens.

26 From the **Equipment** grid, select the module which you want to check CV port sequence.

The bottom part of screen becomes populated.

27 Select Connection validation facility from Facility navigator.

The Connection validation details opens.

28 Browse Port Sequence for Tx or Rx in its details.

29 If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 53 High Temperature

Requirements

To perform this procedure, you must observe all safety requirements described in *6500 RLS Shelf Installation Guide*, 323-2051-201.

Probable cause

This alarm is raised against a slot when the recorded temperature is too high.

The following conditions can cause this alarm:

- The operating environment exceeds the temperature and/or altitude limits specified for the shelf. Refer to the “Operating specifications and standards compliance” section in *6500 RLS Planning Guide*, NTRN10WA.
- There are one or more empty slots in the shelf which must be equipped with modules or filler cards. Any “Circuit Pack Missing” alarms must be cleared first.
- The shelf cooling system is not functioning correctly. Any “Circuit Pack Failed” alarm against fan slot (51 or 52) must be cleared first.
- The shelf is operating without a cooling fan module equipped (for example, one or more fan modules are missing or not fully inserted).
- The air exhaust port or air inlet plenum is blocked.
- The air filter has a blockage.
- The shelf exhaust air is being trapped in an enclosed space or cabinet and is re-circulating into the air inlet plenum.
- Hot exhaust air from other equipment is mixing with the shelf's intake air.
- There is a problem with a module in the shelf.

Note: It may take some time for a shelf to cool off and the alarm to clear after the cause is corrected.

Impact

Critical, non-service-affecting (C, NSA)

Steps

1

DANGER
Risk of eye injury
Wear eye protection such as safety goggles or safety glasses with side guards when you work with fan modules, air filters or in proximity to the shelf air exhaust.

Copyright© 2019-2025 Ciena® Corporation

CAUTION
Risk of damage to modules
Do not attempt to cause this alarm to be raised by removing any cooling fan modules or filler cards or by blocking the shelf air inlet or exhaust ports as it will compromise shelf cooling. A shelf with a compromised cooling system may result in module failures prior to the assertion of a High Temperature Warning or High Temperature alarm.

Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.

2 Make sure that the shelf operating environment is within the specified temperature and altitude limits. Refer to the “Operating specifications and standards compliance” in *6500 RLS Planning Guide*, NTRN10WA.

3

If the operating temperature for the altitude is	**Then**
within the specified limits	go to step 4
not within the specified limits	correct the office temperature and go to step 8

4 Perform visual checks to ensure that the shelf air intake is not obstructed and that air is exhausting from each fan module or from the shelf's exhaust port as applicable. Verify the following:

- Make sure that there is clearance between the back of the shelf and any other shelf, wall, or obstruction.
- Inspect the grill at the air exhaust of the cooling unit or the grill integrated into the shelf cover/door, the grill on the cooling fan module, and the grill on the air inlet plenum. If any have an accumulation of dust, vacuum the grill.

5 Visually inspect the shelf to confirm that all slots are filled (including all modules and common equipment slots).

6

If the shelf has	**Then** go to
all slots filled	step 8
empty slots	step 7

7 Re-insert any missing module or install filler cards into any empty slots. Refer to the “Module replacement” procedures in this document.

8 Remove and inspect the shelf air filter and replace it with a new one if there is a visible accumulation of dust. Refer to the Procedure 149, “Replacing a shelf air filter in R2 or R4 shelf” procedure in this document.

Copyright© 2019-2025 Ciena® Corporation

9 Monitor the temperatures on the modules by retrieving the inventory and check whether the current temperature of all the supported modules decreases. If the temperature did not decrease even after ten minutes or if the CTM is still reporting a current temperature of 50 °C or greater, continue to the step 10.

Note: The “High Temperature” alarm automatically clears if the temperature drops to an appropriate level.

10 Replace the cooling fan module(s). Refer to the Procedure 148, “Replacing a shelf fan module” procedure in this document.

11 Monitor the temperatures on the cards by retrieving the inventory and check whether the current temperature of all the supported modules decreases. If the temperature did not decrease even after ten minutes or if the CTM is still reporting a current temperature of 50 °C or greater, go to step 12.

12 If the alarm does not clear, it could be due to a problem with a module. Contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 54 High Temperature Warning

Requirements

Observe all safety requirements described in *6500 RLS Shelf Installation Guide*, 323-2051-201.

Probable cause

This alarm is raised against the slot as a warning to the user when the recorded temperature is too high. The following conditions are applicable:

- The operating environment exceeds the temperature and/or altitude limits specified for the shelf. Refer to the “Operating specifications and standards compliance” in *6500 RLS Planning Guide*, NTRN10WA.
- There are one or more empty slots in the shelf which must be equipped with modules or filler cards. Any “Circuit Pack Missing” alarms must be cleared first.
- The shelf cooling system is not functioning correct. Any “Circuit Pack Failed” alarm against fan slot (51 or 52) must be cleared first.
- The shelf is operating without a cooling fan module equipped (one or more fan modules are missing or not fully inserted).
- The air exhaust port or air inlet plenum is blocked.
- The air filter has a blockage.
- The shelf exhaust air is being trapped in an enclosed space or cabinet and is re-circulating into the air inlet plenum.
- Hot exhaust air from other equipment is mixing with the shelf's intake air.
- There is a problem with a module in the shelf.

ATTENTION

If a high temperature warning condition prevails for a while, it could potentially lead to a “High Temperature” condition. Refer to Procedure 53, “High Temperature” for high temperature condition information.

The Raised temperature warning condition is cleared on a slot automatically if the temperature on these modules decreases to an acceptable level.

Impact

Major, non-service-affecting (M, NSA)

Copyright© 2019-2025 Ciena® Corporation

Steps

1

DANGER
Risk of eye injury
Wear eye protection such as safety goggles or safety glasses with side guards when you work with fan modules, air filters or in proximity to the shelf air exhaust.

CAUTION
Risk of damage to modules
Do not attempt to cause this alarm to be raised by removing any cooling fan modules or filler cards or by blocking the shelf air inlet or exhaust ports as it will compromise shelf cooling. A shelf with a compromised cooling system may result in module failures prior to the assertion of a High Temperature Warning or High Temperature alarm.

Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.

2 Temperature can be monitored through inventory retrieval, which displays the current and average temperature on the supported modules. Display the inventory information:

If you want to perform the procedure using	**Then** go to the
CLI commands	“CLI INTERFACE STEPS”
Node Essentials	“NODE ESSENTIALS STEPS”

CLI INTERFACE STEPS

3 To display the inventory information, enter the following command:

```
show slots inventory circuit-pack pec [c-type] [label]
[power...] [admin-state] [operational-state] [slot-type]
[type] [form-factor] [diagnostic...] [hardware-release]
[common-language-equipment-identifier] [serial-number]
[manufacturing-date] [age] [on-since] [current-
temperature] [average-temperature]
```

4 Go to step 6.

NODE ESSENTIALS STEPS

5 From the **Chassis** menu, select the slot that you want to display the information.

The inventory information for the chosen slot is displayed on right hand side the screen in the slot details.

6 Make sure that the shelf operating environment is within the specified temperature and altitude limits. Refer to the “Operating specifications and standards compliance” section in *6500 RLS Planning Guide*, NTRN10WA.

Copyright© 2019-2025 Ciena® Corporation

7

If the operating temperature for the altitude is	**Then**
within the specified limits	go to step 8
not within the specified limits	correct the office temperature and go to step 8

8 Perform visual checks to ensure that the shelf air intake is not obstructed and the air is exhausting from each fan module or from the shelf exhaust port as applicable. Verify the following:

- Make sure that there is clearance between the back of the shelf and any other shelf, wall, or obstruction.
- Inspect the grill at the air exhaust of the cooling unit or the grill integrated into the shelf cover/door, the grill on the cooling fan module, and the grill on the air inlet plenum. If any have an accumulation of dust, vacuum the grill.

9 Visually inspect the shelf to confirm that all slots are filled (including all module and common equipment slots).

10

If the shelf has	**Then** go to
all slots filled	step 12
empty slots	step 11

11 Re-insert any missing modules or install filler cards into any empty slots. Refer to the "Module replacement" procedures in this document.

12 Remove and inspect the shelf air filter and replace it with a new one if there is a visible accumulation of dust. Refer to the Procedure 149, "Replacing a shelf air filter in R2 or R4 shelf" procedure in this document.

13 Monitor the temperatures on the modules by retrieving the inventory and check whether the current temperature of all the supported modules decreases. If the temperature does not decrease after ten minutes, go to step 14. If the temperature falls to normal on all the supported modules wait for 6 minutes for the alarm to clear.

14

If the original alarm has	**Then**
cleared	the procedure is complete
not cleared, even after all the modules are at a normal temperature for more than six minutes	go to step 15

15 Replace the cooling fans module(s) Refer to the Procedure 148, "Replacing a shelf fan module" procedure in this document.

16 If the alarm does not clear, it could be due to a problem with a module. Contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 55 Incomplete Software Package Lineup

Requirements

To perform this procedure, you must use an account with at least an Admin user access level.

Probable cause

This alarm is raised when the committed software version on the NE is known but the release version is either not present or the package and uncompressed files are not complete on the NE.

This alarm can also be raised when an AP is replaced and the new AP is running a different software release than the active release on the network element.

Auto upgrade and cancel is not possible until the alarm is cleared.

Impact

Warning, non-service-affecting (W, NSA)

Steps

1. Retrieve the software release and upgrade information. Refer to “Retrieving software release and upgrade information” in *6500 RLS Licensing, Security, and Administration*, 323-2051-300.
2. Deliver the software release load with the committed version to repopulate the required release files by executing the following command:

   ```
   software-deliver uri <value>
   ```

   ```
   URI format to deliver the software load file stored
   remotely is: <sftp|scp>://
   <userid>:<password>@<host>[:port]/<directory path>/<RLS-
   xx.yy.zz.bbbb.tgz (where xx.yy.zz is the RLS release
   number and bbbb is the unique build number)
   ```
3. If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 56 Input Loss Of Signal

Requirements

To perform this procedure, you must:

- use an account with at least an Admin user access level
- observe all safety requirements described in *6500 RLS Shelf Installation Guide*, 323-2051-201
- have a network and site diagram
- have a fiber cleaning kit
- have the LOS threshold level for this amplifier

Probable cause

This alarm is raised against an AMP facility when the total input optical power to the amplifier has fallen below the provisioned input LOS threshold level.

The conditions that can cause the input power level to fall below the threshold level include:

- a disconnected fiber
- a dirty optical fiber connector at the receiver or adjacent transmitter
- a failure of the transmitting laser at the adjacent Tx
- a defective fiber optic patchcord
- a defective module
- an incorrect provisioned value
- a reflective event, indicated by an Automatic Power Reduction Active alarm at an upstream booster amplifier or pre-amplifier

This alarm can remain active after the fault has cleared and the original power level is restored. This occurs when the power level is lower than the user-provisioned LOS threshold plus the hysteresis value. The hysteresis value is not user provisionable and is set at 3 dB.

Impact

Major, service-affecting (M, NSA)

Steps

1 Check for and clear any active Optical Line Failed alarm.

2

If the original alarm has	**Then**
cleared	the procedure is complete
not cleared	go to step 3

Copyright© 2019-2025 Ciena® Corporation

3 Check for and clear any active Automatic Power Reduction Active alarm at the upstream booster amplifier or pre-amplifier that is providing output power to the alarmed amplifier.

4

If the original alarm has	**Then**
cleared	the procedure is complete
not cleared	repeat step 1 for each booster amplifier or pre-amplifier farther upstream from the alarmed amplifier. Then go to step 5.

5 Check for and clear any active Input Loss Of Signal alarms at the amplifiers farther upstream.

6 Repeat step 1 to step 5.

7 Verify the AMP facility parameters are correctly provisioned. If required, correct any discrepancies. Refer to *Equipment/Facility Provisioning and Protection*, 323-2051-310.

8

If the original alarm has	**Then**
cleared	the procedure is complete
not cleared	go to step 9

9 Place the admin state of the alarmed AMP facility to “Disabled”. Refer to the “Facilities” section in *Equipment/Facility Provisioning and Protection*, 323-2051-310.

10

CAUTION
Risk of laser radiation exposure
Do not look directly into the optical beam. Invisible light can severely damage your eyes.

CAUTION
Risk of damage to modules
Never disconnect an optical fiber that is connected to an active or powered up optical amplifier. To disconnect or reconnect an optical fiber, make sure the optical amplifier is “Disabled”, then disconnect or reconnect the fiber.

CAUTION
Risk of damage to modules
Wear an antistatic wrist strap to protect the equipment from static damage. Connect the wrist strap to the ESD jack on the shelf or module.

Clean and then reconnect the output fibers and connectors at the amplifier. Refer to *Optical Connector Inspection and Cleaning*, 323-1859-500.

Copyright© 2019-2025 Ciena® Corporation

11 Place the amplifier back “Enabled”. Refer to *Equipment/Facility Provisioning and Protection*, 323-2051-310.

12

If the original alarm has	**Then**
cleared	the procedure is complete
not cleared	go to step 13

13 Clear any upstream (either at the local to the network element reporting the alarm or other upstream remote network elements) alarms that could be causing this alarm, such as Circuit Pack Failed and Circuit Pack Missing.

If there are no upstream alarms, then verify the optical patchcord connected to the port reporting the alarm:

- ensure it is connected at both ends and that there is no problem with the optical patchcord
- clean the connectors.

14

If the original alarm has	**Then**
cleared	the procedure is complete
not cleared	go to step 15

15 Provision the **Input LOS Threshold** value for the AMP facility reporting the alarm to be 5 dB less than the current value. For example, if the **Input LOS Threshold** is -22 dB, change the value to -27 dB. Refer to *Equipment/Facility Provisioning and Protection*, 323-2051-310.

16 Wait at least one minute for the alarm to clear. Change the **Input LOS Threshold** value back to the original value.

17

If the original alarm has	**Then**
cleared	the procedure is complete
not cleared	go to step 18

18 Restart the module supporting the alarmed AMP facility. Refer to Procedure 5, “Restarting an interface module or the CTM” in this document.

19 If the alarm does not clear, gather the following diagnostic information and contact your next level of support or your Ciena support group. Refer to *6500 RLS CLI Reference*, 323-2051-190 for the CLI commands.

a. Amp config and inventory data raising the alarm

b. Immediate upstream power data

— Upstream amp config and inventory data (if upstream amp present)

— Upstream voa config and inventory data (if upstream voa present)

— Upstream pwrmon inventory data (e.g. line in/out ports)

— Upstream optmon inventory data facility (e.g. CCMD ch-in ports, RLA/LRU switch ports, SRA ports)

c. Preceding link data

d. other local alarms

Copyright© 2019-2025 Ciena® Corporation

e. upstream alarms

Copyright© 2019-2025 Ciena® Corporation

Procedure 57 Intercard Suspected

Requirements

To perform this procedure, you must:

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *6500 RLS Shelf Installation Guide*, 323-2051-201
- have an antistatic wrist strap to dissipate electrostatic charges
- If the alarm is raised against a pluggable module, obtain a supported pluggable module. Refer to “Ordering information” in *6500 RLS Planning Guide*, NTRN10WA.

Probable cause

This alarm is raised when a data path, control, or communications path fault is detected within the product, but the fault is unable to be isolated to a specific interface module or backplane. Because the fault cannot be isolated to a specific interface module, the alarm will be raised against more than one interface module. Examples are:

- An interface module that has a loss of traffic or degraded signal integrity on a backplane link which interfaces to another interface module in the shelf. The alarm would be raised against both interface modules.
- A communications bus (clock, parity, or interprocessor communication) failure between a CTM and an interface module. The alarm would be raised against the CTM and the other interface module. This could include Fans, PIMs, or the access panel.
- A fan module in an R8-300 shelf with one or more integrated fans running at maximum speed because the temperature is not being sensed from the access panel. The alarm would be raised against the fan module and the access panel.
- A PIM module with one or multiple modules. This could include CTM, FAN, interface module.
- A pluggable module that reports suspected communications bus failures. The fault may be on the module or on the pluggable module but the software is unable to determine exactly where the fault exists.

Impact

Critical, service-affecting (C, SA) alarm if raised on the CTM, IM, Fan, AP, or PIM and the module is currently active

Minor, non-service-affecting (MN, NSA) alarm if the module is not currently active, or if it is a Photonics interface module or an access panel

Copyright© 2019-2025 Ciena® Corporation

Critical, service-affecting (C, SA) alarm for an active pluggable module Minor, non-service-affecting (m, NSA) alarm for an inactive pluggable

The status of the circuit pack can be unknown because of the loss of communications. Additional failures can be service-affecting

Steps

1 Identify the interface module or pluggable raising the alarm.

If you want to perform the procedure using	**Then** go to the
CLI commands	step 2
Node Essentials	See the Node Essential steps in "Retrieving the data for the active alarm object" on page 32.

2 Identify the module raising the alarm, enter:

```
show active-alarm <id> [name] [resource] [raise-time]
[raise-time] [cause] [condition-type] [direction]
[location] [severity] [service-impact] [additional-info]
[user-notes...]
```

Refer to "Alarm parameters" on page 27 for applicable parameters.

3 Determine the time since the "Intercard Suspected" alarm was raised. It is recommended that modules are not restarted until at least 10 minutes after the "Intercard Suspected" alarm was raised so that data collection can complete for the fault, in case design investigation is required

4 If the alarm is raised on a module which has a red LED turned on, and that module has not been replaced within the past 48 hours or if the traffic is impacted, then replace the module. Refer to the appropriate module replacement procedure in "Module replacement" section in this document.

5 If the alarm persists after 10 minutes and that module has not been replaced within the past 48 hours, replace the module then contact your next level of support or your Ciena support group.

6 If the alarm is raised on any of the following combinations of modules, perform the actions identified below, until the alarm clears. After each step, if the alarm does not return after 10 minutes then the procedure is complete.

CAUTION
Risk of traffic loss
A cold restart on an unprotected module causes a traffic loss. A cold restart on an active protected module causes a protection switch that impacts traffic.

Copyright© 2019-2025 Ciena® Corporation

7

If the alarmed modules are	**Then**
One CTM and all interface modules, AP, Fan power input module	1- Ensure that alarmed CTM is seated properly. Refer to appropriate procedure in "Module replacement" section in this document. 2- Cold restart the alarmed CTM 3- Replace the alarmed CTM
One CTM, and Fan or Power Input Module	1- Ensure the alarmed CTM, Fan or Power Input Module are seated properly. Refer to appropriate procedure in "Module replacement" section in this document. 2- Cold restart the alarmed CTM 3- If the shelf has dual CTM, replace the CTM, otherwise. 4- Replace the Fan or Power Input Module 5- Replace the CTM when the shelf has single CTM.
Both CTM and AP, or Fan, or power input module, or Interface module	1- Ensure that alarmed CTM, AP, or Fan or power input module, or interface module are seated properly. Refer to appropriate procedure in the "Module replacement" section in this document. 2- Cold restart the active CTM 3- Cold restart the newly active CTM 4- Replace the alarmed AP, or Fan or power input module, or interface module 5- Replace the active CTM 6- Replace the newly active CTM
Two CTM only	1- Ensure that both alarmed CTM are seated properly. Refer to appropriate procedure in the "Module replacement" section in this document. 2- Cold restart the active CTM 3- Replace the original active CTM 4- Cold restart the newly active CTM 5- Replace the newly active CTM
Active CTM and access panel	1- Ensure that alarmed CTM and access panel are seated properly. Refer to appropriate procedure in the "Module replacement" section in this document 2- Cold restart active CTM 3- Replace access panel 4- Replace active CTM

Copyright© 2019-2025 Ciena® Corporation

If the alarmed modules are	**Then**
Inactive CTM and access panel	1- Ensure that alarmed CTM and access panel are seated properly. Refer to appropriate procedure in the "Module replacement" section in this document. 2- Cold restart inactive CTM 3- Replace inactive CTM 4- Replace access panel
One CTM and only one Interface module	1- Cold restart the alarmed Interface module 2- Replace the alarmed Interface module 3- Replace the alarmed CTM
one PIM and multiple modules	1- Ensure that alarmed PIM and other modules are seated properly. Refer to appropriate procedure in the "Module replacement" section in this document. 2- Replace the PIM 3-Replace the other alarmed modules
one PIM and one module	1- Ensure that alarmed PIM and the other module are seated properly. Refer to appropriate procedure in the "Module replacement" section in this document. 2- Replace the module 3- Replace the PIM
a fan module and an access panel	1- Ensure that alarmed fan module and access panel are seated properly. Refer to appropriate procedure in the "Module replacement" section in this document. 2- Replace the access panel 3- Replace the fan module

Copyright© 2019-2025 Ciena® Corporation

If the alarmed modules are	**Then**
a pluggable and an interface module	1- Ensure that alarmed pluggable module and the interface module are seated properly. Refer to appropriate procedure in the "Module replacement" section in this document. 2-Perform a cold restart on the interface module 3- If the alarm persists after 10 minutes, replace the pluggable module
a pluggable and an access panel	1- Ensure that alarmed pluggable module and the access panel are seated properly. Refer to appropriate procedure in the "Module replacement" section in this document. 2- Perform a cold restart on the active CTM 3- If the alarm persists after 10 minutes, replace the pluggable module

Note: Replace a module only if it has not been replaced within the past 48 hours. To replace a module, refer to the appropriate module replacement procedure in "Module replacement" section in this document.

8 If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 58 Internal Management Comms Suspected Fault

Requirements

To perform this procedure, you must:

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *6500-RLS Shelf Installation Guide*, 323-2051-201
- have an antistatic wrist strap to dissipate electrostatic charges

Probable cause

This alarm is raised when the communication channel failure between two modules is suspected. The alarm is raised against both modules suspected of being the cause of the failure.

Impact

Major

Steps

1 Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf

2 Identify the module raising the alarm.

If you want to perform the procedure using	**Then** go to the
CLI commands	step 3
Node Essentials	See the Node Essential steps in “Retrieving the data for the active alarm object” on page 32. Then go to step 4.

3 To identify the module raising the alarm using CLI commands, enter:

```
show active-alarm <id> [name] [resource] [raise-time]
[raise-time] [cause] [condition-type] [direction]
[location] [severity] [service-impact] [additional-info]
[user-notes...]
```

Refer to “Alarm parameters” on page 27 for applicable parameters.

4 Perform a warm restart on the module raising the alarm. Refer to Procedure 5, “Restarting an interface module or the CTM” in this document.

5

CAUTION
Risk of traffic loss
A cold restart on an unprotected module causes a traffic loss. A cold restart on an active protected module causes a protection switch that impacts traffic.

Copyright© 2019-2025 Ciena® Corporation

If the alarm does not clear, perform a cold restart on the alarmed module. Refer to Procedure 5, “Restarting an interface module or the CTM” in this document.

6. If the alarm is not clear, reseat one of the modules raising the alarm. Refer to the “Reseating a module” procedure in this document.
7. If the alarm is not clear, reseat the other module raising the alarm.
8. If the alarm is not cleared and the module has not replaced in the past 48 hours, replace the module. Refer to “Module replacement” on page 285.
9. If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 59 ISIS Level1/Level2 Adjacency Loss

Requirements

To perform this procedure, you must use an account with at least an Admin user access level.

Probable cause

This alarm is raised when ISIS is enabled on an interface and there is no ISIS neighbor reachable or passing Exchange state on that interface.

Impact

Minor, non-service-affecting (m, NSA)

Steps

1. Ensure that at least one of the ISIS neighbors is reachable or passing Exchange state on the interface.
2. If the alarm does not clear and you are certain this ISIS neighbor is no longer needed, delete the ISIS on the interface to clear the alarm. Refer to *OAM Communications*, 323-2051-101 for the commands and instructions.
3. If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 60 Lan Port Down

Requirements

To perform this procedure, you must use an account with at least an Admin user access level.

Probable cause

This alarm is raised when a LAN port on the access panel does not receive any Ethernet packets. This occurs if there is a bad Ethernet connection, or the LAN port fails.

Impact

Minor, non-service-affecting (m, NSA)

Steps

1. Check the DCN information to determine if the appropriate LAN port must be enabled.
2. Select your next step.

If the LAN port must be	**Then** go to
disabled	step 3
enabled	step 4

3. Disable the appropriate LAN port.
4. Check that the LAN configuration at both ends of the link are the same.
5. If the configuration is different, edit the configuration as required.
6. At the local network element, retrieve all alarms to determine if the original alarm has cleared.
7. If the alarm is not clear, ensure that the appropriate cable is correctly connected to the required LAN port on the access panel or CTM.
8. If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 61 Latch Open

Requirements

To perform this procedure, you must:

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *6500 RLS Shelf Installation Guide*, 323-2051-201
- have an antistatic wrist strap to dissipate electrostatic charges

Probable cause

This alarm is raised when the locking lever is not fully closed on a module that is inserted into a slot, or the latch on the module is broken.

Impact

Minor, non-service-affecting (m, NSA)

Steps

1. Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
2. Identify the module raising the alarm.
3. Ensure that the module raising the alarm is pushed all the way into its slot, until the latches click into place.
4. If the module does not lock into place, remove the module and examine the connector at the back of the module. Look for bent pins or damage.

   ATTENTION
   Do not force to close the latches. If the latches do not close correctly, gently re-insert the module. If the module cannot be re-inserted, remove the module and go to the next step.

5. If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 62 License Violation

Probable cause

This alarm is raised against a shelf if it is using features that require licenses but is missing at least one license.

The alarm can be raised under the following conditions:

- license granted for a feature while shelf in licensing commissioning mode and therefore in arrears
- license granted for a feature as a pre-authorized feature license and therefore in arrears
- license granted for a feature as a strict feature license and subsequently the license was returned to license server/manager and not re-acquired due to a network communication error during a shelf configuration change or shelf reconfiguration and therefore in arrears
- license granted for a feature as a strict or pre-authorized feature license but loss of DCN connectivity with license server/manager resulted in the license being reclaimed by the license server/manager and given out to another shelf before connectivity issue was fixed and therefore in arrears.
- the shelf current date and time is incorrect. For example, the current set system time is away from one or more license(s) start and/or expiry date limits.

The shelf tracks only a count of items licensed and then raises the “License Violation” alarm when the total number of licenses acquired do not equal the total number of licensed elements.

To clear this alarm, a licensing server needs to be provisioned and the shelf needs to be able to communicate properly with the licensing server. The management of licenses on a network is part of networking planning. The correct amount of licenses need to be purchased and allocated for all the shelves on the network expecting to use features that require licensing.

> ***Note:*** When the NE is in commissioning state, an active “License Violation” alarm does not restrict any action (such as software upgrade) on the NE.

Impact

Major, non-service-affecting (M, NSA)

> ***Note:*** This alarm automatically clears when the licensing software retrieves the missing licenses from the license server/manager.

Copyright© 2019-2025 Ciena® Corporation

Steps

1. Determine the licenses that are causing the alarm. Look for licenses which have counts higher than 0 for their arrears value. Those are the licenses and the counts that are required to clear the alarm. Refer to in *Licensing, Security, and Administration*, 323-2051-300.
2. Query the configured license server for available counts:

If you want to perform the procedure using	**Then** go to the
CLI commands	"CLI INTERFACE STEPS"
Node Essentials	"NODE ESSENTIALS STEPS"

CLI INTERFACE STEPS

3. The following step is performed using CLI commands.

   `license-client-query-server-available-count`
4. Add the licenses to the license server/manager. The new licenses can be purchased and loaded onto the licensing server. Refer to "Downloading a license from the Ciena Portal to the RLS shelf" procedure in *6500 RLS Licensing, Security, and Administration*, 323-2051-300 Go to step 7.

NODE ESSENTIALS STEPS

5. From the Node Essentials navigation menu, select **Configuration->License page**.

   The License files and license server details appear in the licence information grid.
6. Add licenses to the license server/manager by clicking on the "+" sign on top of the License servers grid.
7. Once the licenses are present on the license server/manager, operate License Audit manually.

   The alarm will also clear after the daily License Audit that occurs nightly (default 3 am).
8. If the alarm is not clear, manually set the shelf date and time to the current local date and time, or provision an external NTP server. Refer to "Retrieving and provisioning the NE time zone, date, and time" procedure in *6500 RLS Licensing, Security, and Administration*, 323-2051-300
9. If the alarm does not clear, contact your next level of support or Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 63 Link Down

Requirements

To perform this procedure, you must:

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *6500 RLS Shelf Installation Guide*, 323-2051-201
- have an antistatic wrist strap to dissipate electrostatic charges
- have the fiber connection information (that is, how the optical modules on each network element connect to other network elements)
- use an account with at least an Admin user access level

Probable cause

This alarm is raised against a COLAN, ILAN or OSC interface when a fiber is disconnected from the port, or a fault on the interface is detected.

The alarm is masked when interface is set to “disabled” and is raised when the interface is changed from “disabled” to “enabled”.

Impact

Minor, non-service-affecting (m, NSA)

Steps

1. Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
2. Ensure that the fibers between the subtending equipment and the COLAN, ILAN or OSC port are properly connected and are not damaged.
3. Ensure that the subtending client equipment is correctly provisioned, functioning, and transmitting a valid signal.
4. If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 64 Lockout Active

Requirements

To perform this procedure, you must use an account with at least an Admin user access level.

Probable cause

This alarm is raised on TPS when a user successfully operates a lockout protection switch.

Impact

Minor, non-service-affecting (m, NSA)

Steps

1. No action is required if a user is performing a test or maintenance operation. This alarm is a reminder not to leave a potentially service-affecting condition on the system.
2. The alarm clears when the user releases the lockout request. Release the indicated protection switch. Refer to the “Releasing a Manual switch, Forced switch, or Lockout” procedure in *Equipment/Facility Provisioning and Protection*, 323-2051-310.
3. If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 65 Lockout Active - Remote

Requirements

To perform this procedure, you must use an account with at least an Admin user access level.

Probable cause

This alarm is raised on TPS when a user successfully operates a lockout protection switch on the remote TPS.

Note: This alarm is only applicable for DCI TPS configurations.

Impact

Minor, non-service-affecting (m, NSA)

Steps

1. No action is required if a user is performing a test or maintenance operation. This alarm is a reminder not to leave a potentially service-affecting condition on the system.
2. The alarm clears when the user releases the lockout request on the remote TPS. Release the indicated protection switch. Refer to the “Releasing a Manual switch, Forced switch, or Lockout” procedure in *Equipment/Facility Provisioning and Protection*, 323-2051-310.
3. If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 66 Log Collection In Progress

Probable cause

This event is raised when a user invokes the log collection process.

Impact

Warning, non-service-affecting (W, NSA)

Steps

1. No action is required. The alarm clears when the log collection process is completed.
2. If the alarm is not clear or is unexpected, contact your next level of support or Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 67 Loopback Active - Facility

Requirements

To perform this procedure, you must use an account with at least an Admin user access level.

Probable cause

This alarm is raised when a facility loopback is active on the RLA/LRU.

Impact

Warning, non-service affecting (W, NSA)

Steps

1. If the alarm is raised during facility/connection testing, no action is required. The alarm clearS once the testing is complete and the loopback is released.
2. Release the loopback by deleting the mc/nmc-path objects or sparse discrete provisioning.
3. If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 68 Loss of Signal

Requirements

To perform this procedure, you must:

- use an account with at least an Admin user access level
- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation – 6500 RLS Shelf*, 323-2051-201
- have a network and site diagram
- have a fiber cleaning kit
- obtain a replacement module, if required

Probable cause

This alarm is raised against an OPTMON, PWRMON, OSC, VOA, or SRA Telemetry Rx facility when:

- the measured facility type optical power value has fallen below the provisioned LOS threshold level of the alarmed facility
- all line cards connected to the same passive Photonic Mux/Demux and subsequent cascaded Photonic Mux/Demux detected no input signal when shelf alarm correlation is turned on.

The conditions that can cause this alarm include:

- a disconnected, or defective fiber optic patchcord
- a dirty optical fiber connector
- a defective module (for instance, at an NE upstream from the location where the LOS alarm is raised locally)
- a provisioning error where the config admin-state of the facility is disabled on a module located at an upstream location
- defective transmitting subtending equipment
- a provisioning error in the LOS threshold of the alarmed facility
- Pilot Tone is in LOS
- LRU module has been added, provisioned, and fibered but recalibration augment-l-band has not yet been performed
- CCMD Tx port not tuned or tuned to wrong frequency
- Power is too low
- CCMD Tx blanking is on
- Tx is connected to the wrong port

Copyright© 2019-2025 Ciena® Corporation

- Fiber misconnected/disconnected between CCMD and RLA/RLU (switch In port)
- Fiber misconnected/disconnected between RLA/RLU and CCMD (common In port)
- Low Optical Power

This alarm can remain active after the fault has cleared and the original power level is restored. This occurs when the power level is lower than the user-provisioned LOS threshold plus the hysteresis value. The hysteresis value is not user provisionable and is set at 3 dB.

Impact

Major, service-affecting (M, SA)

Steps

1 This condition may be caused by an upstream fault. Before following this procedure, check for and clear any upstream alarms. A non-exhaustive list includes for example, Circuit Pack Missing, Circuit Pack Fail, Hardware Subsystem Failure or Software Subsystem Failure.

2 Check for and clear any of the following alarms before clearing this alarm. These alarms are related to optical power being interrupted due to reasons such as a fiber-cut , fiber-pinch, or fiber-degradation in the span, or within the ROADM mux-demux structure:

- Automatic Power Reduction Active
- Automatic Shutoff
- Input Loss Of Signal
- Optical Line Failed
- Shutoff Threshold Crossed

3 If LRU module has been added, provisioned, and fibered, perform the recalibration augment-l-band if it has not yet been performed. Note that LRUs must be physically equipped, provisioned and fibered at both ends of the link before attempting to recalibrate augment-l-band.

4 Verify that the OPTMON, OSC, VOA, or SRA Telemetry Rx facility parameters are provisioned correctly. If necessary, correct any discrepancies.

To display or edit the OPTMON facilities, refer to “Provisioning OPTMON facilities” procedure in *Equipment/Facility Provisioning and Protection*, 323-2051-310.

To display or edit VOA, facilities, refer to “Provisioning VOA facilities” procedure in to *Equipment/Facility Provisioning and Protection*, 323-2051-310.

To display or edit the OSC facilities, refer to “Provisioning OSC facilities” procedure in *Equipment/Facility Provisioning and Protection*, 323-2051-310.

Copyright© 2019-2025 Ciena® Corporation

5

If the alarm is raised against	**Then** go to
CCMD8x24, CCMD16 or RLA input port	step 6
SRA Telemetry Rx facility	step 10
DLM, DLA, DLE or RLA or TLM	step 15
any other port	step 14

6 Verify the optical patchcord between the subtending equipment and the CCMD8x24, CCMD16 or RLA.

- ensure it is connected at both ends and that there is no problem with the optical patchcord
- clean the connectors. Refer to *Optical Connector Inspection and Cleaning*, 323-1859-500.
- ensure the transmitting subtending equipment is functioning correctly and transmitting a valid signal

7

If the original alarm has	**Then**
cleared	the procedure is complete
not cleared	go to step 8

8 Verify the optical patchcord connected to the port reporting the alarm:

- ensure it is connected at both ends and that there is no problem with the optical patchcord
- clean the connectors. Refer to *Optical Connector Inspection and Cleaning*, 323-1859-500.

9

If the original alarm has	**Then**
cleared	the procedure is complete
not cleared	go to step 10

10 For the CCMD8x24, CCMD16 or RLA input port, compare the facility measurement value or PM untimed bin optical-power level to the LOS threshold. For the SRA Telemetry Rx facility, facility measurement value or PM untimed bin optical-power level to the LOS threshold. If the power level is greater than the threshold but by less than 3 dB, there is not enough power to clear the alarm hysteresis. Decrease the LOS threshold by 3 dB. Refer to the “Facilities” section in *6500 RLS Equipment/Facility Provisioning and Protection*, 323-2051-310.

Copyright© 2019-2025 Ciena® Corporation

11 If the alarm is related to the OSC facility, user can perform the following actions:

- If the remote OSC service is out of service and there is no transmit power by this remote side OSC SFP. User must verify the remote OSC admin state is not disabled and the Tx Power is up to the mark.
- If the remote OSC launch power (TargetPeakPower) is low, then user can verify that OSC VOA target peak power is provisioned and the target surveillance power is achieved.
- If the span length is high and received OSC signal power is still lower than the LOS provisioned, then user must verify that provisioned LOS threshold is not provisioned too low so that it cannot detect higher span length.

12 Wait at least one minute for the Loss Of Signal alarm to clear. Change the **LOS Threshold** value back to the original value.

13

If the original alarm has	**Then**
cleared	the procedure is complete
not cleared	go to step 14

14

If the alarm is raised against	**Then** go to
an unused DLM, DLA, DLE or RLA or TLM ingress port (the port with no adjacency provisioned)	step 15
any other port	step 16

15 Run another OTDR trace on the faulted DLM, DLA, DLE or RLA or TLM module. Refer to *Optical Control, SPLI, and OTDR*, 323-2051-318.

16 If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 69 Low Fiber Loss

Requirements

To perform this procedure, you must:

- use an account with at least an Admin user access level
- observe all safety requirements described in *6500 RLS Shelf Installation Guide,* 323-2051-201

Probable cause

This alarm is raised when the measured loss between near-end and the far-end is lower than the provisioned loss threshold because the span loss has improved beyond a defined threshold on a span compared to the expected fiber loss or if the provisioned expected line fiber loss is incorrect and too high (for example, more than 3.0 dB compared to the measured physical loss).

The alarm is raised when:

(Expected-physical-loss - measured-physical-loss) > low-fiber-loss-alarm-threshold

The alarm is cleared when:

(low_fiber_loss_threshold-low_fiber_loss_hysteresis) >= (expected_physical_loss - measured_physical_loss

Where the low-fiber-loss-alarm-threshold by default = 3 dB. A 0.5 dB hysteresis is also applied for the alarm to clear, which prevents the alarm from clearing until the measured loss has gone below the threshold(s) by more than 0.5 dB.

Note 1: The expected-physical-loss is system derived and must not be changed manually.

Note 2: This alarm is newly introduced in RLS release 3.1 and is Inhibited by default after an upgrade from a previous release. The user needs to explicitly enable the alarm, using changed-alarms.

Impact

Minor, non-service-affecting (m, NSA)

Steps

1 Verify the currently derived “expected-physical-loss” and compare it to the “measured-physical-loss” value shown in the response:

Copyright© 2019-2025 Ciena® Corporation

If you want to perform the procedure using	**Then** go to the
CLI commands	“CLI INTERFACE STEPS”
Node Essentials	“NODE ESSENTIALS STEPS”

CLI INTERFACE STEPS

2 To display the currently provisioned line fiber expected loss, enter the following command:

```
show link <name> [from] [to] [expected-line-fiber-loss]
[expected-physical-loss] [measured-physical-loss] [low-
fiber-loss-threshold]
```

3 Go to step 7.

NODE ESSENTIALS STEPS

4 From the **Topology** menu, click on the **Links** to display the Links grid.

5 Use the Row selector in the Links grid to select the link you want to display the information.

6 Using the right-most “Columns” selector, enable the Line fiber attributes -> Expected line fiber loss (dB). Refer to Photonic Links provisioning in *Optical Control, SPLI, and OTDR*, 323-2051-318.

7 Check for proper fiber connection to the expected port, then edit the “expected-line-fiber-loss” value as appropriate.

8 If the “expected-line-fiber-loss” value was adjusted and the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 70 Low Optical Return Loss

Requirements

To perform this procedure, you must:

- use an account with at least an Admin user access level
- observe all safety requirements described in *6500 RLS Shelf Installation Guide,* 323-2051-201
- have an antistatic wrist strap to dissipate electrostatic charges
- have the Engineering Documentation Package (EDP)
- have a fiber cleaning kit
- have a replacement module

Probable cause

This alarm is raised when the Optical Return Loss (ORL) drops below a fixed threshold.

Low ORL indicates high reflection at the amplifier output/Raman input and output, which can be caused by:

- dirty optical connectors
- improper optical cable mating
- a disconnected optical fiber at the amplifier
- an optical fiber cut
- a degraded optical fiber
- a disconnected or missing termination
- misprovisioning of an amplifier

Note: An upstream fiber cut in the path can cause a low Line OUT power and trigger a false Low ORL alarm. It is because the gap between output power and the reflected power on line out port is reduced. Hence a false Low ORL can get triggered even though the fibers are good.

For examples of ORL trouble clearing methods, refer to "Tracing and clearing the OTDR high reflection" on page 44.

Impact

Minor, non-service-affecting (m, NSA)

Steps

1 Choose your next step:

Copyright© 2019-2025 Ciena® Corporation

If the alarm	**Then**
is raised as a result of a maintenance activity or during SLAT and is expected	no action is required. The alarm will clear when the maintenance activity or SLAT is completed.
is unexpected	go to step 2

2

ATTENTION
Continuing with this procedure triggers Automatic Line Shut Off (ALSO) and will cause traffic loss in both directions.

DANGER
Risk of laser radiation exposure
Do not look directly into the optical beam. Invisible light can severely damage your eyes.

Identify the module raising the alarm, enter:

```
show active-alarm
```

Refer to "Alarm parameters" on page 27 for applicable parameters.

3 Check the alarmed amplifier power level defined in your EDP against the provisioned AMP facility parameter values. Edit the power level values as required. Refer to *Equipment/Facility Provisioning and Protection*, 323-2051-310.

4

If the original alarm has	**Then**
cleared	the procedure is complete
not cleared	go to step 5

5 If the alarmed amplifier is a pre-amplifier, ensure that all connectors located after the amplifier output are properly mated. Verify this on both ends of the connector-mating receptacles.

6 Ensure that the termination plugs are present and are mated properly on unused ports.

7

If the original alarm has	**Then**
cleared	the procedure is complete
not cleared	go to step 8

8

CAUTION
Risk of damage to modules
Never disconnect an optical fiber that is connected to an active or powered up optical amplifier. To disconnect or reconnect an optical fiber, make sure the optical amplifier is "Disabled", then disconnect or reconnect the fiber.

Copyright© 2019-2025 Ciena® Corporation

CAUTION
Risk of damage to modules
Wear an antistatic wrist strap to protect the equipment from static damage. Connect the wrist strap to the ESD jack on the shelf or module.

CAUTION
Risk of traffic loss
Only disconnect the output fiber of the alarmed optical amplifier. It is not necessary to disconnect any other output fibers, which could affect service. Disconnecting the Line B out fiber will impact traffic in both directions, as this triggers Automatic Line Shut Off (ALSO).

Disconnect the fiber of the alarmed optical amplifier, clean the fiber and connectors at the amplifier, then reconnect the fiber.

9 If the alarm is the result of a fiber cut, run an automatic office trace as part of go-no-go on the line out port to verify the back-reflection on both Raman or non-Raman fiber spans. If a single reflection is lower than 22 dB, the “OTDR High Reflection Detected” alarm is raised on the line out port to indicate the calibration may not succeed or the link may not perform as expected (degraded performance).

10 If the alarm does not clear, you may need to clean a specific connector or connectors that may not be immediately connected to the alarmed amplifier. For information on isolating connector losses, refer to “Locating a reflective event” on page 41.

11 If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 71 Low Optical Return Loss Input

Requirements

To perform this procedure, you must:

- use an account with at least an Admin user access level
- observe all safety requirements described in *6500 RLS Shelf Installation Guide*, 323-2051-201
- have an antistatic wrist strap to dissipate electrostatic charges
- have the Engineering Documentation Package (EDP)
- have a fiber cleaning kit
- have a replacement module

Probable cause

This alarm is raised against a RAMAN facility of an SRA circuit pack when the Optical Return Loss (ORL) at the input drops below a fixed threshold.

Low ORL indicates high reflection at the amplifier output/Raman input and output which can be caused by:

- dirty optical connectors
- improper optical cable mating
- a disconnected optical fiber at the amplifier
- an optical fiber cut
- a degraded optical fiber

For examples of ORL trouble clearing methods, refer to "Tracing and clearing the OTDR high reflection" on page 44.

Impact

Minor, non-service-affecting (m, NSA)

Steps

1 Change the admin state of the facilities to "Disabled" and check any upstream patch panel connectors at that site.

> **CAUTION**
> **Risk of traffic loss**
> The following steps will impact traffic. If possible, re-route the traffic to minimize the traffic loss.

Copyright© 2019-2025 Ciena® Corporation

ATTENTION
Continuing with this procedure triggers Automatic Line Shut Off (ALSO) and causes traffic loss in both directions.

DANGER
Risk of laser radiation exposure
Do not look directly into the optical beam. Invisible light can severely damage your eyes.

CAUTION
Risk of damage to modules
Never disconnect an optical fiber that is connected to an active or powered up optical amplifier. To disconnect or reconnect an optical fiber, make sure the optical amplifier is “Disabled”, then disconnect or reconnect the fiber.

CAUTION
Risk of damage to modules
Wear an antistatic wrist strap to protect the equipment from static damage. Connect the wrist strap to the ESD jack on the shelf or module.

CAUTION
Risk of traffic loss
Only disconnect the input fiber of the alarmed optical amplifier. It is not necessary to disconnect any other fibers, which could affect service. Disconnecting the Line B out fiber will impact traffic in both directions, as this triggers Automatic Line Shut Off (ALSO).

2 Choose your next step:

If you want to perform the procedure using	**Then** go to the
CLI commands	“CLI INTERFACE STEPS”
Node Essentials	“NODE ESSENTIALS STEPS”

CLI INTERFACE STEPS

3 To change the admin state of the facilities to “Disabled”, enter the following command:

```
set slots <slot #> config ramans LINE-IN admin-state
Disabled
```

4 Go to step 12.

NODE ESSENTIALS STEPS

5 Select **Facilities** from the Node Essentials navigation menu.

Copyright© 2019-2025 Ciena® Corporation

The Facilities menu opens.

6 From the **Equipment** grid, select the module with the alarmed RAMAN facility.

The bottom part of screen becomes populated.

7 Select RAMAN facility from Facility navigator.

The RAMAN Facilities grid opens.

8 Select the alarmed RAMAN facility by Row selector from the RAMAN Facilities grid.

9 Click the **Pencil** icon.

The related Edit dialog opens.

10 Edit the RAMAN facility as required.

Admin state: Disabled

11 Click **Confirm**.

12 Inspect and clean the input fiber/port between the SRA port 6 and the patchcord connected to the patch panel.

13 If the alarm does not clear, you may need to clean a specific connector or connectors that may not be immediately connected to the alarmed amplifier input. For information on isolating connector losses, complete Procedure 6, “Locating a reflective event”.

14 If the alarm does not clear, capture the OTDR Office and Short traces for the interconnected RLA/DLE/DLA input port (port 54 or port 64) by following the procedures in *Optical Control, SPLI, and OTDR*, 323-2051-318 document.

15 Open the OTDR traces (Office/Short) and inspect the Office and Short traces for any large reflections that were not captured by the OTDR alarms, possibly because of the pulse width/event spacing. If events are overlapping, re-run the trace using a smaller pulse by following the procedures in *Optical Control, SPLI, and OTDR*, 323-2051-318 document.

16 Perform the fiber/port/patch-panel cleaning procedure(s) on the event in question.

17 When cleaning the connection, a new go-nogo OTDR trace is triggered. Wait for the “local-otdr-in-progress” alarm to clear before reconnecting the fiber(s); this will initiate another go-nogo OTDR trace automatically.

18 Set the Raman Facility back to Enabled. If fault/failure persists, continue to next step otherwise the procedure is complete.

19 Contact your next level support to assist with conducting the attenuation introduction procedure (attenuator required) to isolate the source of the reflection.

20 If the alarm does not clear, gather the following diagnostic information and contact your next level of support or your Ciena support group. Refer to *6500 RLS CLI Reference*, 323-2051-190 for the CLI commands.

a. raman facility config and inventory data

b. SRA card optmon inventory data

Copyright© 2019-2025 Ciena® Corporation

c. Current OTDR Office traces

d. Adjacent amp config and inventory data

e. Pwrmon inventory data of adjacent RLA/DLx line port

f. Adjacent link data

g. Other local alarms

h. Upstream alarms

Copyright© 2019-2025 Ciena® Corporation

Procedure 72 Low Optical Return Loss Output

Requirements

To perform this procedure, you must:

- use an account with at least an Admin user access level
- observe all safety requirements described in *6500 RLS Shelf Installation Guide*, 323-2051-201
- have an antistatic wrist strap to dissipate electrostatic charges
- have the Engineering Documentation Package (EDP)
- have a fiber cleaning kit
- have a replacement module

Probable cause

This alarm is raised against a RAMAN facility of an SRA circuit pack when the Optical Return Loss (ORL) at the output drops below a fixed threshold.

Low ORL indicates high reflection at the amplifier output/Raman input and output which can be caused by:

- dirty optical connectors
- improper optical cable mating
- a disconnected optical fiber at the amplifier
- an optical fiber cut
- a degraded optical fiber
- express out ORL crosses below the low ORL threshold
- line IN power crosses above -5 dBm threshold

For examples of ORL trouble clearing methods, refer to “Tracing and clearing the OTDR high reflection” on page 44.

Impact

Minor, non-service-affecting (m, NSA)

Steps

1 Change the admin state of the facilities to “Disabled” and check any upstream patch panel connectors at that site.

> **CAUTION**
> **Risk of traffic loss**
> The following steps will impact traffic. If possible, re-route the traffic to minimize the traffic loss.

Copyright© 2019-2025 Ciena® Corporation

ATTENTION
Continuing with this procedure triggers Automatic Line Shut Off (ALSO) and causes traffic loss in both directions.

DANGER
Risk of laser radiation exposure
Do not look directly into the optical beam. Invisible light can severely damage your eyes.

CAUTION
Risk of damage to modules
Never disconnect an optical fiber that is connected to an active or powered up optical amplifier. To disconnect or reconnect an optical fiber, make sure the optical amplifier is “Disabled”, then disconnect or reconnect the fiber.

CAUTION
Risk of damage to modules
Wear an antistatic wrist strap to protect the equipment from static damage. Connect the wrist strap to the ESD jack on the shelf or module.

CAUTION
Risk of traffic loss
Only disconnect the output fiber of the alarmed optical amplifier. It is not necessary to disconnect any other fibers, which could affect service. Disconnecting the Line B out fiber will impact traffic in both directions, as this triggers Automatic Line Shut Off (ALSO).

2 Choose your next step:

If you want to perform the procedure using	**Then** go to the
CLI commands	“CLI INTERFACE STEPS”
Node Essentials	“NODE ESSENTIALS STEPS”

CLI INTERFACE STEPS

3 To change the admin state of the facilities to “Disabled”, enter the following command:

```
set slots <slot #> config ramans LINE-IN admin-state
Disabled
```

4 Go to step 12.

NODE ESSENTIALS STEPS

5 Select **Facilities** from the Node Essentials navigation menu.

Copyright© 2019-2025 Ciena® Corporation

The Facilities menu opens.

6 From the **Equipment** grid, select the module with the alarmed RAMAN facility.

The bottom part of screen becomes populated.

7 Select RAMAN facility from Facility navigator.

The RAMAN Facilities grid opens.

8 Select the alarmed RAMAN facility by Row selector from the RAMAN Facilities grid.

9 Click the **Pencil** icon.

The related Edit dialog opens.

10 Edit the RAMAN facility as required.

Admin state: Disabled

11 Click **Confirm**.

12 Inspect and clean the input fiber/port between the SRA port 6 and the patchcord connected to the patch panel.

13 If the alarm does not clear, you may need to clean a specific connector or connectors that may not be immediately connected to the alarmed amplifier input. For information on isolating connector losses, complete Procedure 6, “Locating a reflective event”.

14 If the alarm does not clear, capture the OTDR Office and Short traces for the interconnected RLA/DLE/DLA input port (port 54 or port 64) by following the procedures in *Optical Control, SPLI, and OTDR*, 323-2051-318 document.

15 Open the OTDR traces (Office/Short) and inspect the Office and Short traces for any large reflections that were not captured by the OTDR alarms, possibly because of the pulse width/event spacing. If events are overlapping, re-run the trace using a smaller pulse by following the procedures in *Optical Control, SPLI, and OTDR*, 323-2051-318 document.

16 Perform the fiber/port/patch-panel cleaning procedure(s) on the event in question.

17 When cleaning the connection, a new go-nogo OTDR trace will be triggered. Wait for the “local-otdr-in-progress” alarm to clear before reconnecting the fiber(s). This will initiate another go-nogo OTDR trace automatically.

18 Set the Raman facility back to Enabled. If the “low-optical-return-loss-output” alarm has cleared then the procedure is complete, otherwise continue to the next step.

19 Contact your next level support to assist with conducting the attenuation introduction procedure (attenuator required) to isolate the source of the reflection.

20 If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 73 Low Voltage

Requirements

To perform this procedure, you must:

- observe all safety requirements described in *6500 RLS Shelf Installation Guide,* 323-2051-201
- have an antistatic wrist strap to dissipate electrostatic charges
- have a standard multimeter
- have a spare Power Input Module (PIM) to replace each PIM in the shelf

You do not have to replace each PIM with a new PIM. Use a single spare PIM of the correct type to replace each PIM in turn.

Probable cause

This alarm is raised against the shelf equipped with DC Power Input Modules when a power brownout occurs because the DC battery voltage to the shelf drops below a minimum level. To determine the power requirement of the shelf, refer to “Power and grounding specifications” section in *6500 RLS Planning Guide*, NTRN10WA.

The difference (hysteresis) in the detection and recovery voltages makes it possible for the battery voltage to drop below the brownout voltage on multiple occasions without causing the circuit packs to restart each time.

A power brownout can occur at different voltages for different circuit packs.

Impact

Major, non-service affecting (M, NSA)

Steps

1 Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.

2 In the R2 or R4 shelf, the PIMs are located on the rear of the shelf. The status of the module is indicated by the LEDs on the Access Panel “Rear Alarm” LED. A “Rear Alarm” red LED indicates if there are any alarms against the shelf fan modules and/or PIMs. If the LED is lit requiring the user to service the rear of the shelf to clear the alarm.

3 At the shelf faceplate, identify any PIM with “Power OK” LED that is not illuminated. If power is not reaching the system through the PIM (due to a tripped breaker or externally disconnected power feed), the “Power OK” LED on the faceplate of the PIM is off. Refer to the “Power Failure Fault” procedure to clear the power fault to any PIM without an illuminated “Power OK” LED first. A PIM with a “Power OK” LED that is still is illuminated may still be supplying power to the system.

Copyright© 2019-2025 Ciena® Corporation

4 Use your company procedure to measure the DC voltage of the power feeds to each PIM using a multimeter. Make sure that both feeds are the correct polarity and that the voltage is in the expected voltage range (-43.5 to -75 Vdc between the L+ return reference and L- power feed or equivalently 43.5 to 75 Vdc between the L- power feed and L+ return).

> **CAUTION**
> **Risk of traffic loss**
> Do not reseat any circuit pack while this alarm is active. Unexpected problem conditions result when a circuit pack is reseated.

If	Then
both DC feeds are within the operating voltage range and the polarity is correct	go to step 5
one or both of the DC feeds are between 0V and -43.5 Vdc	use your company procedures to investigate and correct the fault in the power distribution system. Go to step 5.

5 If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 74 MAA Dropped From Area

Requirements

To perform this procedure, you must have the network plan.

Probable cause

This alarm is raised when a provisioned manual area address is dropped from the computed area address set of the network.

Impact

Major, non-service-affecting (M, NSA)

Steps

1. Log into one of the network elements in the system to determine the manual area addresses provisioned in the network.
2. Query all area addresses and record the list of addresses in the computed set.
3. Determine if the area addresses belong in the network by referring to the network plan:

If the dropped area address	**Then**
belongs in the network	contact your next level of support or Ciena support group.
does not belong in the network	go to step 4.

4. Log into the network element where the manual area address(es) that is not configured properly, is provisioned.
5. Delete the manual area address that does not belong in the network.
6. Repeat step 4 and step 5 to delete each manual area address that is not configured properly.
7. If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 75 Manual Switch Active

Requirements

To perform this procedure, you must use an account with at least an Admin user access level.

Probable cause

This alarm is raised when a user successfully operates a manual switch on a protected configuration with “revertive” set to True. This alarm is cleared when the user releases the manual switch, or when a higher priority request overrides it.

> ***Note:*** This alarm is not applicable if the protected configuration with “revertive” is set to False.

Impact

Minor, non-service-affecting (m, NSA)

Steps

1. No action is required if a user is performing a test or maintenance operation. This alarm is a reminder not to leave a potentially service-affecting condition on the system.
2. Release the indicated protection switch. Refer to *Equipment/Facility Provisioning and Protection*, 323-2051-310.
3. If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 76 Neighbor Mismatch

Requirements

To perform this procedure, you must use an account with at least an Admin user access level.

Probable cause

This alarm indicates a difference between the expected downstream neighbor in a functional-group (DOWNSTR-PFG-NEIGHBOR) and the discovered downstream neighbor (DISC-DOWNSTR-PFG-NEIGHBOR).

DOWNSTR-PFG-NEIGHBOR is an optional parameter configured by the user based on the deployment plan.

DISC-DOWNSTR-PFG-NEIGHBOR is populated when the LLDP neighbors are discovered on the OSC interfaces and communications to the downstream neighbor are available.

Impact

Major, non-service-affecting (M, NSA)

Steps

1. Verify that the DOWNSTR-PFG-NEIGHBOR is provisioned correctly. Enter the following command to verify both the provisioned and discovered PFG Neighbor.

   ```
   show functional-group <PFG-name> | grep -A1 DOWNSTR
   ```

2. For a LINE-AMP functional-group, this alarm may indicate that the fibers connected to Line-1 and Line-2 are swapped. Check that the discovered LLDP neighbor on the LINEINOSC of the functional-group is correct.
3. If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 77 Node Unreachable

Requirements

To perform this procedure, you must use an account with at least an Admin user access level.

Probable cause

This alarm is raised when the local end RLS is unable to communicate with the remote RLS or Platform node(s).

This alarm is also raised when:

- The Comms are down and no SPLI message is received within 20 minutes.
- Remote shelf is constantly restarting.
- Restarting a remote shelf one time and the system is restoring slowly, and connectivity is not restored for more than two minutes. The alarm will not raise if the system is recovered fast and the connectivity is restored after the CTM restart within one minute.
- The SiteId/SiteGroup or TID/nodeName on the remote shelf is changed without changing it on the RLS neighbor list.
- Unreachable IP address is provisioned in the neighbor list.
- External IP address is provisioned instead of internal IP address in the neighbor list.
- IPV4+IPV6 is provisioned on one end of link and far end only has IPV6 provisioned. Show nodes is selecting IPV4 IP not IPV6 causing the alarm to be raised.

Note: For SPLI, the “Node Unreachable” alarm will not re-raise until 20 minutes after a CTM cold restart. If you perform a cold restart on an active CTM, you must wait 20 minutes to confirm that the alarm is cleared. Also, the alarm will only be raised after the RLS and Platform shelf have previously reached a “reliable” connection-state.

Impact

Major, non-service-affecting (M, NSA)

ATTENTION

This alarm does not impact traffic instantly, but it leaves the network in the compromised state. Therefore, this alarm must be resolved immediately to avoid service-impact due to subsequent faults or calibration actions. This alarm generally compromises OMS communication and local span controller operations.

Copyright© 2019-2025 Ciena® Corporation

Steps

1. Check the “additional-info” field for all the remote nodes that are currently unreachable. There is always a single “Node Unreachable” alarm, but there can be more “unreachable” nodes.
2. Check the node-type of the “unreachable” nodes using “show nodes” CLI command.
3. Perform “show nodes” from CLI to check the node operations status under specific nodes diagnostic container.

   ```
   show nodes <node-name> diagnostic
   ```

4. If there are “unreachable” nodes that have node-type of section (amp sites or section tail), then check all nodes in the section for OSC alarms (loss-of-frame or Optical Line Fail). Follow the alarm clearing procedure for those alarms to clear this alarm.
5. Verify the provisioned OSPF Area of the local alarmed node and its OSC neighbor. Correct the OSC OSPF area if needed using the EDP document. Refer to *OAM Communications*, 323-2051-101for more information.
6. If there are “unreachable” nodes that have node-type of site (connected using ILAN) then check the ILAN interface for alarms and clear any alarms on the ILAN interface.
7. Ensure both shelves use the same protocol (IPv4 requires IPv4 addresses on both nodes, IPv6 requires IPv6 addresses on both nodes). If there are mix IPv scenarios, delete IPv4, or IPv6 on one shelf depending what is provisioned on the other shelf. The comms requirement is that networks must use either IPv4 only, IPv6 only, or IPv4+IPv6. Refer to *OAM Communications*, 323-2051-101 for more information.
8. If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 78 NTP Time Offset Exceeded

Requirements

To perform this procedure, you must use an account with at least an Admin user access level.

Probable cause

This alarm is raised when the time difference between the NTP server and the local clock exceeds 1000 seconds.

Impact

Minor, non-service-affecting (m, NSA)

Steps

1. Issue the following CLI command:

   ```
   force-ntp-sync confirm ntp-restart
   ```

   Note: There is no equivalent Node Essentials menu items of this command in this release.

2. If the alarm does not clear, then issue the following CLI command to identify those network NTP servers which has offset value greater than "1000000000" nanoseconds (“1000” seconds) or less than “-1000000000” nanoseconds.

   ```
   show openconfig-system:system ntp servers
   ```

3. Validate the network NTP servers, as identified in the previous command.
4. If the network NTP servers are working as expected, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 79 NTP Server Not Provisioned

Requirements

To perform this procedure, you must use an account with at least an Admin user access level.

Probable cause

This alarm is raised when NTP configuration is enabled but the NTP server is not provisioned.

Impact

Minor, non-Service affecting (m, NSA)

Steps

1. Provision the NTP server that is causing the alarm to raise. Refer to "Displaying and configuring the NTP server parameters" on *OAM Communications*, 323-2051-101.
2. If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 80 NTP Server Unreachable

Requirements

To perform this procedure, you must use an account with at least an Admin user access level.

Probable cause

This alarm is raised with “Minor” severity when:

- NTP is configured and enabled and at least one NTP server is configured and all configured NTP servers are unreachableThis alarm is raised with “Warning” severity when:NTP is configured and enabled andat least one NTP server is unreachable andnot all of the configured NTP servers are unreachable

NTP Audit Procedure

The Network Time Protocol (NTP) audit procedure is designed to monitor the status of the NTP servers and raises an alarm when specific conditions are met. This feature has two severities: Warning and Minor. The Warning alarm is raised when at least one NTP server is not reachable, but not all. The Minor alarm is raised when all NTP servers are not reachable.

The NTP audit procedure is performed every 6 minutes, triggered by the application of NTP configuration changes or the last modification made.

To gather the necessary data for alarm calculation, a custom periodic NTP audit mechanism has been implemented. This mechanism invokes the “ntpq” utility program, enabling communication with 'ntpd' (standard NTPD program) or ‘chronyd’ to retrieve relevant information.

The retrieved data is processed to determine if any NTP alarms should be raised or cleared based on predefined thresholds and conditions.

The additional-info field in this alarm is used to display the IP addresses of all the unreachable NTP servers, and in case if the display string exceeds 126 characters in length then the display string is truncated.

NTPD Program Behavior

The behavior of the NTPD program in Linux differs from the standard NTPv4 RFC recommendations. Understanding its behavior is crucial for alarm monitoring.

Upon startup, the NTPD program polls the NTP server every 64 seconds. This polling interval gradually increases from 64 seconds (~1 minute) to 1024 seconds (~17 minutes).

Copyright© 2019-2025 Ciena® Corporation

Example 1: If the NTP server becomes unreachable when the polling interval is approximately 1 minute, it takes 8 consecutive failed polls (approximately 8 minutes) for the NTP program to declare the server unreachable.

Example 2: If the NTP server becomes unreachable when the system is stable and the polling interval is at 17 minutes, the NTP program takes about 39 minutes to decide the server's reachability, contrary to the expected (~17 minutes * 8) ~136 minutes

Transient Alarms Suppression
To avoid transient alarms during system restarts or initial provisioning, a 7-minute hold-off time has been implemented. This hold-off time prevents alarms from being raised during the provisioning process until the changes take effect.

This alarm is raised between 6 minutes and 45 minutes when the NTP server becomes unreachable and clears between 6 minutes and 17 minutes when the NTP server becomes reachable again.

Impact

Minor, non-service-affecting (m, NSA)

Warning, non-service-affecting (W, NSA)

Steps

1. Ensure that at least one of the provisioned NTP servers is reachable over the network. Use ping and other troubleshooting methods as required.
2. Use a “ntpq -p” command from the alarmed node to the NTP IPs to highlight which server(s) are reachable.
3. Disable the NTP server if it is an older/no longer pertinent server that is causing the alarm to raise. Refer to “Displaying and configuring the NTP server parameters” on *OAM Communications*, 323-2051-101.
4. If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 81 Optical Line Failed

Requirements

To perform this procedure, you must:

- log into the CLI of the nodes with an Admin or higher user access level. For login information, see “Accessing and logging in to a network element” procedure in *Licensing, Security, and Administration*, 323-2051-300.
- observe all safety requirements described in *6500 RLS Shelf Installation Guide,* 323-2051-201
- have an antistatic wrist strap to dissipate electrostatic charges
- have a fiber cleaning kit
- have a power meter and a power source

Probable cause

This alarm is usually raised when there is a fiber break or an intermediate connector disconnect between neighboring sites. The alarm is raised against OPTMON and AMP facilities optically downstream of the fiber cut/disconnect.

The Optical Line Failure condition invokes “Automatic Line ShutOff” (ALSO), which is a regulatory safety requirement that automatically shuts down the amplifier optically upstream of the cut/disconnect and in the opposite direction. The “Automatic Shutoff” alarm is also present.

Whether one or both fiber directions have been cut will depend on whether one or two OLF alarms are present across the fiber span.

Note: This alarm masks the “Node Unreachable” and “Neighbor Mismatch” alarms.

CAUTION

Risk of radiation exposure

If light is used to test the broken fiber (for example, with a light source or an OTDR), certain Automatic Line Shut Off (ALSO) and Input Loss Of Signal alarms can clear. When the shelf detects light, the alarms clear and the amplifier facility is powered up. This is an expected behavior because a shelf cannot distinguish between a light source from an optical test set and a light source from a shelf.

Ensure the adjacent optical amplifiers are “Disabled” when performing fiber repairs. If an SRA span, also ensure any Raman amplifiers are “Disabled” as well.

Impact

Major, service-affecting (M, SA)

Copyright© 2019-2025 Ciena® Corporation

Steps

1

> **CAUTION**
> **Risk of laser radiation exposure**
> Do not look directly into the optical beam. Invisible light can severely damage your eyes.

> **CAUTION**
> **Risk of damage to modules**
> Never disconnect an optical fiber that is connected to an active or powered-up optical amplifier. To disconnect or reconnect an optical fiber, ensure the optical amplifier is “Disabled”, then disconnect or reconnect the fiber.

> **CAUTION**
> **Risk of damage to modules**
> Wear an antistatic wrist strap to protect the equipment from static damage. Connect the wrist strap to the ESD jack on the shelf or module.

For the node with the Optical line Failed alarm (the downstream node), select the interface module with the AMP facility showing the associated “Automatic Shutoff” alarm.

In addition, if applicable select the SRA interface module with the RAMAN facility showing the associated “Automatic Shutoff” alarm.

Manually disabling the required facilities in the opposite direction

2 Change the admin state of the specific AMP facility showing the “Automatic Shutoff” alarm to “Disabled”. In addition, if the OLF alarm is raised in an SRA span, change the admin-state of the specific RAMAN Line-In port facility showing the “Automatic Shutoff” alarm to “Disabled”.

CLI INTERFACE STEPS

3 To change the admin state of the facilities to “Disabled”, enter one of the following commands:

for RLA/DLA/DLM/TLM:

```
set slots <name> config amps <name> [admin-state
<Disabled>]
```

for DLE:

```
set slots <name> config dgff <name> fac amps <name>
[admin-state <Enabled|Disabled>]
```

for SRA:

```
set slots <name> config ramans LINE-IN admin-state
Disabled
```


Copyright© 2019-2025 Ciena® Corporation

There is no Node Essentials equivalent for this release.

Determining the neighboring node

4 Select the module that has the OLF alarm (if the OLF is raised against an OPTMON facility, then this will be a different module than selected in step 1).

Manually disabling the required facilities upstream

5 Log into the upstream node. Select the interface module with the amplifier module with the AMP facility showing the associated “Automatic Shutoff” alarm. In addition, if applicable select the SRA interface module with the RAMAN Line-In port facility showing the associated “Automatic Shutoff” alarm.

6 Change the admin state of the specific AMP facility showing the “Automatic Shutoff” alarm to “Disabled”. In addition, if an SRA span, change the admin-state of the specific RAMAN Line-In port facility showing the “Automatic Shutoff” alarm to “Disabled”.

Note: In the case of a dual fiber cut (for example, both directions of the same span), there will also be an OLF alarm present on this node. In this case it is unnecessary to perform step 1 to step 6 again.

The amplifiers pumps (if present) across the affected span are now in a safe state to perform troubleshooting (that is, they will not re-enable during the troubleshooting process when an operator may be attempting to clean a fiber).

Locating the fiber fault

7 Select your next step.

If an	**Then** go to
OTDR is available	step 8
OTDR is not available	step 10

8 Locate the fiber break using the OTDR. This can be performed from the downstream node by connecting the OTDR to the fiber coming into the AMP in OLF, or from upstream by connecting the OTDR to the fiber coming from the AMP in Automatic Shutoff.

9 Select your next step.

If the OTDR indicates the break is at the	**Then**
mid span	end this procedure and contact the relevant operations group
near or far-end of the span	go to step 10

10 Check the fiber connection manually at the downstream node. At the downstream node, systematically clean each optical connection between the fiber plant egress / patch panel towards port of the AMP showing the OLF alarm. Replace any obviously damaged patchcords.

11 Use a separate power source and power meter to measure the loss between the fiber plant ingress and the input port of the AMP.

Copyright© 2019-2025 Ciena® Corporation

12 Check the fiber connections at the upstream node. At the upstream node, systematically clean each optical connection between port of the AMP showing the Automatic Shutoff alarm and the fiber plant ingress / patch panel. Replace any obviously damaged patchcords.

13 Use a separate power source and power meter to measure the loss between port of the AMP and the ingress of the fiber plant / patch panel.

14 Reconnect, replace, or repair the fiber.

15 For the AMP (and if applicable RAMAN) facilities in step 1 and step 6, change the admin state to “Enabled” using the same method. Refer to “Provisioning AMP facilities” procedure, and if applicable, “Provisioning RAMAN facilities” procedure in *Equipment/Facility Provisioning and Protection*, 323-2051-310.

Note: Under double fault scenarios in which there is an OSC facility failure in conjunction with the Optical Line Failure, the ALSO condition may not clear upon repair of the fiber. If the alarm does not clear, follow the troubleshooting guidelines in “Loss of Signal” alarm clearing procedure.

16 Select your next step.

If	Then
the alarm is cleared	the procedure is complete.
it this is an OSC link and the alarm has not cleared	contact your next level of support or your Ciena support group.
there is no OSC	go to step 17

17 At this point, “Optical Line Failed” and “Automatic Shut off” alarms are still active for both ends. Set the ALSO disable on the Pre-AMP (EDFA where the repaired span is coming in) at the end where the OLF alarm is raised.

```
disable-also resource <value> [timer <1-60>]
```

“Optical Line Failed” and “Automatic Shutoff” alarms will clear and “Shutoff Threshold Crossed” alarm may be raised. The ALSO feature can be disabled for an specific duration (5 Minutes). After that duration, if the system is not recovered, the card will go back to ALSO mode and the EDFA will be shut down and the alarms raised again.

The ALSO disable can be performed at the far end where the other “Optical Line Failed” alarm is raised.

18 If the fiber repair is performed correctly, the “Optical Line Failed” and “Automatic Shutoff” clears at the local site. The “Shutoff Threshold Crossed” alarm that was raised at the downstream site will also clear and the system recovers.

19 The ALSO feature can be re-enabled as follow:

```
disable-also resource <value> also-disabled false
```

20 If the alarm does not clear contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 82 Optical Power Degrade Low/High

Requirements

To perform this procedure, you must use an account with at least an Admin user access level.

Probable cause

This alarm is raised when the Optical Power is beyond the provisioned degrade-low/degrade-high thresholds:

— degrade low raised when measured power < degrade-low threshold

— degrade high raised when measured power > degrade-high threshold

On CCMD channel-input ports, the degrade-high/low thresholds will be automatically set at +/- 2dB of the expected total power at the port on channel addition. The user can change the thresholds after adding the channel, but on any future channel add on the port (including restoration), the thresholds will be reset to +/- 2dB.

On SSM customer-input ports, the pwrmon nmcmon degrade-high/low thresholds will be automatically set at channel addition as the expected channel power +/- the degrade-high/low-offset provisioned under the pwrmon nmcmon monitoring-thresholds.

The alarm masking behavior is as follows:

- “Optical Power Out of Range High” alarm masks the “Optical Power Degrade High” alarm.
- “Optical Power Out of Range Low” alarm masks “Optical Power Degrade Low” alarm.
- Low-optical-power (loss of signal) masks “Optical Power Out of Range Low” alarm.

Note: When you upgrade RLS from a pre-R2.4 release to a post-R2.4 release, you may need to manually re-provision the threshold values of the degrade-low and degrade-high parameters for channels on the Optmon ports. The provisioned threshold values of degrade-low and degrade-high are not converted correctly during the upgrade. Instead, the values revert to the default values of –66 (degrade-low) and +66 (degrade-high).

Impact

Minor, non-service affecting (m, NSA)

Steps

1 Identify the SNC raising the alarm:

Copyright© 2019-2025 Ciena® Corporation

If you want to perform the procedure using	**Then** go to
CLI commands	step 2
Node Essentials	See the Node Essential steps in "Retrieving the data for the active alarm object" on page 32. Then go to step 3.

2 To identify the module raising the alarm using CLI commands, enter:

```
show active-alarm <id> [name] [resource] [raise-time]
[raise-time] [cause] [condition-type] [direction]
[location] [severity] [service-impact] [additional-info]
[user-notes...]
```

3 Verify the power at the Tx to ensure the power is as provisioned.

4 Clear the root cause such as fiber pinch, actuator targets not correctly set, or upstream sources not achieving target for the specific use cases.

5 If the alarm is not clear, manually set the degrade to a higher value for the "Optical Power Degrade High" or a lower value for the "Optical Power Degrade Low" alarm.

6 Select your next step:

If the facility raising the alarm	**Then** go to
is an optmon	step 7
is pwrmon	step 13

7 To retrieve the inventory data, enter the following command.

```
show slots <SlotNum> inventory optmons <port>
```

Note: There is no Node Essentials equivalent command for this release.

8 To manually set the degrade to a higher value to clear the "Optical Power Degrade High" alarm, enter:

```
set slots <slots> config optmons <port> degrade-high
<value high enough >1dB to get out of hysteresis>
```

Note: There is no Node Essentials equivalent command for this release.

9 To manually set the degrade to a lower value to clear the "Optical Power Degrade Low" alarm, enter:

```
set slots <slots> config optmons <port> degrade-low
<value low enough >1dB to get out of hysteresis>
```

Note: There is no Node Essentials equivalent command for this release.

10 To retrieve the inventory data, enter the following command:

```
show slots <SlotNum> inventory pwrmon <PwrmonName>
```

11 To manually set the degrade to a higher value to clear "Optical Power Degrade High" alarm, enter:

```
set slots <SlotNum> config pwrmon <PwrmonName>
```


Copyright© 2019-2025 Ciena® Corporation

Note: New offset will be used to recalculate the alarm thresholds for all NMCs on the NMCMON.

12 To manually set the degrade to a lower value to clear “Optical Power Degrade Low” alarm, enter:

```
set slots <SlotNum> config pwrmon <PwrmonName>
```

Note: New offset will be used to recalculate the alarm thresholds for all NMCs on the NMCMON.

13 If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 83 Optical Power Out of Range Low/High

Requirements

To perform this procedure, you must use an account with at least an Admin user access level.

Probable cause

This alarm is raised when Optical Power is beyond the provisioned out-of-range-low/out-of-range-high thresholds:

- OOR low raised when measured power < out-of-range-low threshold
- OOR high raised when measured power > out-of-range-high threshold

The user can manually edit the OOR values but the following conditions must be satisfied:

- out-of-range-high > degrade-high
- out-of-range-low < degrade-low. Recommend to provision above low-pwr-threshold

The alarm masking behavior is as follows:

- “Optical Power Out of Range High” alarm masks the “Optical Power Degrade High” alarm.
- “Optical Power Out of Range Low” alarm masks “Optical Power Degrade Low” alarm.
- Low-optical-power (loss of signal) masks “Optical Power Out of Range Low” alarm.

Note: When you upgrade RLS from a pre-R2.4 release to a post-R2.4 release, you may need to manually re-provision the threshold values of the out-of-range-low and out-of-range-high parameters for channels on the Optmon ports. The provisioned threshold values of out-of-range-low and out-of-range-high are not converted correctly during the upgrade. Instead, the values revert to the default values of –66 (out-of-range-low) and +66 (out-of-range-high)

Impact

Major, Service affecting (M, SA)

Minor, None-Service affecting (m, NSA)

Steps

1 Identify the module raising the alarm:

Copyright© 2019-2025 Ciena® Corporation

If you want to perform the procedure using	**Then** go to
CLI commands	step 2
Node Essentials	See the Node Essential steps in "Retrieving the data for the active alarm object" on page 32. Then go to step 3.

2 to identify the module raising the alarm using CLI commands, enter:

```
show active-alarm <id> [name] [resource] [raise-time]
[raise-time] [cause] [condition-type] [direction]
[location] [severity] [service-impact] [additional-info]
[user-notes...]
```

3 Verify the power at the Tx to ensure the power is as provisioned.

4 Clear the root cause such as fiber pinch, actuator targets not correctly set, or upstream sources not achieving target for the specific use cases.

5 If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 84 OSPFv2 Adjacency Loss

Requirements

To perform this procedure, you must use an account with at least an Admin user access level.

Probable cause

This alarm is raised when OSPFv2 is enabled on an interface and there is no OSPFv2 neighbor reaching or passing Exchange state on that interface.

This alarm is masked by “LAN Port Failure” alarm on Access Panel ports or “LOS/LOF” alarms on the OSC.

This alarm is also raised when user restart an Active CTM, or warm/cold restart an IM circuit pack that is carrying OSPF traffic using its OSC interface.

Impact

Minor, non-service-affecting (m, NSA)

Steps

1. Ensure that at least one of the OSPFv2 neighbors is reaching or passing Exchange state on the interface. Refer to “Displaying OSPFv2/OSPFv3 diagnostics” procedure in *OAM Communications*, 323-2051-101 to determine the OSPF neighbor state.
2. If the alarm does not clear and you are certain that this OSPF neighbor is not required, delete the OSPFv2 on the interface. Then refer to “Configuring and deleting the OSPFv2 protocol” procedure in *OAM Communications*, 323-2051-101 to delete the OSPFv2.
3. If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 85 OSPFv3 Adjacency Loss

Requirements

To perform this procedure, you must use an account with at least an Admin user access level.

Probable cause

This alarm is raised when the OSPFv3 is enabled on an interface and there is no OSPFv3 neighbor reaching or passing Exchange state on that interface.

This alarm is masked by “LAN Port Failure” alarm on Access Panel ports or “LOS/LOF” alarms on the OSC.

This alarm is also raised when user restart an Active CTM, or warm/cold restart an IM circuit pack that is carrying OSPF traffic using its OSC interface.

Impact

Minor, non-service-affecting (m, NSA)

Steps

1. Ensure that at least one of the OSPFv3 neighbors is reaching or passing Exchange state on the interface. Refer to “Displaying OSPFv2/OSPFv3 diagnostics” procedure in *OAM Communications*, 323-2051-101 to determine the OSPF neighbor state.
2. If the alarm does not clear and you are certain that this OSPF neighbor is not required, delete the OSPFv3 on the interface. Refer to “Configuring and deleting the OSPFv3 protocol” procedure in *OAM Communications*, 323-2051-101 to delete the OSPFv3.
3. If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 86 OSRP Connection Mismatch

Requirements

To perform this procedure, you must use an account with at least an Admin user access level.

Probable cause

This alarm is raised when the Optical Signaling and Routing Protocol (OSRP) connections are not vertically synchronized.

The alarm is also raised when there is Inconsistency between snc-group/snc and mcconns.

Impact

Major, service-affecting (M, SA)

Steps

1. Check if OSRP is in idle (for example, no channel-provisioning is ongoing). Enter:

   ```
   action osrp <osrp-node-name> object osrp-node <osrp-node-name> check-channel-provisioning-in-progress
   ```

   ```
   output - channel-provisioning-in-progress : no
   ```

2. If channel-provisioning-in-progress = no then execute below RA initiate-conn-sync utility.

   ```
   WEST# action osrp <osrp-node-name>initiate-conn-syncinstance : "ciena-6500r-osrp-rls-ra-osrp:osrp<osrp-node-name>initiate-conn-sync"error : error-confirmation-requirederror-str : This operation may affect trafficConfirmation required. Confirm? Y/N yresult : initiate-conn-sync executed successfully.
   ```

   Note 1: The above command needs to be executed under expert supervision.

   Note 2: There is no Node Essentials equivalent command for this release.

3. Alarm cleares by itself after CTM reboot without any user intervention.
4. If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 87 OSRP Line Degraded

This alarm indicates that the Control Plane is aware of an underlying issue that can affect existing channels or any new channel.

Requirements

To perform this procedure, you must use an account with at least an Admin user access level.

Probable cause

The following conditions can cause this alarm:

- Circuit Pack Fail
- Major High Fiber Loss
- Low Optical Power on the LRU Monitoring port
- RAMAN operating-state is shutoff

Impact

Warning, non-service-affecting (W, NSA)

Steps

1 Retrieve all the active alarms and alarm details for any issues such as Amplifier Shutoff, OLF, HFL, or OSC LOS.

If you want to perform the procedure using	**Then** go to the
CLI commands	"CLI INTERFACE STEPS"
Node Essentials	See the Node Essential steps in "Retrieving the data for the active alarm object" on page 32 in this document. Then go to step 4.

CLI INTERFACE STEPS

2 The following step is performed using CLI commands.

```
show active-alarm <id> [name] [resource] [raise-time]
[raise-time] [cause] [condition-type] [direction]
[location] [severity] [service-impact] [additional-info]
[user-notes...]
```

The current alarms and alarm details appear.

3 Verify the OSRP link and line data by issuing the following command:

```
show osrp <node-name>:<PFG> object osrp-link <osrplink-#>
```

4 Verify and correct any of the causes listed in the "Probable Cause".

Note: A fault reason is provided within the alarm "Additional Information" field to help with the troubleshooting.

Copyright© 2019-2025 Ciena® Corporation

5 If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 88 OSRP Line Operationally Blocked

Requirements

To perform this procedure, you must use an account with at least an Admin user access level.

Probable cause

The following conditions can cause this alarm:

- Major High Fiber Loss
- RAMAN is in shutoff state, look for
  - Raman APR at output
  - Raman admin-state disabled
  - Raman activation inhibited
  - Raman automatic shutoff
  - Raman forced shutoff
- SRA/RLA/DLA/DLE/CCMD circuit pack fail/circuit pack mismatch
- SRA circuit pack missing
- Circuit pack mismatch
- Bandwidth lockout
- Low priority holdoff timer

Impact

Warning, non-service-affecting (W, NSA)

Steps

1 Retrieve all the active alarms and alarm details for any issues such as Amplifier Shutoff, OLF, HFL, or OSC LOS.

If you want to perform the procedure using	**Then** go to the
CLI commands	"CLI INTERFACE STEPS"
Node Essentials	See the Node Essential steps in "Retrieving the data for the active alarm object" on page 32 in this document. Then go to step 4.

Copyright© 2019-2025 Ciena® Corporation

CLI INTERFACE STEPS

2 The following step is performed using CLI commands.

```
show active-alarm <id> [name] [resource] [raise-time]
[raise-time] [cause] [condition-type] [direction]
[location] [severity] [service-impact] [additional-info]
[user-notes...]
```

The current alarms and alarm details appear.

3 Verify the osrplink/line data by issuing the following command:

```
show osrp <node-name>:<PFG> object osrp-link <osrplink-#>
```

4 If the line is manually blocked, un-block the line by disabling the OSRP bandwidth lockout.

Refer to “Provisioning an OSRP line” procedure in *6500 RLS L0 Control Plane*, 323-2051-330.

5 Verify and correct any of the causes listed in the “Probable Cause”.

Note: A fault reason is provided within the alarm “Additional Information” field to help with the troubleshooting.

6 If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 89 OSRP Link Configuration Mismatch

Requirements

To perform this procedure, you must use an account with at least an Admin user access level.

Probable cause

This alarm is raised when the admin weight or bundle id is different on both sides of a Optical Signaling and Routing Protocol (OSRP) link.

This alarm is also raised when a bandwidth lockout is enabled on one end of an OSRP line and disabled on the other end.

If you apply a bandwidth lockout for maintenance activities to one end of the line, it is required to apply a bandwidth lockout on the other end of the line to clear the alarm.

Impact

Major, service-affecting (M,SA)

Steps

1. Determine if both ends of the OSRP link have the same admin weight and bundle id assigned.

   Refer to “Displaying OSRP network topology” procedure in *6500 RLS L0 Control Plane*, 323-2051-330.

2. If different, provision the OSRP link to have the same admin weight and bundle id assigned.

   Refer to “Provisioning an OSRP line” procedure in *6500 RLS L0 Control Plane*, 323-2051-330.

3. If the alarm is not cleared, determine if a bandwidth lockout is enabled on one end of an OSRP line and disabled on the other end.

   ```
   show osrp <node-name>:<PFG> object osrp-link <osrplink-#>
   line
   ```

4. Disable the bandwidth lockout on the OSRP line or enable the bandwidth lockout at the other end of the OSRP line.

5. If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 90 OSRP Link Down

Requirements

To perform this procedure, you must use an account with at least an Admin user access level.

Probable cause

The following conditions can cause this alarm:

- Fiber Break Detected
- Optical Line Fail
- Amp faults:
  - Input LOS
  - Automatic Power Reduction Active
  - Shutoff Threshold Crossed
  - Admin-state Disabled
  - Forced-shutoff Enabled
  - Automatic Shutoff
- Span Calibration in Progress
- RLA/DLA/DLE/CCMD Circuit Pack Missing

Impact

Warning, non-service-affecting (W, NSA)

Steps

1 Verify the “additional-info” field for the location of the root cause of the alarm.

2 Retrieve all the active alarms at the root cause site.

If you want to perform the procedure using	**Then** go to the
CLI commands	“CLI INTERFACE STEPS”
Node Essentials	See the Node Essential steps in “Retrieving the data for the active alarm object” on page 32 in this document. Then go to step 4.

CLI INTERFACE STEPS

3 The following step is performed using CLI commands.

```
show active-alarm <id> [name] [resource] [raise-time]
[raise-time] [cause] [condition-type] [direction]
[location] [severity] [service-impact] [additional-info]
[user-notes...]
```


Copyright© 2019-2025 Ciena® Corporation

The current alarms and alarm details will appear.

4 Clear the active alarms at the root cause site. Refer to the appropriate alarm clearing procedures in this document.

Note: A fault reason is provided within the alarm “Additional Information” field to help with the troubleshooting.

5 Verify the alarm(s) have cleared from the ROADM shelves.

6 If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 91 OSRP Node Is Not Up

Requirements

To perform this procedure, you must use an account with at least an Admin user access level.

Probable cause

This alarm is raised when the CTM or OSRP micro-service restarts.

This alarm is raised when the OSRP node is administratively blocked by the user.

This alarm is also raised when a node is administratively blocked by the user.

Impact

Critical, service-affecting (C,SA)

Steps

1. If the node is manually blocked, un-block the node by changing the OSRP node “Admin state” to “Unlocked”.

   Refer to “Provisioning an OSRP node” procedure in *6500 RLS L0 Control Plane*, 323-2051-330.

2. This alarm is raised and cleared in under 1 minute. If the alarm did not clear, perform a CTM restart. Refer to “Restarting an interface module or the CTM” on page 37.

3. If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 92 OSRP Node Operationally Blocked

Requirements

To perform this procedure, you must use an account with at least an Admin user access level.

Probable cause

This alarm is raised when a node is administratively blocked by the user.

The alarm is also raised in the presence of a “Software Subsystem Failure” alarm, where the subsystem is required for Control Plane to add or delete channels.

Impact

Minor, non-service-affecting (m, NSA)

Steps

1. If the node is manually blocked, un-block the node by changing the OSRP node “Admin state” to “Unlocked”.

   Refer to “Provisioning an OSRP node” procedure in *6500 RLS L0 Control Plane*, 323-2051-330.

2. If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 93 OTDR File Transfer Failed

Requirements

To perform this procedure, you must use an account with at least an Admin user access level.

Probable cause

This alarm is raised when the transfer of the OTDR trace Standard OTDR Record (SOR) files to a destination has failed.

The failure can be caused by a missing Access Panel or when the Access Panel is full.

When the automatic upload feature is enabled and the file transfer fails, the system retries the file transfer with increasing waiting times (for example; 1, 2, 5 minutes). If the file transfer fails 3 consecutive times, the “OTDR File Transfer Failed” alarm is raised. The alarm clears when all of the failed uploads succeed or auto upload is disabled.

This alarm can also be raised (with a delay) after a CTM restart.

Impact

Minor, non-service-affecting (m, NSA)

Steps

1. Transfer the OTDR trace SOR file again using the following command:

   `otdr-upload-sor-files`

2. Verify that the authority is set correctly, user name and password are valid, the host is accessible and folder is present on the remote server.
3. If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 94 OTDR High Loss Detected

Requirements

To perform this procedure, you must:

- use an account with at least an Admin user access level
- observe all safety requirements described in *6500 RLS Shelf Installation Guide*, 323-2051-201
- have a fiber cleaning kit (for Photonic configurations, LC cleaning kits are needed). See the *Optical Connector Inspection and Cleaning*, 323-1859-500
- obtain a fiber patchcord, if required

Probable cause

This alarm is raised by the OTDR on both Line In and Line Out when the single or total loss is higher than the loss threshold.

If the span loss is less than the event detection range for the OTDR office trace, being 2 km, that alarms may be raised due to high loss detected.

> ***Note:*** The OTDR event-range is based on the distance of the end point of the event.A user can provision the event-range parameter to avoid unwanted alarm in such case. For detail, see the *6500 RLS Optical Control, SPLI, and OTDR*, 323-2051-318.

If you do not want to see alarms raised for OTDR, then the admin-state of the OTDR facility can be set to Disabled. Once Disabled, the alarms will be cleared.

This alarm is also raised as part of the Go/No-Go pass criteria for the SRA when the event loss calculated by the OTDR trace is higher than the provisioned threshold. The Raman pumps shut off when ALSO is active or when the following conditions are met:

- If the measured return loss at the SRA Express Out port (port 3) is less than the ORL threshold (default 22dB).
- If the measured power at the SRA Express Out port (port 3) is greater than the power threshold (default 20.3dBm).
- If the loss of the event is greater than the threshold (Default 0.5 dB), the alarm is raised on the Line Out Port.
- If the total loss for the length of the office trace (2 km) is greater than the threshold (default 1.0 dB).

Look into the additional info of the alarm for details regarding the Go/No-Go failure.

Copyright© 2019-2025 Ciena® Corporation

Note: If RAMAN pumps are already turned on and in-service OTDR detects high loss, the alarm is raised but the Raman pumps do not shutoff.

The alarm can only be cleared when the Go/No-Go trace is a “Pass”.

Impact

Major, non-service-affecting (M, NSA), for SRA Go/NoGo “nogo” trace results (since they are service blocking)

Minor, non-service-affecting (m, NSA), for all other OTDR High Loss alarms

Steps

1 Check the additional info field for the alarm for the information about the trace causing the alarm. Alarms against the interconnected RLA/DLE/DLA input port (port 54 or 64) will prevent the Raman pumps from turning on.

a. High Loss - Short Trace

b. High Loss - Office Trace

c. Flat Trace - Long Trace

Note: Any troubleshooting will be from the RLA/DLE/DLA input port (port 54 or port 64) and SRA ports 3 and 6, on all the fiber and patch panels in the site and including the outside fiber.

2 Choose your next step:

If the alarm is raised	**Then** go to
as part of the Go/No-Go pass criteria for the SRA	step 3
by OTDR on Line In and Line Out when the loss is higher than the loss threshold	step 17

3 It is recommended to re-run the Go/No-Go before starting any troubleshooting to make sure the issue is still present.

4 Place the RAMAN pumps into the “Disabled” state to allow the Go/No-Go trace to run:

If you want to perform the procedure using	**Then** go to the
CLI commands	“CLI INTERFACE STEPS”
Node Essentials	“NODE ESSENTIALS STEPS”

CLI INTERFACE STEPS

5 To place the RAMAN pumps into the “Disabled” state, enter the following command:

```
set slots <slot number> config ramans LINE-IN [admin-
state <Disabled>]
```

6 Go to step 14.

Copyright© 2019-2025 Ciena® Corporation

NODE ESSENTIALS STEPS

7 Select **Facilities** from the Node Essentials navigation menu.

The Facilities menu opens.

8 From the **Equipment** grid, select the module with the alarmed RAMAN facility.

The bottom part of screen becomes populated.

9 Select RAMAN facility from Facility navigator.

The RAMAN Facilities grid opens.

10 Select the alarmed RAMAN facility by Row selector from the RAMAN Facilities grid.

11 Click the **Pencil** icon.

The related Edit dialog opens.

12 Edit the RAMAN facility as required.

Admin state: Disabled

13 Click **Confirm**.

14 Manually run the OTDR Go/No-Go trace. Enter the following command:

```
start-otdr-trace name "slot-<slot number>-port-<port
number>" trace-type go-nogo
```

Note: There is no Node Essentials equivalent command for this release.

15 When the trace is completed, place the RAMAN pumps into the "Enabled" state.

16 If the alarm is still present, based on which trace is the cause for the alarm, verify the respective trace in the OTDR. Refer to "Provisioning OTDR trace" procedure in *Optical Control, SPLI, and OTDR*, 323-2051-318.

17 Display the OTDR events raising the issue:

If you want to perform the procedure using	**Then** go to the
CLI commands	"CLI INTERFACE STEPS"
Node Essentials	"NODE ESSENTIALS STEPS"

CLI INTERFACE STEPS

18 To display the OTDR events raising the issue. Enter the following command:

```
show-otdr-events name slot-<slot #>-port-<port #> trace-
type <trace-type> trace-tag <trace-tag>
```

19 Go to step 23.

NODE ESSENTIALS STEPS

20 Select **Tools** from the Node Essentials navigation menu.

The OTDR grid opens.

21 Use row selector to select the **OTDR** that you ran the OTDR Go/No-Go trace to display the OTDR events in the SOR traces grid.

Copyright© 2019-2025 Ciena® Corporation

22 Choose the desired SOR Trace and click on the “View trace” icon on the top corner of the SOR traces grid. Click on the key events or parameters in the OTDR trace window to see the resulting information.

23 Examine the resulting information on the event (event type, distance, and measurement) to determine the location of the fault(s).

24 From the resulting information, find the highest event loss within the first 20 km to see which event is triggering the alarm.

```
Output example
SITEG-01# show-otdr-events name slot-3-port-53 trace-type
office trace-tag current
output
result : success
name : 53
trace-event:
- trace-type : office
- trace-tag : current
trace-date-time : 2021-05-07T12:32:00Z
num-event : 1
events:
- event-num : 1
event-type : reflection
event-distance : 0
event-reflection : -52.79
event-loss : 12.30
```

25 If the issue is outside of the fiber-plant, the fiber may need to be repaired.

26 If the loss is within the fiber plant, use a fiber cleaning kit to clean all the connectors and then reconnect the fibers. Refer to *Optical Connector Inspection and Cleaning*, 323-1859-500.

27 If traces were run remotely, dispatch someone to site to perform this task. For the SRA scenario, it is recommended to send a spare SRA circuit pack if a known good SRA circuit pack is not present at site.

Disconnecting and reconnecting the fiber in the fiber plant that is already connected, triggers automatic OTDR traces to run. It is recommended to wait for the OTDR traces that were triggered automatically to be completed. If you disconnect a fiber connection and need to clean more, do all the cleaning and then reconnect the first connector that was disconnected. This prevents multiple OTDR triggers which can take longer to complete.

28 If the alarm is raised as part of the Go/No-Go pass criteria for the SRA and the span is not bookended by SRA, run the trace manually to clear the alarm.

29 If cleaning connectors fails to resolve the issue, replace faulty fiber patch cords.

Copyright© 2019-2025 Ciena® Corporation

30 Once the fiber is reconnected, the OTDR Traces run automatically. If the new trace passes, the alarm will clear.

31 For the SRA, if the alarm is still present, run the Go/No-Go on the unit for the SRA scenario.

32 If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 95 OTDR High Reflection Detected

Requirements

To perform this procedure, you must:

- use an account with at least an Admin user access level
- observe all safety requirements described in *6500 RLS Shelf Installation Guide*, 323-2051-201
- have a fiber cleaning kit (for Photonic configurations, LC cleaning kits are needed). See the *Optical Connector Inspection and Cleaning*, 323-1859-500
- obtain a fiber patchcord, if required

Probable cause

This alarm is raised by the OTDR on both Line In and Line Out when the reflection is below the threshold.

This alarm is also raised as part of the Go/No-Go pass criteria for the SRA when the event reflection calculated by the OTDR trace is higher than the provisioned threshold. The Raman pumps shut off when ALSO is active or when the following 2 conditions are met:

- If the measured return reflection at the SRA Express Out port (port 3) is less than the ORL threshold (default 22 dB)
- If the measured power at the SRA Express Out port (port 3) is greater than the power threshold (default 20.3 dBm)

Look into the additional info of the alarm for details regarding the Go/No-Go failure.

> ***Note:*** If RAMAN pumps are already turned on and in-service OTDR detects high reflection, the alarm is raised but the Raman pumps do not shutoff.

Impact

Major, non-service-affecting (M, NSA), for SRA Go/NoGo “nogo” trace results (since they are service blocking)

Minor, non-service-affecting (m, NSA), for all other OTDR High Reflection alarms

Steps

1 Check the additional info field of the alarm for the information about the trace causing the alarm. Alarms against the interconnected RLA/DLE/DLA input port (port 54 or 64) will prevent the Raman pumps from turning on.

a. High Reflection - Short Trace

Copyright© 2019-2025 Ciena® Corporation

b. High Reflection - Office Trace

c. Flat Trace - Long Trace

Note: Any troubleshooting will be from the RLA/DLE/DLA input port (port 54 or port 64) and SRA ports 3 and 6, on all the fiber and patch panels in the site and including the outside fiber.

2 Choose your next step:

If the alarm is raised	**Then** go to
as part of the Go/No-Go pass criteria for the SRA	step 3
by OTDR on Line In and Line Out when the loss is higher than the loss threshold	step 5

3 It is recommended to re-run the Go/No-Go before starting any troubleshooting to make sure the issue is still present. Refer to *Optical Control, SPLI, and OTDR*, 323-2051-318.

4 If the alarm is still present, based on which trace is the cause for the alarm, verify the respective trace in the OTDR. Refer to “Provisioning OTDR trace” procedure in *Optical Control, SPLI, and OTDR*, 323-2051-318.

5 Display the OTDR events raising the issue:

If you want to perform the procedure using	**Then** go to the
CLI commands	“CLI INTERFACE STEPS”
Node Essentials	“NODE ESSENTIALS STEPS”

CLI INTERFACE STEPS

6 To display the OTDR events raising the issue. Enter the following command:

```
show-otdr-events name slot-<slot #>-port-<port #> trace-
type <trace-type> trace-tag <trace-tag>
```

7 Go to step 11.

NODE ESSENTIALS STEPS

8 Select **Tools** from the Node Essentials navigation menu.

The OTDR grid opens.

9 Use row selector to select the **OTDR** with the alarmed OTDR facility.

10 Choose the desired SOR Trace and click on the “View trace” icon on the top corner of the SOR traces grid. Click on the key events or parameters in the OTDR trace window to see the resulting information.

11 Examine the resulting information on the event (event type, distance, and measurement) to determine the location of the fault(s).

12 From the resulting information, find the highest event loss within the first 20 km to see which event is triggering the alarm.

Copyright© 2019-2025 Ciena® Corporation

```
CLI Output example
SITEG-01# show-otdr-events name slot-3-port-53 trace-type
office trace-tag current
output
result : success
name : 53
trace-event:
- trace-type : office
- trace-tag : current
trace-date-time : 2021-05-07T12:32:00Z
num-event : 1
events:
- event-num : 1
event-type : reflection
event-distance : 0
event-reflection : -52.79
event-loss : 12.30
```

13 If the issue is outside of the fiber plant, the fiber may need to be repaired.

14 If the reflection is within the fiber plant, use a fiber cleaning kit to clean all the connectors and then reconnect the fibers. Refer to *Optical Connector Inspection and Cleaning*, 323-1859-500.

15 If traces were run remotely, dispatch someone to site to perform this task. For the SRA scenario, it is recommended to send a spare SRA circuit pack if a known good SRA circuit pack is not present at site.

Disconnecting and reconnecting the fiber in the fiber plant that is already connected, triggers automatic OTDR traces to run. It is recommended to wait for the OTDR traces that were triggered automatically to be completed. If you disconnect a fiber connection and need to clean more, do all the cleaning and then reconnect the first connector that was disconnected. This prevents multiple OTDR triggers which can take longer to complete.

16 If the alarm is raised as part of the Go/No-Go pass criteria for the SRA and the span is not bookended by SRA, run the trace manually to clear the alarm.

17 If cleaning connectors fails to resolve the issue, replace faulty fiber patch cords.

18 Once the fiber is reconnected, the OTDR Traces run automatically. If the new trace passes, the alarm will clear.

19 For the SRA, if the alarm is still present, run the Go/No-Go on the unit.

20 If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 96 OTDR Trace In Progress

Probable cause

This alarm is raised when the OTDR trace is in progress.

Impact

Warning, non-service-affecting (W, NSA)

Steps

1. No action is required. The alarm clears when the trace completes automatically.
2. You can also stop the current trace in progress to clear the alarm:

If you want to perform the procedure using	**Then** go to the
CLI commands	"CLI INTERFACE STEPS"
Node Essentials	"NODE ESSENTIALS STEPS"

CLI INTERFACE STEPS

3. To stop the current trace in progress to clear the alarm. Enter the following command:

```
stop-otdr-trace name <string> [trace-type
<long|office|short>]
```

4. Go to step 8.

NODE ESSENTIALS STEPS

5. Select **Tools** from the Node Essentials navigation menu.
6. From the **Tools** menu, select OTDR.

   The list of available OTDR facilities are displayed in the OTDR grid.
7. Select the **OTDR** unit that you want to stop the current trace and click on the **Stop trace** icon on the top right of the screen.
8. If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 97 Permanent Snc-Group Unavailable

Requirements

To perform this procedure, you must use an account with at least an Admin user access level.

Probable cause

This alarm is raised when the SNCG cannot be managed due to problems along the path (comms, CTM failed, fiber cut).

Note: It can take at least 15 minutes before the alarm is raised after the fault causing the alarm.

Impact

Critical, service-affecting (C,SA)

Steps

1 Identify the node raising the alarm and note any additional information:

If you want to perform the procedure using	**Then** go to the
CLI commands	"CLI INTERFACE STEPS"
Node Essentials	See the Node Essential steps in "Retrieving the data for the active alarm object" on page 32 of this document. Then go to step 3.

CLI INTERFACE STEPS

2 The following step is performed using CLI commands.

```
show active-alarm [id] [name] resource raise-time [clear-time] cause [condition-type] [direction] [location] severity service-impact [additional-info] [user-notes...]
```

Refer to "Alarm parameters" on page 27 for applicable parameters. Go to step 3.

3 Verify the SNCG diagnostics information. Enter the following command.

```
action osrp <osrp-node-name>:<PFG> object snc-group <sncg-name> show-diagnostics
```

4 If the SNCG raising the alarm is recently added, verify the end-to end provisioning. If mis-provisioning is identified, delete and re-create the SNCG.

5 If the alarm does not clear, verify if any equipment alarms are raised against circuit packs carrying the SNCG. If there are, clear these alarms before continuing this procedure.

6 Display the SNCG route list. Enter:

Copyright© 2019-2025 Ciena® Corporation

```
show osrp <osrp-node-name>:<PFG> object snc-group <SNCG-name> route-list
```

7

If the current route is	**Then** go to
available	step 8
not available	step 10

8 View the provisioning of the alarming P-SNCG and note its member SNCs. From the SNC list, note the nodes and ports of the home route.

```
show osrp <osrp-node-name>:<PFG> object snc-group <SNCG-name>
```

Refer to “Displaying and clearing SNC/SNCG diagnostics information” procedure in *6500 RLS L0 Control Plane*, 323-2051-330.

9 Verify if any equipment alarms exist. See step 1 for the commands. If there are any active alarms, clear these alarms. Go to step 12.

10 Verify the SNCG Status Diagnostic.

```
action osrp <osrp-node-name>:<PFG> object snc-group <sncg-name> show-diagnostics
```

Refer to “Displaying and clearing SNC/SNCG diagnostics information” procedure in *6500 RLS L0 Control Plane*, 323-2051-330.

11 If the event detail currently indicates failures or errors, stop the procedure and contact your network administrator.

12 If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 98 Power Failure Fault

Requirements

To perform this procedure, you must:

- observe all safety requirements described in *6500 RLS Shelf Installation Guide,* 323-2051-201
- have an antistatic wrist strap to dissipate electrostatic charges
- have a standard multimeter
- have a spare Power Input Module (PIM) to replace each PIM in the shelf
- have spare main and indicator fuses to replace (if alarm is raised against a fused PIM

You do not have to replace each PIM with a new PIM. Use a single spare PIM of the correct type to replace each PIM in turn.

Probable cause

This alarm is raised against a PIM when the CTM detects that low or no voltage exists on the backplane power feed. If one power source has failed, the shelf traffic is not usually affected. Failure of more than one feed on a shelf may affect service if both PIMs have failed.

This alarm can also be raised against a fused PIM when the fuse cartridge has been removed, or if the indicator fuse is not present on the module and the main fuse has blown.

> ***Note:*** The time delay between the condition occurring and the alarm being raised is 10 seconds. The time delay between the condition being removed and the alarm being cleared is 50 seconds.

Impact

Major, non-service affecting (M, NSA)

Steps

1 Open the shelf inventory and verify that the PIM associated with the alarm is listed. To display the inventory, refer to “Provisioning a slot” procedure in *Equipment/Facility Provisioning and Protection*, 323-2051-310.

2 Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.

3 In the R2 or R4 shelf, the PIMs are located on the rear of the shelf. The status of the module is indicated by the LEDs on the Access Panel “Rear Alarm” LED. A “Rear Alarm” red LED indicates if there are any alarms against the shelf fan modules and/or PIMs. If the LED is lit requiring the user to service the rear of the shelf to clear the alarm.

Copyright© 2019-2025 Ciena® Corporation

4 At the shelf faceplate, identify the PIM that is the source of the alarm. If power is not reaching the system through the PIM (due to a tripped breaker or externally disconnected power feed), the “Power OK” LED on the faceplate of the PIM is off.

5

If the LED is	**Then** go to
on	step 7
off	step 6

6

If the associated PIM is	**Then** go to
breakered	step 8
breakerless	step 9
fused	step 7

7 Make sure the removable fuse cartridge is properly seated. If the original alarm clears, the procedure is complete. Otherwise, replace the cartridge fuse and optional indicator fuse (if previously equipped and blown) with the same size fuse. If the original alarm clears, the procedure is complete. Otherwise go to step 9.

8 Check if the breaker is tripped. If so, reset it to the ON position. If the original alarm clears, the procedure is complete; otherwise, go to step step 9.

9

CAUTION
Risk of electrical shock and short circuit
Ensure that there is no chance of coming in contact with the power cables of the PIM. Electrical shock or short circuit can result.

Use your company procedure to measure the DC voltage between the L+ return reference and L- power feed using a multimeter. Make sure that the feed is the correct polarity. For the AC power source, you can use an AC power tester to check the voltage as per your company procedure. For a high-voltage DC (240 Vdc) power source (China only), use a DC power tester as per your company procedure.

10 Choose your next step:

Copyright© 2019-2025 Ciena® Corporation

If the feed and voltage is	**Then**
DC and is between 43.5 and 75 Vdc and the polarity is correct or AC and is between 100 and 240 Vac, 50-60 Hz or high-voltage DC (for China only) and is between 180 and 300 Vdc	go to step 11
DC and between 0V and 43.5 Vdc or if the polarity is reversed or is AC and is less than 100 Vac or is high-voltage DC (for China only) and is less than 180 Vdc	use your company procedure to investigate and correct the fault in the power distribution system. Go to step 4.

11 If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 99 Preferred IP Not Available

Requirements

To perform this procedure, you must use an account with at least an Admin user access level.

Probable cause

This alarm is raised when a user sets node IP preference to the desired IP to be used for inter-shelf messaging and the remote node does not contain the preferred IP version.

Impact

Minor, non-service-affecting (m, NSA)

Steps

1. Verify the additional information text to find out which nodes have mismatch in IP comms provisioning (discovery) versus the IP version preference configured by the user. Fix the IP comms provisioning in the local or remote node as indicated by the additional information text in the alarm.
2. Set “node-ip-version-preference” based on remote node discovered IP or local node IP comms.

   ```
   set node-ip-version-preference ip-version ipv4
   ```

   Or

   ```
   set node-ip-version-preference ip-version ipv6
   ```
3. You can also delete the preferred IP version as follows:

   ```
   delete node-ip-version-preference ip-version <version>
   ```


Copyright© 2019-2025 Ciena® Corporation

Procedure 100 Protection Switch Complete Revertive

Requirements

To perform this procedure, you must use an account with at least an Admin user access level.

Probable cause

This alarm is raised when the protection mode is provisioned as revertive, and a protection switch has completed.

Impact

Warning, non-service affecting (w, NSA)

Steps

1 No action is required if a user is performing a test or maintenance operation. This alarm is a reminder not to leave a potentially service-affecting condition on the system.

2 Check the traffic protection status. Refer to the “Retrieving TPS/TPS2 protection group information” procedure in *Equipment/Facility Provisioning and Protection*, 323-2051-310.

3 If an automatic protection switch is active, check for equipment failure, signal failure or degraded signal alarms related to this alarmed unit. Clear any alarm by following the appropriate trouble clearing procedure in this document.

4

If	Then
no automatic switches are active	go to step 5
the original alarm has cleared	the procedure is complete.
the original alarm has not cleared	go to step 5

5 Determine if a user switch is active, release the switch. Refer to the *Equipment/Facility Provisioning and Protection*, 323-2051-310.

6

If	Then
no user switches are active	go to step 7
the original alarm has cleared	the procedure is complete.
the original alarm has not cleared	go to step 7

7 If the alarm remains active, ensure that no other alarm is active.

8 If the alarm does not clear, contact your next level of support or Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 101 Protection Switch Complete

Requirements

To perform this procedure, you must use an account with at least an Admin user access level.

Probable cause

This alarm is raised when a protection switch has completed.

This alarm can be raised momentarily after restoring the protection switch. The alarm is also raised after a CTM restart, a module restart (notably the TPS), shelf power cycle, and shelf upgrade (which involves CTM and module restart) without an actual switch occurring.

This alarm will take some time to appear again after a CTM restart because of the following factors:

- the time between issuing the restart command and first getting the first logs
- the time until card sends a card ready trap
- the time until CTM sends a re-raise request, which depends on the number of modules in the shelf
- the time between the diagnostic being set to true and alarm being raised, which could be affected by other masking conditions

Impact

Warning, non-service-affecting (W, NSA)

Steps

1 No action is required if a user is performing a test or maintenance operation. This alarm is a reminder not to leave a potentially service-affecting condition on the system.

2 Retrieve the traffic protection status for the alarmed circuit pack. Refer to the “Retrieving TPS/TPS2 protection group information” procedure in *Equipment/Facility Provisioning and Protection*, 323-2051-310. If an automatic protection switch is active, check for equipment failure, signal failure or degraded signal alarms related to this alarmed unit. Clear any alarms by following the appropriate trouble clearing procedure in this document.

3

If the original alarm has	**Then**
cleared	the procedure is complete.
not cleared	go to step 4

4 If the alarmed amplifier is a pre-amplifier, ensure that all connectors located after the amplifier output are properly mated. Verify this on both ends of the connector-mating receptacles.

Copyright© 2019-2025 Ciena® Corporation

5. Ensure that the termination plugs are present and are mated properly on unused ports.
6. If the alarm is not clear, determine if any user request resulted in a dropped protection switch. Check for protection switching alarms. Refer to the “Protection configurations and CTM redundancy” procedure in *Equipment/ Facility Provisioning and Protection*, 323-2051-310.
7. If the alarm does not clear, contact your next level of support or Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 102 Provisioning Incompatible

Requirements

To perform this procedure, you must:

- use an account with at least an Admin user access level
- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *6500 RLS Shelf Installation Guide*, 323-2051-201
- have an antistatic wrist strap to dissipate electrostatic charges

Probable cause

This alarm is raised when a circuit pack or pluggable is inserted in a slot with auto-equip enabled, and the circuit pack or pluggable cannot be provisioned in that slot.

This alarm is also raised when specific provisioning is missing. For example, the frequency range is not provisioned.

Impact

Minor, non-service-affecting (m, NSA)

Steps

1 Wear an antistatic wrist strap.

CAUTION
Risk of damage to module
Wear an antistatic wrist strap to protect the equipment from static damage. Connect the wrist strap to the ESD jack on the shelf or module.

2 Unseat the alarmed circuit pack from the shelf. The alarm should clear.

3 Determine if the alarmed circuit pack is incompatible with the shelf type.

4

If the circuit pack is	**Then**
not compatible	replace the circuit pack with one that is compatible with the shelf. The procedure is complete.
is compatible	go to step 5

5 Retrieve the cooling types currently configured on the shelf.

6 Compare the Provisioned and Actual cooling capacity with the required cooling capacity value for the new module. Refer to *6500 RLS Planning Guide*, NTRN10WA, for engineering information on the module.

Copyright© 2019-2025 Ciena® Corporation

7

If the module	**Then**
is not compatible with the shelf cooling	replace the cooling module with one that is compatible with the shelf. The procedure is complete.
is compatible with the shelf cooling	go to the next step

8 Retrieve the shelf power budget and provisioned shelf current.

9 Determine the power requirement of the alarmed module. Refer to “Shelf Power Budget” section in *6500 RLS Planning Guide*, NTRN10WA, for more information.

10

If the power requirements of the alarmed module are	**Then**
greater than the available power	shelf power overload is causing the alarm. Provision the Provisioned shelf current value equal to the power feed amperage.
less than the available power	contact your next level of support or Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 103 Provisioning Incomplete

Requirements

To perform this procedure, you must use an account with at least an Admin user access level.

Probable cause

This alarm is raised when the Photonic Functional Group (PFG) provisioning is missing. For example, the frequency range and PFG data was not provisioned.

Impact

Minor

Steps

1. Provision the PFG parameters to recover the missing data. Refer to *ZTP and Manual Commissioning*, 323-2051-220.
2. If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 104 Provisioning Mismatch

Requirements

To perform this procedure, you must use an account with at least an Admin user access level.

Probable cause

This alarm is raised against the CV supported Rx port. It is raised when a local CV Rx expected-port-id does not match the remote link “from” port.

This alarm is also raised when performing a manual CV test on SSM add/drop ports (looped back). For RLA-SSM or WSS-SSM links on SSM add/drop ports with loopback connectors (unused), when CV is enabled with a Rx expected-port-id provisioned, the alarm is raised. This is because the from port of the link does not match the CV Rx expected-port-id. SSM is passive and does not have a CV component.

Impact

Warning, non-service-affecting (W, NSA)

Steps

1. Identify the local CV expected-port-id for which the alarm is raised against.
2. Find the local CV expected-port-id and expected-nbr-ids using command:

   ```
   show slots <slot#> config cv ports rx <port#>
   ```

3. Log into the shelf of the expected-port-id (using node details in expected-nbr-ids).
4. On the remote shelf, identify the problematic link then retrieve link details:

   ```
   show link <link-name> from to
   ```

5. Identify the incorrect link “from” provisioning then correct it using:

   ```
   set link <link-name> from “nodes <node> data slots <slot#>
   config port <port#>”
   ```


Copyright© 2019-2025 Ciena® Corporation

Figure 12 Example

```
Mumbai-2# show slots 1 config cv ports rx 21-7
 slots:
 - name   : 1
  config:
   cv:
    ports:
     rx:
     - name              : 21-7
       expected-port-id   : slot.1_port.21-5  <--------------- Mismatch raised for.
       expected-nbr-ids:
         ipv4-address   : 10.184.14.74
         system-name    : Mumbai-1

Mumbai-1# show link link-slot1-port21-5
 link:
 - name                      : link-slot1-port21-5
  from                       : ciena-6500r-nodes:nodes Mumbai-1 data slots 1 config port 21-6 <--------------- should be 21-5.
  to                         : ciena-6500r-nodes:nodes Mumbai-2 data slots 1 config port 21-7
  link-type                  : logical

Mumbai-1# set link link-slot1-port21-5 from " ciena-6500r-nodes:nodes Mumbai-1 data slots 1 config port 21-5"
```

6 If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 105 RADIUS Server(s) Unavailable

Requirements

To perform this procedure, you must use an account with at least a Super user access level.

Probable cause

This alarm is raised when

- all requests to the primary and secondary RADIUS servers of a CTM time out
- all requests to a RADIUS server of a CTM time out and only one RADIUS server is provisioned

Impact

Major, non-service-affecting (M, NSA)

Steps

1. The alarm clears when connectivity is re-established between the shelf and the RADIUS server. If the alarm does not clear, perform one of the following:
   a. clear the security alarms. Refer to appropriate alarm clearing procedures in this document.
   b. disable RADIUS server. Refer to “Displaying and provisioning security authentication parameters” procedure in *Licensing, Security, and Administration*, 323-2051-300.
2. If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 106 Raman Activation Inhibited

Requirements

To perform this procedure, you must use an account with at least an Admin user access level.

Probable cause

This alarm is raised against a RAMAN facility when the Raman pumps are prevented from turning on because of No-Go condition. The alarm clears when the No-Go condition clears.

Impact

Warning, Service Affecting (W, SA)

Steps

1 Manually run the OTDR Go/No-Go trace.

If you want to perform the procedure using	**Then** go to the
CLI commands	"CLI INTERFACE STEPS"
Node Essentials	"NODE ESSENTIALS STEPS"

CLI INTERFACE STEPS

2 To manually run the OTDR Go/No-Go trace, enter the following CLI command:

```
start-otdr-trace name "slot-<slot number>-port-<instance name>" trace-type go-nogo
```

Note: The iC&L RLA has two CV instances on the same port, so the input is an instance name instead of port number.

3 Go to step 7.

NODE ESSENTIALS STEPS

4 Select **Tools** from the Node Essentials navigation menu.

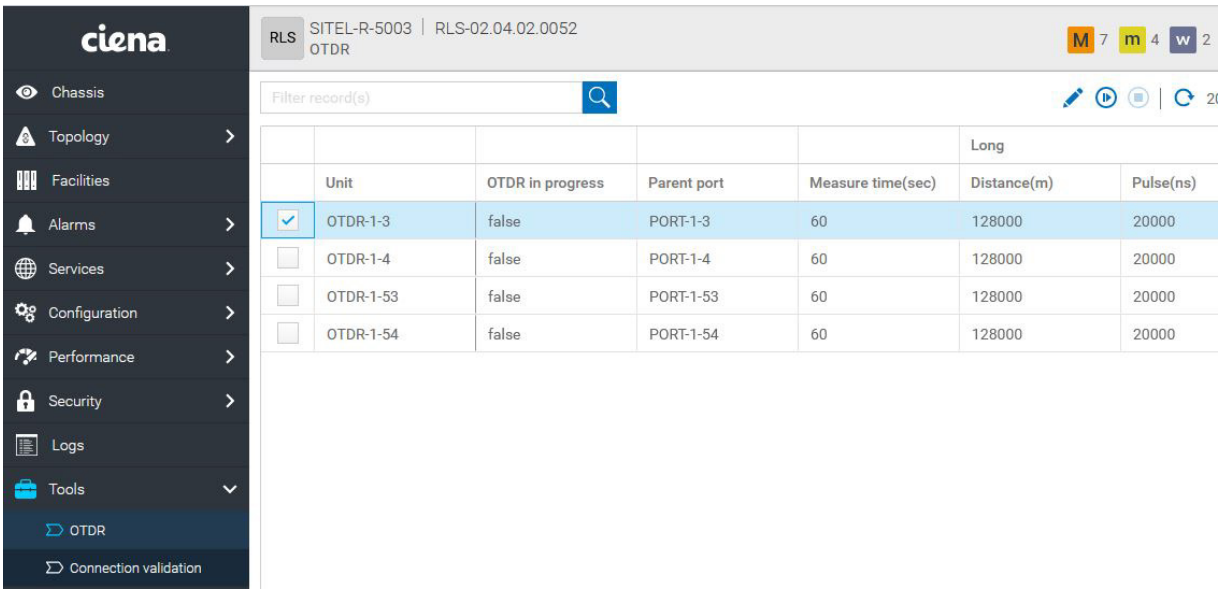
5 From the **Tools** menu, select OTDR.

The list of available OTDRs are displayed in the OTDR grid.

6 Select the **OTDR** that you want to run the OTDR Go/No-Go trace and click on the **Start trace** icon on the top right of the screen.

Copyright© 2019-2025 Ciena® Corporation

Figure 13 OTDR Go/No-Go trace



7 For more information regarding the OTDR and Go/No-Go traces, refer to *Optical Control, SPLI, and OTDR*, 323-2051-318.

8 If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 107 Remote Node Unreachable

Requirements

To perform this procedure, you must use an account with at least an Admin user access level.

Probable cause

This alarm can be raised in the following conditions:

- remote ILA or ROADM restart against the osrp-link facilities
- remote osrp (ROADM) or osrp-rls-ra (ILA) micro-service restarts (without the whole CTM restarting) (the alarm is raised and cleared in less than a minute)

For the inter-site osrplinks this alarm is raised when there is an issue with intermediate ILA site between this ROADM and the remote. For the inter-shelf OSRP links the root cause is the inter-shelf comms, usually ILAN but can be whatever is used for inter-shelf comms (for example, 3rd party switch or router).

Impact

Minor, non-service-affecting (m,NSA)

Steps

1 Retrieve the data for the active-alarm object:

If you want to perform the procedure using	**Then** go to the
CLI commands	"CLI INTERFACE STEPS"
Node Essentials	See the Node Essential steps in "Retrieving the data for the active alarm object" on page 32 in this document. Then go to step 3.

CLI INTERFACE STEPS

2 The following step is performed using CLI commands.

```
show active-alarm [id] [name] resource raise-time [clear-time] cause [condition-type] [direction] [location] severity service-impact [additional-info] [user-notes...]
```

Refer to "Alarm parameters" on page 27 for applicable parameters. Go to step 3.

3 Check for and clear any OSC or ILAN related alarms or service state.

4 For the inter-site, verify the local and far end ROADM shelf, and all intermediate ILA sites.

Copyright© 2019-2025 Ciena® Corporation

5. If the alarm does not clear, verify the datacomms setting of the port raising the alarm and compare it to the settings for the neighbor node. Both sides must have the same setting for the alarm to clear.
6. If the ports are not configured correctly, change appropriate side to the correct setting. Refer to Provisioning an OSRP node procedure in *6500 RLS L0 Control Plane*, 323-2051-330.
7. If the alarm does not clear, verify if the Line Module is in a reboot state, wait five minutes for the Line Module to complete the boot cycle.
8. If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 108 Remote Switch Mismatch

Requirements

To perform this procedure, you must use an account with at least an Admin user access level.

Probable cause

This alarm is raised when the traffic switches between a local and remote TPS are mismatched.

Impact

Minor, non-service-affecting (m, NSA)

Steps

1. Align the local and remote switches. The order of commands to clear varies depending on the circumstances that triggered the alarm. You can run a force switch to bring the switches back into alignment.

   Note: If the local TPS is currently running on switch 2, but the remote TPS is currently running on switch 1, execute a force switch on the local TPS to run on switch 1.

2. If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 109 reset-to-factory-default Check In Progress

Probable cause

The alarm is raised when the software reset to factory default check is In progress.

Impact

Warning, non-service-affecting (W, NSA)

Steps

1. No action is required. The alarm clears either when RTFD checks finish successfully or times out in which case, the “reset-to-factory Factory Release Check Failed” alarm is raised.
2. If the alarm is not clear, contact your next level of support or Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 110 reset-to-factory Factory Release Check Failed

Requirements

To perform this procedure, you must use an account with at least an Admin user access level.

Probable cause

The alarm is raised when the software factory release check is failed or when the reset to factory default check times out.

Impact

Warning, non-service-affecting (W, NSA)

Steps

1. Perform another RTFD. The alarm clears after a successful RTFD (clean-all true) operation (if factory release check passes).
2. If the operation keeps failing, attempt to put a good factory release on the CTM with the swmgr commands. Refer to “software-set-factory-release’ commands in *6500 RLS CLI Reference*, 323-2051-190 or call Ciena support to help install a correct factory release on the CTM.
3. If the alarm is not clear, contact your next level of support or Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 111 Section Calibration In-Progress

Probable cause

This alarm is raised when manual calibrating or re-calibrating is in progress.

Impact

Warning, non-service-affecting (W, NSA)

Steps

1. No action is required. The alarm clears when the calibration process is completed.
2. If the Section Calibration In Progress does not clear after the expected time-frame, check the span calibration orchestrator (SCO) to determine the current fsm-states of the nodes along the calibration path.

If you want to perform the procedure using	**Then** go to the
CLI commands	"CLI INTERFACE STEPS"
Node Essentials	"NODE ESSENTIALS STEPS"

CLI INTERFACE STEPS

3. To check the span calibration orchestrator (SCO) current state. Enter the following CLI command:

```
display table
action sco <name> show-oms-view
```

4. Review each of the nodes in the output of this command, their corresponding local-state, and their current-operation.
5. Calibration may not complete for a variety of reasons, including but not limited to: missing link configuration, amplifier shutoff, connection validation issues. Investigate the local configuration and alarms on the node or nodes in the section that do not have calibrated local-state.
6. Check if a "Node Unreachable" alarm is raised in the section. Refer to "Node Unreachable" alarm clearing procedure for more details.
7. Go to step 14.

NODE ESSENTIALS STEPS

8. From the **Topology** menu, select Photonic functional groups.
9. Place the cursor over the Calibration status icon of the calibrated PFG to display the calibration information in the pop-up box.

   Note: If the alarm is active, the Calibration status icon is either yellow or red.

   The icon is yellow when the Local state is calibrated but Section state is calibrating. The icon is red when the Local state and Section state are both calibrating.

Copyright© 2019-2025 Ciena® Corporation

10 If the LINE-DEMUX fsm-state is stuck in “wait-upstream-calibrated”, the problem is unrelated to the local circuit pack and troubleshooting must take place on the upstream LINE-MUX.

11 If the LINE-DEMUX fsm-state is stuck in “wait-raman-directed”, then the go-nogo trace yielded a “nogo”. verify if another alarm causing the “nogo” status and clear the alarm using alarm clearing procedures in this document.

12 If the LINE-DEMUX fsm-state is “wait-raman-pump-on”, contact your next level support and continue troubleshooting the fault/failure.

13 If the alarm is raised on the TPS configuration, verify if the “Low Optical Return Loss” alarm is raised on the AMP facility under calibration. If yes, clear the alarm following the “Low Optical Return Loss” alarm clearing procedure. Once the “Low Optical Return Loss” alarm is cleared, the SCO “local-state” will get out of the “amp configuring” state to the next state.

Note: The Automatic Power Reduction Active (APR) alarm can prevent the calibration to complete. The user needs to perform another recalibration after clearing this alarm. Refer to “Automatic Power Reduction Active” alarm procedure to clear the alarm and the *6500 RLS Optical Control, SPLI, and OTDR*, 323-2051-318 for more information.

14 If the alarm is not clear, contact your next level of support or Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 112 Section Degraded

Requirements

To perform this procedure, you must use an account with at least an Admin user access level.

Probable cause

This alarm is raised if measured spectrum is dropped or heavily tilted at the pre-amp out location beyond a threshold (max-profile-error-threshold) with default value of 4dB, consistently for two minutes. This prevents a channel add on the next mux and hence, prevents the mission critical restoration. This alarm is to notify that the section has run out of its dynamic range and the threats against future channel restorations.

This alarm clears when the following conditions are met on the power profile:

`max-profile-error < max-profile-error-threshold + max-profile-error-hysteresis`

AND

`total-power-unachievable` diagnostics is `false`

The error in the measured spectrum should be less than hysteresis (max-profile-error-hysteresis) with a default value of 2dB from the max-profile-error-threshold.

This alarm masks the corresponding local pTU (Target Unachievable) alarm.

This alarm is `inhibited` by default when upgrading (brown-field deployments) to release 4.0. After the upgrade is completed, Ciena strongly recommends to manually enable this alarm by using the following command:

```
set changed-alarms section-degraded template-state
enabled
```

This alarm is `enabled` by default on any fresh (greenfield) deployments.

Impact

Major, service-affecting (M, SA)

Steps

1. Clear any “High Fiber Loss” alarm within the OMS. Refer to “High Fiber Loss” alarm clearing procedure in this document.
2. If the alarm is persistent even after clearing “High Fiber Loss” alarms, re-calibrate the section.

Copyright© 2019-2025 Ciena® Corporation

3 If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 113 Secure Erase Completed

Requirements

To perform this procedure, you must:

- have a replacement module. Review “Ordering information” in *6500 RLS Planning Guide*, NTRN10WA, to make sure you select the correct replacement part.
- observe all safety requirements described in *6500 RLS Shelf Installation Guide,* 323-2051-201

CAUTION
Risk of equipment damage
Electrostatic discharge (ESD) can damage electrostatic sensitive devices. You must use antistatic protection while unpacking and installing all Field-Replaceable Units (FRU) and cables.

Probable cause

This alarm is raised when the secure erase operation is completed successfully.

Impact

Warning, non-service-affecting (W, NSA)

Steps

1. Remove or cold restart the module to clear the alarm. Refer to “Restarting an interface module or the CTM” on page 37 of this document for instructions.
2. If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 114 Secure Erase Failed

Requirements

To perform this procedure, you must:

- have a replacement CTM module. Review “Ordering information” in *6500 RLS Planning Guide*, NTRN10WA, to make sure you select the correct replacement part
- observe all safety requirements described in *6500 RLS Shelf Installation Guide,* 323-2051-201

CAUTION
Risk of equipment damage
Electrostatic discharge (ESD) can damage electrostatic sensitive devices. You must use antistatic protection while unpacking and installing all Field-Replaceable Units (FRU) and cables.

Overview

This alarm is raised when the secure erase operation fails to complete successfully.

Impact

Major, non-service-affecting (M, NSA)

Steps

1. Replace the impacted CTM. Refer to Procedure 140, “Replacing a Control and Timing Module (CTM)”.

   Note: If you perform a Secure Erase on the CTM and the secure erased module is returned to Ciena, there is no information remaining on the module that can be used for analysis or troubleshooting.

2. If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 115 Secure Erase In Progress

Probable cause

This alarm is raised when the secure erase action is initiated on a circuit pack. The alarm is active for the duration of the secure erase operation and clears when the secure erase is completed.

Impact

Warning, non-service-affecting (W, NSA)

Steps

1. No action is required. The alarm clears after the Secure Erase action is completed.
2. If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 116 Shutoff Threshold Crossed

Requirements

To perform this procedure, you must:

- log into the CLI of the nodes with admin or higher privilege level. For login information, see “Accessing and logging in to a network element” procedure in *Licensing, Security, and Administration*, 323-2051-300.
- observe all safety requirements described in *6500 RLS Shelf Installation Guide,* 323-2051-201
- have a network and site diagram
- have a fiber cleaning kit
- have the Shutoff threshold level for this amplifier

Probable cause

This alarm is raised against an AMP facility when the total input optical power to the amplifier has fallen below the provisioned Shutoff Threshold level. The conditions that can cause the input power level to fall below the threshold level include:

- a disconnected fiber
- a pinched fiber connection
- a dirty optical fiber connector
- a defective fiber optic patchcord
- a defective module
- an incorrect provisioned value
- the incoming channel frequency on the CCMD port does not match the provisioned frequency for that port

This alarm can remain active after the fault has cleared and the original power level is restored. This occurs when the power level is lower than the user-provisioned Shutoff threshold plus the hysteresis value. The hysteresis value is not user provisionable and is set at 3 dB.

Impact

Major, service-affecting (M, SA)

Steps

1 Place the alarmed AMP facility to “Disabled”.

If you want to perform the procedure using	**Then** go to the
CLI commands	“CLI INTERFACE STEPS”
Node Essentials	“NODE ESSENTIALS STEPS”

Copyright© 2019-2025 Ciena® Corporation

CLI INTERFACE STEPS

2 To place the alarmed AMP facility to “Disabled”. Enter the following command:

```
set slots <name> config amps <name> [admin-state
<Disabled>]
```

3 Go to step 11.

NODE ESSENTIALS STEPS

4 Select **Facilities** from the Node Essentials navigation menu.

The Facilities menu opens.

5 From the **Equipment** grid, select the module with the alarmed AMP facility.

The bottom part of screen becomes populated.

6 Select AMP facility from Facility navigator.

The AMP Facilities grid opens.

7 Select the alarmed AMP facility by Row selector from the AMP Facilities grid.

8 Click the **Pencil** icon.

The related Edit AMP dialog opens.

9 Edit the Admin state of the AMP facility to Disabled.

10 Click **Confirm**.

11 Clean and then reconnect the input fibers and connectors at the amplifier or CMD. Refer to *Optical Connector Inspection and Cleaning*, 323-1859-500.

12 Place the amplifier back to “Enabled”.

13 If the alarm still persists, check the upstream connection for mating or pinched fibers.

14 If the alarm does not clear, verify the actual Tx center frequency is properly tuned on the transponder matching exactly the center frequency of the NMC or SNC provisioned on the CCMD Tx/Rx port.

15 If the alarm does not clear, restart the amplifier or CMD module supporting the alarmed AMP facility. Refer to Procedure 5, “Restarting an interface module or the CTM”.

16 If the alarm does not clear, gather the following diagnostic information and contact your next level of support or your Ciena support group. Refer to *6500 RLS CLI Reference*, 323-2051-190 for the CLI commands.

a. Amp config and inventory data raising the alarm

b. Immediate upstream power data

— Upstream amp config and inventory data (if upstream amp present)

— Upstream voa config and inventory data (if upstream voa present)

— Upstream pwrmon inventory data (e.g. line in/out ports)

— Upstream optmon inventory data facility (e.g. CCMD ch-in ports, RLA/LRU switch ports, SRA ports)

c. Preceding link data

d. other local alarms

Copyright© 2019-2025 Ciena® Corporation

e. upstream alarms

Copyright© 2019-2025 Ciena® Corporation

Procedure 117 SID Fault

Requirements

To perform this procedure, you must:

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *6500 RLS Shelf Installation Guide*, 323-2051-201.
- have an antistatic wrist strap to dissipate electrostatic charges.

CAUTION
Risk of equipment damage
Wear an antistatic wrist strap to protect the equipment from static damage. Connect the wrist strap to the ESD jack on the shelf or module.

CAUTION
Risk of traffic loss
A cold restart on an unprotected module causes traffic loss. A cold restart on an active protected module causes a protection switch that impacts traffic.

Probable cause

This alarm is raised when the shelf identifier unit on the backplane is failed, is missing, has invalid data, or cannot be read. This alarm is also raised when the inventory data cannot be retrieved from a shelf.

Impact

Minor, non-service-affecting (m, NSA)

Steps

1 Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.

2 Choose your next step:

If the alarm is raised against a	**Then** go to
simplex CTM	step 3
duplex CTM	step 5

3 Cold Restart the CTM. Wait five minutes for the CTM to restart. Refer to Procedure 5, “Restarting an interface module or the CTM”.

4

If the alarm is	**Then**
cleared	this procedure is complete.
no cleared	go to step 8

Copyright© 2019-2025 Ciena® Corporation

5. Perform a cold restart on the active CTM. This causes an automatic protection switch of the CTM. Refer to Procedure 5, “Restarting an interface module or the CTM”.
6. If the alarm is cleared, perform a cold restart on the newly active CTM. This causes an automatic protection switch back to the originally active CTM. This procedure is complete.
7. If the alarm is not clear, re-seat or cold restart the active CTM. This causes an automatic protection switch of the CTM.
8. If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 118 Slot Empty

Requirements

To perform this procedure, you must:

- observe all safety requirements described in the “Observing product and personnel safety guidelines” section in *6500 RLS Shelf Installation Guide*, 323-2051-201
- obtain a filler card or a module to install in the empty slot

Probable cause

This alarm is raised on a CTM/IM the card slot when card is not present and not provisioned, or the card is provisioned and the admin-state is “Disabled”.

ATTENTION

You must install filler cards in all slots that do not contain a module to ensure sufficient air flow for cooling the shelf. Failure to do so can cause the shelf to exceed the maximum temperature, which may cause component damage.

Impact

Minor, non-service-affecting (m, NSA)

Steps

1 Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.

2 Identify the module raising the alarm:

If you want to perform the procedure using	**Then** go to the
CLI commands	“CLI INTERFACE STEPS”
Node Essentials	See the Node Essential steps in “Retrieving the data for the active alarm object” on page 32 in this document. Then go to step 4.

CLI INTERFACE STEPS

3 The following step is performed using CLI commands.

```
show active-alarm [id] [name] resource raise-time [clear-time] cause [condition-type] [direction] [location] severity service-impact [additional-info] [user-notes...]
```

Refer to “Alarm parameters” for applicable parameters. Go to step 4.

Copyright© 2019-2025 Ciena® Corporation

4

If	Then
the slot is empty	insert a module or a filler card of the correct type into the slot. Go to step 5.
otherwise	go to step 6.

5 Wait 30 seconds and retrieve all alarms to determine if the original alarm has cleared.

If the original alarm has	**Then**
cleared	the procedure is complete
not cleared	go to step 6

6 Ensure that the card is provisioned and the admin state is “Enabled”.

7 If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 119 Snc Datapath Fault

Requirements

To perform this procedure, you must use an account with at least an Admin user access level.

Probable cause

This alarm is raised when the datapath is down for an Snc because the underlying Channel Control Service has not achieved the end-to-end In-service state within the provisioned “Datapath fault alarm timer period” (default is 15 minutes).

If you do not want the Snc to raise the “Snc Datapath Fault” alarm, you must set the Snc Datapath Fault timer to 0 before bringing the Snc into service.

When an Snc enters to the working state, the OSRP starts Snc monitoring by querying at each hop along the Snc for the channel state in the Channel Control Service that corresponds to the Snc. OSRP continues the query periodically until a timer expires (default is 15 minutes) or all hops are in-service. If all hops are not in-service within 15 minutes, the alarm is raised against the Snc facility.

Impact

Major, service-affecting (M, SA)

Steps

1 Identify the Snc raising the alarm:

If you want to perform the procedure using	**Then** go to
CLI commands	step 2
Node Essentials	See the Node Essential steps in “Retrieving the data for the active alarm object” on page 32. Then go to step 3.

2 To identify the Snc raising the alarm using CLI commands, enter:

```
show active-alarm <id> [name] [resource] [raise-time]
[raise-time] [cause] [condition-type] [direction]
[location] [severity] [service-impact] [additional-info]
[user-notes...]
```

3 Verify the End to End diagnostics to view the faults that raised the alarm. Enter:

```
action osrp <osrp-node-name>:<PFG> object snc <snc-name>
show-end-to-end-channel-diagnostics
```


Copyright© 2019-2025 Ciena® Corporation

4 If the alarm is raised due to a channel not being added properly along the path in the Channel Control Service, identify the node and view the Channel Control Service related alarms. See step 1. Enter:

```
show ccs-instance <PFG> (Where PFG should be indicated by
the active alarms)
```

Clear these alarms before continuing this procedure.

5 Check the presence of HFL alarm on any of the ROADM intra-site fiber links including (1) CCMD to RLA/LRU in the add direction, (2) RLA to RLA or (3) LRU to LRU. If HFL alarm is raised on any of the locations, clear the alarm by following the "High Fiber Loss" on page 119 alarm clearing procedure.

6 If the end to end diagnostic information indicates Rx Fault for the Snc on the transponder link, Loss of Signal, or Loss of Clock, then clear these alarms.

7 If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 120 Snc Unavailable

Requirements

To perform this procedure, you must use an account with at least an Admin user access level.

Probable cause

This alarm is raised when the terminating Subnetwork Connection (SNC) is in the creating or starting state. For MR-SNCs, it is typically caused by an underlying fault with the destination. For example, insufficient bandwidth, missing or faulty physical facility at the destination or by mis-provisioned far-end address.

Impact

Critical, service-affecting (C,SA)

Steps

1 Identify the node raising the alarm and note any additional information:

If you want to perform the procedure using	**Then** go to the
CLI commands	"CLI INTERFACE STEPS"
Node Essentials	See the Node Essential steps in "Retrieving the data for the active alarm object" on page 32 in this document. Then go to step 3.

CLI INTERFACE STEPS

2 The following step is performed using CLI commands.

```
show active-alarm <id> [name] [resource] [raise-time]
[raise-time] [cause] [condition-type] [direction]
[location] [severity] [service-impact] [additional-info]
[user-notes...]
```

3 If the SNC raising the alarm is recently added, verify the end-to end provisioning. If mis-provisioning is identified, delete and re-create the SNCG.

```
show osrp <osrp-node-name>:<PFG> object snc <snc-name>
```

4 If the alarm does not clear, verify if any equipment alarms are raised against circuit packs carrying the SNC. If there are, clear these alarms before continuing this procedure.

5 Verify whether a current route is available (listed).

6

If the current route is	**Then** go to
available	step 7
not available	step 9

Copyright© 2019-2025 Ciena® Corporation

7 View the provisioned SNCG and note the member SNCs. From the SNCG configuration, note the nodes and ports of the home route. Enter:

```
show osrp <osrp-node-name>:<PFG> object snc-group <SNCG-name> route-list
```

8 Verify if any equipment alarm exist. If there are, clear these alarms. Go to step 10.

9 Verify the SNC Status Diagnostic. Enter:

```
action osrp <osrp-node-name>:<PFG> object snc <snc-name> show-snc-diagnostics
```

Refer to “Displaying and clearing SNC/SNCG diagnostics information” procedure in *6500 RLS L0 Control Plane*, 323-2051-330.

10

If the route is	**Then**
available	go to step 11
not available	establish a route

11 If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 121 Snc-Group Not Mesh-Protected

Requirements

To perform this procedure, you must use an account with at least an Admin user access level.

Probable cause

This alarm is raised against a dynamic snc-Group with mesh-protection = yes when it has no available protection paths.

This alarm is a secondary alarm raised to identify services that are mesh-restorable but have no protection paths available. It indicates there is currently no trouble with the service, but in the event of a fault, the service cannot restore.

Impact

Warning, non-service-affecting (W, NSA)

Steps

1. The alarm is cleared within 5 minutes of a protection path becoming available.
2. Verify which DTL-SET the alarming SNCG is using with the following command.

   ```
   show osrp <osrp-node-name>:<PFG> object snc-group <sncg-name>
   ```

3. Investigate the protect and non-working DTLs that are configured within the DTL-SET attached to the alarming SNCG using the following command. Take note of any errors that are shown after validation is run. If any errors are shown, investigate the location in the validation output.

   action osrp <osrp-node-name>:<PFG> object dtl <dtl-name> validate

4. If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 122 Snc-Group Not on Home Path

Requirements

To perform this procedure, you must use an account with at least an Admin user access level.

Probable cause

This alarm is raised on an Snc-Group (SNCG) after a restoration event and the SNCG is not on its home path.

This alarm is a secondary alarm raised to identify services impacted by a network fault event. The alarm is raised when SNCGs recover from a fault by mesh restoring to a protection path and cleared when the SNCG is either put administratively out of service, or the SNCG reverts back to its home path.

This alarm is also raised if the SNCG is not on the home path because the user performed a Manual Switch. If the home path is available the alarm can be cleared by performing a Revert or another Manual Switch (back to home path).

Impact

Warning, non-service-affecting (W, NSA)

Steps

1 Identify what the current working path is for the alarming SNCG.

2 Show active alarms:

If you want to perform the procedure using	**Then** go to
CLI commands	step 2
Node Essentials	See the Node Essential steps in "Retrieving the data for the active alarm object" on page 32. Then go to step 6.

3 To identify the active alarms using CLI commands, enter:

```
show active-alarm <id> [name] [resource] [raise-time]
[raise-time] [cause] [condition-type] [direction]
[location] [severity] [service-impact] [additional-info]
[user-notes...]
```

4 Using the SNCG name, issue the following command to identify the current "working-route" and the "home-route.

```
show osrp <osrp-node-name>:<PFG> object snc-group <SNCG-
name> route-list
```


Copyright© 2019-2025 Ciena® Corporation

5 Investigate the home-path using the following command, specifying the home-path DTL identified in step 4. Review the output of the DTL validation to pinpoint where any outstanding issues are along this route.

```
action osrp <osrp-node-name>:<PFG> object dtl <dtl-name>
validate
```

6 If the SNCG is provisioned to automatically revert to the home path, the alarm will clear when the SNCG reverts itself. Otherwise, verify that the SNCG home path is available, and revert the SNCG back on home path.

> **CAUTION**
> **Risk of traffic loss**
> Reverting the SNCG will cause the channel to go down for several minutes.

7 If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 123 Snc-Group Unavailable

Requirements

To perform this procedure, you must use an account with at least an Admin user access level.

Probable cause

This alarm is raised when the terminating Subnetwork Connection Group (SNCG) is in the creating or starting state. For MR-SNCGs, it is typically caused by an underlying fault with the destination. For example, insufficient bandwidth, missing or faulty physical facility at the destination or by mis-provisioned far-end address.

Impact

Critical, service-affecting (C,SA)

Steps

1 Identify the node raising the alarm and note any additional information:

If you want to perform the procedure using	**Then** go to the
CLI commands	"CLI INTERFACE STEPS"
Node Essentials	See the Node Essential steps in "Retrieving the data for the active alarm object" on page 32 in this document. Then go to step 3.

CLI INTERFACE STEPS

2 The following step is performed using CLI commands.

```
show active-alarm <id> [name] [resource] [raise-time]
[raise-time] [cause] [condition-type] [direction]
[location] [severity] [service-impact] [additional-info]
[user-notes...]
```

3 Verify the SNCG diagnostics information using CLI command.

```
action osrp <osrp-node-name>:<PFG> object snc-group
<sncg-name> show-snc-group-diagnostics
```

Refer to "Displaying and clearing SNC/SNCG diagnostics information" procedure in *6500 RLS L0 Control Plane*, 323-2051-330.

4 If the SNCG raising the alarm is recently added, verify the end-to end provisioning. If mis-provisioning is identified, delete and re-create the SNCG.

```
show osrp <osrp-node-name>:<PFG> object snc-group <SNCG-
name> route-list
```

Refer to "Displaying and clearing SNC/SNCG diagnostics information" procedure in *6500 RLS L0 Control Plane*, 323-2051-330.

Copyright© 2019-2025 Ciena® Corporation

5 If the alarm does not clear, verify if any equipment alarms are raised against circuit packs carrying the SNCG. If there are, clear these alarms before continuing this procedure.

6 Display the SNCG route list.

```
show osrp <osrp-node-name>:<PFG> object snc-group
<SNCGname> route-list
```

7

If the current route is	**Then** go to
available	step 8
not available	step 11

8 View the provisioned SNCG and note the member SNCs. From the SNC list, note the nodes and ports of the home route.

```
show osrp <osrp-node-name>:<PFG> object snc-group <SNCG-
name>
```

Refer to “Displaying and clearing SNC/SNCG diagnostics information” procedure in *6500 RLS L0 Control Plane*, 323-2051-330.

9 Validate the home and protect routes that are configured for the alarming SNCG using the following command. Based on the output, as well as the SNCG diagnostic data collected in step 3, pinpoint the location along the desired route where equipment may be encountering an issue.

```
action osrp <osrp-node-name>:<PFG> object dtl <dtl-name>
validate
```

10 Verify if any equipment alarm exist. If there are, clear these alarms. Go to step 13.

11 Verify the SNCG Status Diagnostic.

```
action osrp <osrp-node-name>:<PFG> object snc-group
<sncg-name> show-snc-group-diagnostics
```

Refer to “Displaying and clearing SNC/SNCG diagnostics information” procedure in *6500 RLS L0 Control Plane*, 323-2051-330.

12 If the event detail currently indicates failures or errors, stop the procedure and contact your network administrator.

13 If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 124 Software Deliver Failed

Requirements

To perform this procedure, a user must have an account with at least admin access privileges.

Probable cause

This alarm is raised when the software-deliver process failed.

Impact

Minor, non-service-affecting (M, NSA)

Steps

1. Verify the IP reachability to the release server (ping, SSH, or SFTP).
2. Re-deliver the software release load to the shelf, if the IP server is reachable, by executing the following command:

   ```
   software-deliver uri <value>
   ```

   ```
   URI format to deliver the software load file stored
   remotely is: <sftp|scp>://
   <userid>:<password>@<host>[:port]/<directory path>/<RLS-
   xx.yy.zz.bbbb.tgz (where xx.yy.zz is the RLS release
   number and bbbb is the unique build number)
   ```
3. If the alarm does not clear or the alarm is raised again due to subsequent deliver attempt, cancel the software-deliver process.

   ```
   software-cancel
   ```
4. Contact your next level of support or your Ciena support group for necessary actions.

Copyright© 2019-2025 Ciena® Corporation

Procedure 125 Software Release Unknown

Requirements

To perform this procedure, log into the CLI with an access level of Limited or higher.

Probable cause

This alarm is raised when a software release is UNKNOWN on the system. A version of UNKNOWN signifies an upgrade is required.

If this alarm is encountered during a greenfield deployment, see the “Software Upgrade Procedures” document for the upgrade procedures. If this occurs during a brownfield deployment or raises outside of a deployment activity, the recommended steps must be performed during a maintenance window.

Impact

Minor, non-service-affecting (m, NSA)

Steps

1. Retrieve the software release and upgrade information. Refer to “Retrieving software release and upgrade information” in *6500 RLS Licensing, Security, and Administration*, 323-2051-300.

   CAUTION
   Risk of traffic loss
   The following steps will impact traffic. If possible, re-route the traffic to minimize the traffic loss.

2. Upgrade the shelf software. Refer to “Upgrading a shelf software load (one-step)” procedure in *6500 RLS Licensing, Security, and Administration*, 323-2051-300.
3. If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 126 Software Service Inactive

Probable cause

This alarm is raised when a software system internal to the CTM was automatically shut down due to an internal problem, or was not able to start due to an initialization problem.

Impact

Major, service-affecting (M, SA)

Steps

1. Retrieve the system logs on the RLS shelf. Enter the following CLI command:

   `retrieve-logs slots ALL mode full`

2. Contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 127 Software Subsystem Failure

Requirements

To perform this procedure, you must use an account with at least an Admin user access level.

Probable cause

This alarm is raised when a module has a software failure that cannot be recovered on its own or when a module fails to boot up after few attempts.

For the SSM this alarm is raised when the communication between OCM/host or POM/host is lost.

The alarm is also raised after the system upgrade to RLS2.6 with addition text “CV SFP STUCK”.

This alarm is also raised if the amp target-power is set too low such that the measured “gain” (delta between out-current-power and in-current-power) is reported to be 0 (zero).

Impact

Major, non-service-affecting (M, NSA)

Steps

1 If the alarm is raised with “CV SFP STUCK”, contact your next level of support or your Ciena support group.

2 If the alarm is raised when the measured “gain” (delta between out-current-power and in-current-power) is reported to be 0, contact your next level of support or your Ciena support group.

3 Perform a diagnose equipment CLI command to evaluate alarm on the effected module. See the example below:

```
rls# action slots <slot|all> diagnose-equipment
```

The command have the following options:

```
<all> re-evaluate circuit pack failed alarm on all
equipment on the shelf
```

```
<slot> re-evaluate circuit pack failed alarm on a
particular slot on the shelf
```

If Diagnose Equipment is successful and the slot is in “ok” status, the alarm for that slot clears.

4 If the alarm did not clear, perform a protection switch on the module. Refer to the “Protection configurations and CTM redundancy” procedure in *Equipment/Facility Provisioning and Protection*, 323-2051-310.

Copyright© 2019-2025 Ciena® Corporation

5 If the alarm does not clear, reseat the module. Refer to Procedure 138, “Reseating a module” in the “Module replacement” section in this document.

6 If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 128 Spectral loading degraded

Requirements

To perform this procedure, you must use an account with at least an Admin user access level.

Probable cause

This alarm is raised against line-out Power Profile at ROADM locations only (line-mux PFG) when the power delta between current and baseline ASE spectra is more than 10 dB (default value, provisionable) over a spectrum slice with a minimum size of 25 GHz (default value, provisionable). Narrow gaps (< 25 GHz) not to be counted.

This alarm can raise due to gaps adjacent to BU filter. In this case, the alarm can be inhibited if needed. The alarm can also be raised and cleared when the capacity changes are completed. No action is required in this case.

Impact

Minor, non-service affecting (m, NSA)

Steps

1 Select your next step.

If	**Then** go to
the loopback is in progress	step 2
ASE replacement is disabled	step 3
restricted PFG is used	step 4

2 Ensure no channel is being added. If an ASE replacement is in progress, cancel the loopback until the channels are added or re-added and then try the loopback again.

3 Enable the ASE replacement feature to ensure no gaps in spectrum.

4 If range has been changed since the initial deployment, a recalibrate command should be performed to calibrate with proper range.

5 If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 129 Syslog Server(s) Unavailable

Requirements

To perform this procedure, you must log into the CLI of the nodes with admin or higher privilege level. For login information, See “Accessing and logging in to a network element” in *Licensing, Security, and Administration*, 323-2051-300.

Probable cause

The alarm is raised when Syslog server(s) are provisioned but unreachable.

Impact

Minor, non-service-affecting (m, NSA) if all provisioned Syslog servers are unreachable

Warning, non-service-affecting (W, NSA) if at least one provisioned Syslog server(s) is unreachable and at least one other provisioned Syslog server is reachable

Steps

1. Identify the provisioned unreachable Syslog server from the alarm and its additional info field.
2. Ensure the provisioned Syslog server(s) are up and running.
3. If the provisioned Syslog server(s) has been decommissioned or has a wrong IP address provisioned, correct or delete its IP address in the node.
4. Verify the connection between the alarmed node and the alarmed SYSLOG Server(s) and re-establish the connection if needed.
5. If TLS is provisioned for Syslogs, verify that its certificate is still valid, activated and committed. Upload and commit a new certificate if needed.
6. If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 130 TACACS Server(s) Unavailable

Requirements

To perform this procedure, you must use an account with at least a Super user access level.

Probable cause

This alarm is raised when the server is not reachable and all requests to the server times out. The alarm clears when connectivity is re-established between the shelf and any enabled TACACS+ server.

Impact

Major, non-service-affecting (M, NSA)

Steps

1 The alarm clears when connectivity is re-established between the shelf and the TACACS server. If the alarm does not clear, perform one of the following:

- clear the security alarms. Refer to appropriate alarm clearing procedures in this document.
- disable TACACS. Refer to “Displaying and provisioning TACACS+ attributes” procedure in *Licensing, Security, and Administration*, 323-2051-300.

2 If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 131 Target Unachievable

Requirements

To perform this procedure, you must:

- use an account with at least an Admin user access level
- observe all safety requirements described in *6500 RLS Shelf Installation Guide,* 323-2051-201
- obtain a fiber patchcord, if required

Probable cause

This alarm is raised on any of the following facilities, when the target power is not achieved within a given threshold:

- Channel Controller (ccs-instance)
- Spectrum Power Profile (target line-out, baseline line-in, baseline Pre-Amp out)
- OSC Add Power
- RAMAN Gain

Here are the details for each facilities in the following sections (including Node Essentials in each section), followed by Alarm masking behavior in each section.

Alarm raised against channel controller

This alarm is raised against the channel controller provisioned on a section-mux PFG when the difference between the “measured-power” and the “expected-power” at the output showing in the “ccs-instance” (see the examples below) are greater than the provisioned “target-power-alarm-threshold” on the CCS-instance config data.

Sources of power error can be caused by:

- Tx power at channel-mux add port not matching the target power published under tx-proxy (for example; due to excess loss between Tx and CMD add port)
  - — power delta can be visible by comparing add port optmon power reading versus tx-proxy target-power
  - — Optical Power Degrade Low alarm is expected if the tx power delta is greater than default 2dB.
- excess loss between CCMD/CMD to RLA fibers
  - — power delta can be visible from RLA/LRU inventory pwrmon nmcmon-<switch-in> facilities for measured versus expected powers
  - — similar delta can also be seen from mux channel-controller instances

Copyright© 2019-2025 Ciena® Corporation

The input power delta needs to be verified to clear the alarm.

CLI Example:

The following shows an example of channel controller instance as visible in CLI.

As explained, when the channel-power/output shows a delta between measured-power and expected-power by > target-power-alarm-threshold, the target-unachievable diagnostic is set to true.

```
show ccs-instance SEC-MUX-1 channel-controller 191381.250
  ccs-instance:  - name   : SEC-MUX-1
    channel-controller:
    - center-frequency         : 191381.250
      spectral-width           : 101.800
      nmc-instance             : ciena-6500r-slots:slots 1 config link '30
101' mc RLAMUX-1-30-MC-1 nmc 22000-STR10-STR12-5-2-5-2-191381.250fc
      operational-state        : in-service
      additional-info          :
      control-mode             : power
      channel-power:
        input:
          port-instance    : ciena-6500r-slots:slots 1 config port 30
          measured-power   : 4.46
          expected-power   : 3.73
        output:
          port-instance    : ciena-6500r-slots:slots 1 config port 100
          measured-power   : 4.48
          expected-power   : 4.55
      attenuation-adjustment   : -0.10
      config:
        target-power-alarm-threshold   : 2.00
        closed-loop                    : enabled
        ase-replacement-holdoff        : 0
        max-undershoot-compensation    : 3.00
        ase-replacement-trigger        : fault-state
        max-compensation-mode          : control-range-limited
      diagnostic:
        target-unachievable       : false
        capacity-change-pending   : false
```

Alarm masking behavior of Channel "Target Unachievable" alarm
When there is a fiber fault occurs such as fiber disconnection, unexpected fiber loss raising “High-fiber-loss” alarm, alarm correlation masks all the downstream channel-related “Target Unachievable” alarms, and also masks "Target Unachievable" alarms on all downstream spectrum power profiles. Alarms are similarly masked if the associated module/card admin-state is disabled, missing or mismatched.

Channel “Target Unachievable” alarms mask downstream channel “Target Unachievable” alarms for the same channel along the entire channel path.

Copyright© 2019-2025 Ciena® Corporation

Channel Controller using Node Essentials:
The data is available in Node essentials by choosing Topology -> Photonic functional groups, then select the corresponding LINE PFG and click on View spectrum icon on the top right of the screen. The data is displayed when a channel is selected in the graph.

The default alarm threshold is 2 dB with a 0.5 dB hysteresis. The alarm threshold is provisionable, but the hysteresis is neither visible nor provisionable. This means that the alarm is raised when the “measured-power” at the output is greater or less than the “expected-power” at the output by 2.0 dB (default value). The alarm is cleared when the difference becomes less than +/- 1.5 dB (2 - 0.50 db). If this power delta was previously >1.5 dB but less than < 2db, and a fault happens to cause the output power to drop below the 2.0 dB threshold, this alarm will be raised. But after the fault has cleared and even if the measured output power comes back to the previous value that is 1.5dB < (channel-power delta) < 2dB, the alarm does not clear since hysteresis to clear is 0.5 dB.

Alarm raised against spectrum power profiles
This alarm is raised per band against spectrum power profile instances (such as target or baseline pwr-profiles/band) if any of the following is/are true:

- total-power-unachievable
- tilt-unachievable
- mean-psd-unachievable

The “Target Unachievable” alarm is cleared when all the above diags are false. total-power-unachievable diag will have a hysteresis of 3dB and the mean-psd-unachievable diag will have a hysteresis of 0.5dB.

Hold-off/hold-on timer for mean-psd-unachievable is 120s and 15s, respectively.

On an upgrade from previous releases to Release 3.3 or higher:

- total-pwr-delta-threshold on all profiles are transferred to evaluate mean-psd-delta-threshold.

  Note: The mean-psd-delta-threshold default is 2dB, unless modified prior to upgrade.

- A new threshold is set for total-pwr-delta-threshold = 10dB.
- mean-psd is calculated for a given slot / config / pwr-profile (target or baseline) and populated.
- measured mean-psd is available under slot / inventory / pwr-profile.

Copyright© 2019-2025 Ciena® Corporation

The alarm is currently supported on the following pwr-profile locations:

- line-out / case-out: alarm is raised comparing target pwr-profile and measured spectrum, where measured spectrum comes from SDMON associated with the given port
- line-in / case-in / pre-amp-out: alarm is raised comparing baseline pwr-profile and measured spectrum, where baseline pwr-profile is automatically taken at section-calibration time, and measured spectrum comes from SDMON associated with the given port

The alarm can be raised for the following criteria:

- Total power: if total-power of measured power profile < > total-power of target/baseline power profile, by more than total-pwr-delta-threshold.

  Default total-pwr-delta-threshold = 10dB (provisionable), with alarm clear hysteresis of 3dB.
- Spectrum-tilt: if tilt from measured power profile < > tilt from target/baseline power profile, by more than tilt-alarm-threshold.

  Default tilt-alarm-threshold = 2.5dB (provisionable), with alarm clear hysteresis of 0.5dB.
- Mean power spectral density (mean-psd): if mean-psd from measured power profile < > mean-psd from target/baseline power profile, by more than mean-psd-delta-threshold.

  Default mean-psd-delta-threshold = 2dB (provisionable), with alarm clear hysteresis of 0.5dB.

Both mean-psd and spectrum-tilt are derived from the effective operating spectrum after filtering out any spectrum-holes (that are > 25GHz wide has per bin power delta of > 10dB between configured and measured powers).

Alarm masking behavior of power profile “Target Unachievable” alarm

The scope of profile “Target Unachievable” alarm masking is limited within one optical multiplex section (OMS) where the TU alarm is raised, not beyond the OMS boundary. OMS boundary is within section-mux to section-demux.

The Profile “Target Unachievable” alarm masking is on per spectrum band basis. The upstream profile “Target Unachievable” alarm masks downstream profile “Target Unachievable” alarm per band in the same direction.

- Upstream profile “Target Unachievable” alarm on C-band only masks downstream profile “Target Unachievable” alarm on C-band.

- Upstream profile “Target Unachievable” alarm on L-band only masks downstream profile “Target Unachievable” alarm on L-band.

Copyright© 2019-2025 Ciena® Corporation

AMP related alarms are raised on a per band basis. If any AMP alarms are raised for C and/or L band then they will mask the respective C and/or L band profile alarms. For example, if APR alarm is only raised on C-band AMP, it masks the downstream profile “Target Unachievable” alarm on both C-band and L-band profile if their diagnostic are raised to be True.

This alarm could also be raised momentarily after a fault condition recovery, power cycle recovery, connection addition, or mesh restoration.

CAUTION
Risk of equipment damage
Electrostatic discharge (ESD) can damage electrostatic sensitive devices. You must use antistatic protection while unpacking and installing all Field-Replaceable Units (FRU) and cables.

Spectrum Power using Node Essentials:

When the alarm is raised against power profiles, the channel power data is displayed by selecting **Facilities** from the Node Essentials navigation menu. The Power Profiles grid displays the total power and spectrum tilt data.

This alarm is raised if the system deviates from its last calibrated state beyond a certain threshold. The alarm is evaluated in every 10 seconds.

Alarm raised against pwrmon for the OSC Add power:
If the alarm is raised against pwrmon for the OSC launch power on the line, verify the target-power and power values and check that the alarm is valid.

CLI Example:

```
ITE-0156# show slots 5 inventory pwrmon “OSC Add”
slots:
- name: 5
inventory:
pwrmon:
- name: OSC Add
power : -4.5
target-power : -4.5
target-pwr-unachievable-threshold : 3.0
diagnostic:
target-unachievable : false
```

To validate that the target-power is within the OSC add power range:

```
SITE-0156# show slots 5 config slots 50 config plug-
defaults
slots:
- name: 5
config:
slots:
```


Copyright© 2019-2025 Ciena® Corporation

```
- name: 50
config:plug-defaults:
frequency : 191194
optical-power:
low-tx-power : 5.20
max-tx-power : 7.00
low-rx-power : -38.00
max-rx-power : -7.00m
low-tx-mon-power : 5.20
max-tx-mon-power : 7.00
low-rx-mon-power : -44.00
max-rx-mon-power : -24.00
```

Alarm raised against RAMAN

For the RAMAN Line-In, this alarm is raised when the abs (measured Raman gain - target Raman gain) > target-unachievable-threshold defined in the Raman facility.

Target and measured RAMAN gain using Node Essentials:

From the Facilities grid, select the module with the alarmed RAMAN facility.

When the alarm is raised against RAMAN, the target and measured gain can be displayed as follows:

- Select RAMAN facility from Facility navigator.

- Select the alarmed RAMAN facility by Row selector from the RAMAN Facilities grid.

The target RAMAN and measured RAMAN gains are displayed in the RAMAN facilities grid.

Impact

Minor, non-service-affecting (m, NSA)

Steps

1 Retrieve all the active alarms and alarm details:

If you want to perform the procedure using	**Then** go to the
CLI commands	"CLI INTERFACE STEPS"
Node Essentials	See the Node Essential steps in "Retrieving the data for the active alarm object" on page 32 in this document. Then go to step 3.

Copyright© 2019-2025 Ciena® Corporation

CLI INTERFACE STEPS

2 The following step is performed using CLI commands.

```
show active-alarm <id> [name] [resource] [raise-time]
[raise-time] [cause] [condition-type] [direction]
[location] [severity] [service-impact] [additional-info]
[user-notes...]
```

The current alarms and alarm details will appear.

3

If the alarm is raised against	**Then** go to
channel controller	step 4
pwrmon for the OSC launch power	step 13
RAMAN Line-IN	step 14
target line-out profile or baseline line-in profile	step 10

Alarm raised against channel controller

4 If there are multiple “Target Unachievable” alarm being raised at different ROADM site along the channel path, start the debugging process from the first ROADM site that raises this alarm. As of 2.6 alarm correlation is available and may negate the redundant alarms found downstream from the source of the issue. Alarm correlation must have the license and feature activated.

5 On the most upstream node raising this alarm, verify whether the delta between measured and expected input power is similar or the same as the delta between measured and expected output power on the channel-controller. To do this use the following command, where the center frequency of the alarming channel is specified:

```
show ccs-instance <PFG> channel-controller <center-freq>
channel-power
```

If the issue originates at	**Then** go to the
the first ROADM site where the channel is locally added	step 6
a passthrough ROADM site where the channel is expressing through	step 7

6 Verify the channel power data in the local OMS as follows:

a. Confirm what the delta between measured and expected channel power is for the alarming channel. Enter the following command:

```
show ccs-instance <PFG> channel-controller <center-
freq> channel-power
```

If L-band:

`show ccs-instance <PFG>-L channel-controller <center-freq>` channel-power

If there is a significant delta between measured and expected input power, the issue is likely located somewhere between the local add transponder and the RLA input switchport.

Example :

Copyright© 2019-2025 Ciena® Corporation

```
EAST# show ccs-instance PFG-1-SECTION-MUX channel-
controller 193250.000 channel-power
  ccs-instance:
  - name   : PFG-1-SECTION-MUX
    channel-controller:
    - center-frequency   : 193250.000
      channel-power:
        input:
          port-instance    : ciena-6500r-slots:slots 1
config port 28-7
          measured-power   : -2.53
          expected-power   : 1.08
        output:
          port-instance    : ciena-6500r-slots:slots 1
config port 100
          measured-power   : 2.03
          expected-power   : 4.66
```

b. Verify the physical fiber connections from the local add transponder to the CCMD channel-in port are is correct and that the fiber is undamaged.

c. Verify the Tx center frequency and power is properly tuned on the transponder, and that it matches exactly the center frequency of the NMC provisioned on the CCMD Tx/Rx port. Use the following command to confirm what the expected channel configuration is:

```
show slots <CCMD> config tx-proxy <input-port>
```

If the configured transponder Tx power does not match the total-target-tx-power, update the transponder Tx power to match. If unsure of how to do so, contact Ciena Support.

d. Verify the provisioning of the MC edges are aligned with the 6.25 GHz grid, as per the guidelines specified in “Retrieving, provisioning and deleting 1xNMC/MC channels using nmc-path and mc-path objects” procedure or “Retrieving, provisioning and deleting Multi-NMC/MC channel using nmcpath and mc-path objects” procedure in *Optical Control, SPLI, and OTDR*, 323-2051-318. If not, the MC must be deleted and re-added following the correct guidelines.

e. Verify that the Mux AMP in the CCMD8x24 or CCMD16 where the channel is added is in “Normal” state (not in “shutoff”, “clamped” and “apr” states). Follow the corresponding procedure to clear the alarm. See “Amplifier in Clamped State” on page 50, “Shutoff Threshold Crossed” or “Automatic Power Reduction Active” on page 56 in this document.

f. Verify there is no “hfl” (High Fiber Loss) alarm raised on the link from CCMD common out port to the RLA switch-in port where the channel ingresses. Refer to “High Fiber Loss” on page 119 to clear the alarm.

Copyright© 2019-2025 Ciena® Corporation

g. Run the following command to validate the expected and measured channel power at each point the channel traverses through the shelf.

```
get-port-trail-power port "slots # config port #"
center-frequency <center-freq>
```

Within each section of the port-trail, examine the difference between the exp-chl-power and channel-power values. If any major delta is seen, investigate that section of the node.

In the example below, we are checking an Add/Drop channel originating from a CCMD (slot 6 port 2). The command specifies the ingress (rx) port of the circuit pack.

```
EAST# get-port-trail-power port "slots 6 config port 2"
 status    : ok
 power-trail:
   center-frequency    : 192200.000
   port-powers:
     port              : ciena-6500r-nodes:nodes EAST data slots 6 config port 2
     channel-power     : -4.90
     exp-chl-power     : -5.00
     total-power       : -4.90
     port              : ciena-6500r-nodes:nodes EAST data slots 6 config port 101-6
     channel-power     : 1.57
     exp-chl-power     : 2.00
     total-power       : -2.29
     port              : ciena-6500r-nodes:nodes EAST data slots 1 config port 28-7
     channel-power     : -3.00
     exp-chl-power     : 2.00
     total-power       : -2.29
     port              : ciena-6500r-nodes:nodes EAST data slots 1 config port 53
     channel-power     : -3.00
     exp-chl-power     : 2.00
     total-power       : 23.40
```

From the example, we can quickly work from top to bottom of the output, comparing the exp-chl-power with the channel-power at each point.

Copyright© 2019-2025 Ciena® Corporation

Looking at slot 1 port 28-7, there is a significant drop in channel power, which then cascades down to the output seen on slot 1 port 53 (Line tx).

```
port            : ciena-6500r-nodes:nodes EAST data slots 1 config port 28-7
   channel-power   : -3.00
   exp-chl-power   : 2.00
   total-power     : -2.29
   port            : ciena-6500r-nodes:nodes EAST data slots 1 config port 53
   channel-power   : -3.00
   exp-chl-power   : 2.00
   total-power     : 23.40
```

This can be an indication that there is some loss present between the CCMD and the RLA circuit pack. The HFL alarm or CV related alarms can be raised in this particular scenario.

Based on which physical segment the excess loss has been identified, follow "High Fiber Loss" on page 119 to resolve that loss. If there are no discrepancies noticed, proceed to h.

h. For ROADM add/drop sites the Section MUX ccs-instance channel controller should have the control-mode set to power. Enter the following command to confirm what the current control-mode is.

```
show ccs-instance <PFG> channel-controller <center-freq> control-mode
```

If the control-mode is not set to power, it should be changed later during a service affecting window. This is not necessarily the cause; however, it will aid in future investigations if set to the recommended control-mode.

7 Verify there is no "hfl" (High Fiber Loss) or "Fiber Break Detected" alarm anywhere at the passthrough site for links between passthrough degrees. Refer to "High Fiber Loss" on page 119 procedure to clear the alarm. Use the following command to check the link loss between RLA and RLA or LRU to LRU for express channel.

```
show link <AMP-to-AMP link name>
```

Example:

```
RLS# show link RLA-1-RLA-3 | grep loss
    insertion-loss                      : 0.6
    excess-loss                         : 0.0
    high-fiber-loss-minor-threshold     : 1.5
    high-fiber-loss-major-threshold     : 10.0
    measured-physical-loss-baseline     : 0.0
    baseline-loss-threshold             : 3.0
    expected-physical-loss              : 0.6
    actual-measured-loss                : 0.0
    measured-physical-loss              : 0.0
      high-fiber-loss                    : false
      high-fiber-loss-major-severity     : false
```


Copyright© 2019-2025 Ciena® Corporation

a. Verify that the upstream AMP where the channel ingresses, is in “Normal” state (not in “shutoff”, “clamped” and “apr” states). Follow the corresponding procedure (“Automatic Shutoff” on page 60, “Amplifier in Clamped State” on page 50 or “Automatic Power Reduction Active” on page 56” to clear the alarm. Go to step 37.

b. Use the get-port-trail-power rpc to verify the channel power as it traverses the passthrough node. Specify the slot and port of the line interface where the channel is ingressing on the passthrough node. If there are any major drops in channel/total power, investigate those further.

```
get-port-trail-power port "slots # config port #"
center-frequency <center-freq>
```

8 If the measured input power is matching the expected input power, but the alarm is still being raised, verify the Booster amplifier in the RLA is in “Normal” state (not “shutoff”, “clamped” or “apr)”.

9 Verify the provisioning of the MC edges are aligned with the 6.25 GHz grid, as per the guidelines specified in “Retrieving, provisioning and deleting 1xNMC/MC channels using nmc-path and mc-path objects” procedure or “Retrieving, provisioning and deleting Multi-NMC/MC channel using nmc-path and mc-path objects” procedure in *6500 RLS Optical Control, SPLI, and OTDR*, 323-2051-318. If not, the MC must be deleted and re-added following the correct guidelines.

Alarm raised against spectrum power profiles

10 Determine what the difference is between the currently measured spectral tilt or total power or mean-psd and the target tilt and/or total power or mean-psd. The example in Figure 14 depicts an alarm raised against the pwr-profile for slot 4 port 5, specifically for L-BAND.

Figure 14 Example

```
active-alarm:
  - id                : 1688
    name              : target-unachievable
    resource          : ciena-6500r-slots:slots 4 config pwr-profile 5,BAND-L
    raise-time        : 2021-07-14T18:30:57Z
    alarm-state       : enabled
    cause             : Target Unachievable
    condition-type    : OTS-SD
    direction         : tx
    location          : near-end
    severity          : minor
    service-impact    : nsa
```

11 Compare the configured pwr-profile “total-power”, “mean-psd”, and “tilt” values with the currently measured values. To do this, use the following commands where “config” is for the configured or “target” pwr-profile and slot inventory is the live reading.

```
show slots <#> config pwr-profile "<port>,BAND-<C|L>
```


Copyright© 2019-2025 Ciena® Corporation

```
show slots <#> inventory pwr-profile "<port>,BAND-<C|L>"
```

Example of “pwr-profile” configuration:

```
RLS# show slots 1 config pwr-profile 53,BAND-C target |
grep t
  slots:
      - parent-port   : 53
        target:
       timestamp              : 2025-04-14T16:26:00.242Z
        total-power         : 15.54
        tilt                : 1.0
        total-pwr-delta-threshold           : 10.0
        tilt-alarm-threshold                : 2.5
        mean-psd-delta-threshold             : 2.0
        spectral-degrade-alarm-hold-off     : 60
        single-spectral-deficit-pwr-delta-th: 10.0
        single-spectral-deficit-bw-th       : 25.000
         aggregate-spectral-deficit-bw-th      : 1206.250
```

Example of “pwr-profile” inventory:

```
STR14-22000-02OLR# show slots 1 inventory pwr-profile
53,BAND-C
  slots:  - name   : 1
    inventory:
      pwr-profile:
      - parent-port   : 53
      - name          : BAND-C
        measured:
          total-power                      : 15.50
          tilt                             : 1.1
          mean-psd                         : -10.36
          aggregate-spectral-deficit-value : 0.000
          max-aggregate-spectral-deficit-value: 2037.500
          max-aggregate-spectral-deficit-timestamp:2025-
04-14T18:26:40Z
          diagnostic:
            total-power-unachievable    : false
            tilt-unachievable           : false
            mean-psd-unachievable       : false
            spectral-loading-degraded   : false
```

Note: There is internal hysteresis for clearing the power profile TU alarm on “total power”, mean-psd and “tilt” as follows:

Default total-pwr-delta-threshold = 10dB (provisionable), with alarm clear hysteresis of 3dB.
Default tilt-alarm-threshold = 2.5dB (provisionable), with alarm clear hysteresis of 0.5dB.
Default mean-psd-delta-threshold = 2dB (provisionable), with alarm clear hysteresis of 0.5dB

Copyright© 2019-2025 Ciena® Corporation

12 If diagnostic flag for “total-power-unachievable” or “tilt-unachievable” or “mean-psd-unachieveable” is set to true, then verify whether there are any internal site losses and/or line fiber losses both upstream and downstream. This can be done using OTDR traces <insert OTDR trace reference>. If there are losses or reflectance present resolve them as necessary <insert HFL Procedure> and verify whether the alarm has cleared. If there are no losses or reflective events found, then this alarm may be cleared by section calibration during a service-affecting maintenance window.

Alarm raised against pwrmon for the OSC launch power on the line

13 If the target-power is greater than the max-to-power then reduce the target-power to the achieved power.

If the alarm clears then this procedure is complete. Otherwise go to step 37.

Alarm raised against RAMAN

14 Verify that the RAMAN facility provisioning matches what is defined in the EDP and fix the provisioning error(s). Refer to the *Equipment/Facility Provisioning and Protection*, 323-2051-310.

15 Verify the Raman facility inventory information:

a. Verify that the target gain is within the range provided by the Raman facility. If the gain range (min-allowed-raman-gain and max-allowed-raman-gain) is showing both 0 values, then there was a issue with calibration and the calibration may need to be performed again.

b. If the gain range (min-allowed-raman-gain and max-allowed-raman-gain) is showing default values (0 and 30), then there was a issue with calibration and the calibration may need to be performed again.

c. Verify that the following parameters are showing in the proper state in the inventory facility:

— gain-mode: provisioned

— forced-shutoff: Disabled

— operating-state: normal

16 If there are any major OTDR events (losses/reflective events) organize a maintenance window during which the Raman admin-state should be set to Disabled.

CAUTION
Risk of traffic loss
The following steps will impact traffic. If possible, re-route the traffic to minimize the traffic loss.

If you want to perform the procedure using	**Then** go to the
CLI commands	“CLI INTERFACE STEPS”
Node Essentials	“NODE ESSENTIALS STEPS”

Copyright© 2019-2025 Ciena® Corporation

CLI INTERFACE STEPS

17 To place the alarmed AMP facility to “Disabled”. Enter the following command:

```
set slots <slot #> config ramans LINE-IN admin-state
Disabled
```

18 Go to step 26.

NODE ESSENTIALS STEPS

19 Select **Facilities** from the Node Essentials navigation menu.

The Facilities menu opens.

20 From the **Equipment** grid, select the module with the alarmed RAMAN facility.

The bottom part of screen becomes populated.

21 Select RAMAN facility from Facility navigator.

The RAMAN Facilities grid opens.

22 Select the alarmed RAMAN facility by Row selector from the RAMAN Facilities grid.

23 Click the **Pencil** icon.

The related Edit dialog opens.

24 Edit the RAMAN facility as required.

Admin state: Disabled

25 Click **Confirm**.

26 Verify the RLA/DLE/DLA input port (port 54 or port 64) Office and Short traces manually for any of the following events:

a. Large losses/reflections that were not captured by the OTDR alarms, possibly because of the pulse width/event spacing. If the events are overlapping, re-run the trace using a smaller pulse by following the appropriate procedures in *Optical Control, SPLI, and OTDR*, 323-2051-318.

b. Check for disparate or mixed fiber types, indicated by “gainers” or exaggerated loss splices.

27 Perform fiber/port/patch-panel cleaning procedure(s) on the event in question.

If the alarm does not clear, continue to next step. Otherwise, this procedure is complete.

28 When cleaning the connection, a new go-nogo OTDR trace is triggered. Wait for the “local-otdr-in-progress” alarm to clear before reconnecting the fiber(s). This initiates another go-nogo OTDR trace automatically.

29 Set the Raman facility back to Enabled. If the “Target Unachievable” alarm has cleared, then the procedure is complete. Otherwise, continue to the next step.

Copyright© 2019-2025 Ciena® Corporation

30 If the major losses/reflections have been resolved and the “arget-unachievable” alarm is still present, increase the “target-unachievable-threshold” by the smallest value possible to clear the alarm.

If you want to perform the procedure using	**Then** go to the
CLI commands	“CLI INTERFACE STEPS”
Node Essentials	“NODE ESSENTIALS STEPS”

CLI INTERFACE STEPS

31 To increase the “target-unachievable-threshold, enter the following command:

```
set slots <SRA slot#> config ramans LINE-IN target-
unachievable-threshold <value>>
```

32 Go to step 36.

NODE ESSENTIALS STEPS

33 In the Facility grid, click the **Pencil** icon.

The related Edit dialog opens.

34 Edit the threshold as required.

35 Click **Confirm**.

36 If the alarm is cleared, re-run PlannerPlus and the procedure is complete. If needed, contact your next level of support or your Ciena support group to access PlannerPlus. Otherwise go to step 37.

37 If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 132 Telemetry - External Alarm

Requirements

To perform this procedure, you must use an account with at least an Admin user access level.

Probable cause

RLS provides general purpose telemetry inputs that can be used to monitor external equipment. This alarm is raised on the Access Panel when an external alarm point is triggered. Refer to "Telemetry - External Alarm" on page 278 in this document for more information.

Impact

Minor, non-service affecting (m, NSA)

Steps

1. To clear the alarm, verify the external equipment for the cause of the alarm and take action accordingly to remove the fault.
2. If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 133 Upgrade Failed

Probable cause

This alarm is raised when failure occurs during a manual or automatic upgrade of circuit packs.

Note: If an Interface module fails during the upgrade, the upgrade will not be interrupted. However, a CTM failure, will stop the upgrade operation.

Impact

Major, non-service-affecting (M, NSA)

Steps

1 Retrieve all the active alarms and alarm details.

If you want to perform the procedure using	**Then** go to the
CLI commands	step 2
Node Essentials	See the Node Essential steps in "Retrieving the data for the active alarm object" on page 32. Then go to step 3.

2 To retrieve all the active alarms and alarm details, enter:

```
show active-alarm <id> [name] [resource] [raise-time]
[raise-time] [cause] [condition-type] [direction]
[location] [severity] [service-impact] [additional-info]
[user-notes...]
```

The current alarms and alarm details will appear.

3 If any of the "Circuit Pack Fail", "Hardware Subsystem Fail", or "Software Subsystem Fail" alarms are active against either CTMs, the upgrade cannot proceed. Follow the corresponding alarm clearing procedures for these alarms before continuing.

4 Confirm whether any of the CTMs have an upgrade-failed state using the following command. Until the upgrade-fail is resolved on the CTM/s the upgrade cannot proceed.

```
show software component <41|42>
```

5 Verify the current state of the upgrade using the following command.

```
show software
```

From the output of the above command, note the following information.

a. upgrade-operational-state

b. operation-info last-operation

c. id (slot number)

6 Collect the logs from the shelf using the following command.

Copyright© 2019-2025 Ciena® Corporation

```
retrieve-logs slot ALL mode full
```

7 Confirm whether the upgrade was a single or multi-step upgrade.

8 If performing an upgrade against a shelf, based on the last-operation data collected in step 5, re-initiate that last-operation. There is an option to re-initiate the entire upgrade process using “software-install” command, but this will retry the entire process from the beginning.

9

If	Then
Load-Failed	re-initiate a software-load. Go to step 10.
Activate-Failed	re-initiate a software-activate using the “software-activate” command.Go to step 11
Commit-Failed	re-initiate a software-commit using the “software-commit” command. Go to step 11

10 Check the last-operation result details to confirm if the delivery failed. If so, verify the IP reachability to release server (ping, SSH, SFTP). If the IP reachability is confirmed, re-initiate the software-deliver and proceed with the remaining steps of the upgrade.

11 If performing a One-Step Upgrade, any of the above three recovery methods will continue the remaining One-Step upgrade stages. For example, if a software-load is run after One-Step Upgrade Failure at the software-load stage, the Activate and Commit phases of the upgrade will follow automatically.

12 If performing a Multi-Step Upgrade, complete the remaining steps of the documented upgrade procedure.

Figure 15 Example of recovery commands

```
software-deliver uri "scp://user:pass@1.2.3.4/RLS/RLS-02.05.00.0907.tgz"

software-load version RLS-02.05.00.0907
OR
software-load uri "scp://user:pass@1.2.3.4/RLS/RLS-02.05.00.0907.tgz"

software-activate [enter]

software-commit [enter]
```

13 If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 134 Upgrade In Progress

Probable cause

This alarm is raised when a software install or multi-step upgrade is in progress.

> ***Note:*** This alarm is not raised for the software delivery stage during multi-step upgrade.

Impact

Warning, non-service-affecting (W, NSA)

Steps

1. No action is required. The alarm clears when the upgrade completes.
2. If the alarm does not clear, contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 135 User Intrusion Attempt

Requirements

Log into the CLI of the nodes with admin or higher privilege level. For login information, see “Accessing and logging in to a network element” procedure in *Licensing, Security, and Administration*, 323-2051-300.

Probable cause

This alarm is raised when the CTM detects an intruder attempting to gain shelf access, and the maximum number of login attempts exceeds the provisioned number allowed.

The alarm is raised when an intrusion is detected and the user account locks. The alarm clears automatically after the lockout period expires. However, a “Super” user can clear the alarm manually before the lockout is cleared. If new intrusion attempts occur before this alarm is cleared, they will be logged in the Security Log and the duration of the lockout will be extended for the lockout period of the latest intrusion attempt.

Impact

Major, non-service-affecting (M, NSA)

Steps

1. Allow the alarm to clear itself when the lockout time expires or go to step 2.
2. Select the alarmed network element and clear the security alarm. Refer to appropriate alarm clearing procedures in this document.
3. Follow your company policy for handling intrusion attempts.
4. If the alarm does not clear, contact your next level of support or Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 136 Wait To Restore

Requirements

To perform this procedure, you must use an account with at least an Admin user access level.

Probable cause

This alarm is raised when the traffic has switched away from the working path in revertive mode.

Impact

Warning, non-service-affecting (m, NSA)

Steps

1. No action is required. The alarm clears once the wait to restore period has completed.
2. If the alarm is still active once the wait to restore time has completed, then contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

Procedure 137 Wait To Restore - Remote

Requirements

To perform this procedure, you must use an account with at least an Admin user access level.

Probable cause

This alarm is raised when the traffic has switched away from the remote working path in revertive mode.

Impact

Warning, non-service-affecting (m, NSA)

Steps

1. No action is required. The alarm clears once the wait to restore period has completed.
2. If the alarm is still active once the wait to restore time has completed, then contact your next level of support or your Ciena support group.

Copyright© 2019-2025 Ciena® Corporation

CHAPTER 3
Module replacement

Overview

This section contains the procedures to replace modules equipped in the 6500 Reconfigurable Line System (RLS) shelf assembly. Read and understand product and personnel safety guidelines described in *6500 RLS Shelf Installation Guide,* 323-2051-201 before replacing equipment.

The following table provides a list of module replacement procedures in this section.

List of procedures

- Procedure 138, “Reseating a module”
- Procedure 139, “Replacing an R2, R4, R6-300, or R8-300 shelf”
- Procedure 140, “Replacing a Control and Timing Module (CTM)”
- Procedure 141, “Replacing a CTM front panel on an R2 shelf”
- Procedure 142, “Reconfiguring a CTM with 8GB DDR memory (RAM) to a CTM with 16GB DDR memory”
- Procedure 143, “Replacing an Access Panel in an R2 shelf”
- Procedure 144, “Replacing an Access Panel in an R4 shelf”
- Procedure 145, “Replacing an Access Panel in an R6-300 shelf”
- Procedure 146, “Replacing an Access Panel in an R8-300 shelf”
- Procedure 147, “Replacing a pluggable module”
- Procedure 148, “Replacing a shelf fan module”
- Procedure 149, “Replacing a shelf air filter in R2 or R4 shelf”
- Procedure 150, “Replacing a shelf air filter in an R6-300 or R8-300 shelf”
- Procedure 151, “Replacing a DC Power Input Module”
- Procedure 152, “Replacing an AC Power Input Module”
- Procedure 153, “Replacing a DLM, TLM C-Band module”
- Procedure 154, “Replacing a CMD, CCMD, or SSM module”

Copyright© 2019-2025 Ciena® Corporation

- Procedure 155, “Replacing a CFIM, UCS, or MonCS in an OMC2 chassis”
- Procedure 156, “Replacing the WSS 32x1 C-Band Module”
- Procedure 157, “Replacing a Fiber Interconnect Module Type 4 (FIM4)/ FIM4A”
- Procedure 158, “Replacing an RLA module”
- Procedure 159, “Replacing LRU module”
- Procedure 160, “Replacing an SRA module”
- Procedure 161, “Replacing a DLE or DLA module”
- Procedure 162, “Replacing an OMC2 Chassis”
- Procedure 163, “Replacing a Trunk Protection Switch module”

Copyright© 2019-2025 Ciena® Corporation

Procedure 138 Reseating a module

Use this procedure to reseat a module.

Requirements

To perform this procedure, you must:

- observe all safety requirements described in *6500 RLS Shelf Installation Guide,* 323-2051-201
- ensure that you have all the documentation referenced in this procedure
- ensure that all alarms are enabled, see the alarm provisioning and alarm profiles procedures in this section
- use an account with admin privileges or higher

CAUTION
Risk of traffic loss
You will lose all traffic while reseating an unprotected module. If possible, ensure that the module you are reseating is protected.

CAUTION
Risk of equipment damage
Electrostatic discharge (ESD) can damage electrostatic sensitive devices. You must use antistatic protection while unpacking and installing all Field-Replaceable Units (FRU) and cables.

Overview

For information about reseating the Access Panel, refer to "Replacing an Access Panel in an R2 shelf" on page 314.

Steps

1 Retrieve all the active alarms and alarm details:

If you want to perform the procedure using	**Then** go to the
CLI commands	"CLI INTERFACE STEPS"
Node Essentials	See the Node Essential steps in "Retrieving the data for the active alarm object" on page 32 in this document. Then go to step 3.

Copyright© 2019-2025 Ciena® Corporation

CLI INTERFACE STEPS

2 The following step is performed using CLI commands.

```
show active-alarm <id> [name] [resource] [raise-time]
[raise-time] [cause] [condition-type] [direction]
[location] [severity] [service-impact] [additional-info]
[user-notes...]
```

The current alarms and alarm details will appear.

3 Record the current state of the system.

4 Wear an antistatic wrist strap or foot straps to protect the shelf from static damage. If using a wrist strap, connect the wrist strap to the ESD jack on the shelf.

5 If applicable, verify the protection scheme of each port/path on the module and record the port information for later use.

6 Select your next step.

If the port of the module you are reseating is part of	**Then** go to
a protected configuration	step 7
an unprotected configuration	step 8
the CTM	step 10
a filler module	step 12

If some ports are protected and some unprotected, switch traffic from protected ports then continue with step 8.

7 Perform a manual switch on the port to verify the inactive path. Refer to *Equipment/Facility Provisioning and Protection*, 323-2051-310.

If traffic switches back autonomously to the active path or if the manual switch is denied, contact your next level of support or your Ciena support group.

8 Change the admin states of all facilities on the module to “Disabled”. Refer to *Equipment/Facility Provisioning and Protection*, 323-2051-310.

9 Change the equipment admin state of the module to “Disabled”. Refer to “Provisioning a circuit pack or pluggable” procedure in *Equipment/Facility Provisioning and Protection*, 323-2051-310.

Go to step 11.

10 Change the equipment admin state of the module to “Disabled”. Refer to “Provisioning a circuit pack or pluggable” procedure in *Equipment/Facility Provisioning and Protection*, 323-2051-310.

The blue LED turns off when the module is set to “Disabled”. This can indicate which module to replace.

Note: In a duplex operation, only the idel (not active) CTM can be replaced. Otherwise, a CTM switch action is needed.

11 Ensure that the blue LED on the module faceplate is off before you remove the module from the backplane.

If the blue LED is on, do not pull out the module.

Copyright© 2019-2025 Ciena® Corporation

12 Push outwards on both pull tabs simultaneously to disengage the module from the backplane.

> **CAUTION**
> **Hot Surface**
> The module may be hot—do not touch hot surfaces.

13 Remove the module from the slot by pulling on the pull tabs.

Alarms are raised, but cleared when the module is inserted back into the slot at the completion of this procedure.

Note: If you are upgrading from RLS R1.0, and reseating a CTM filler module before the upgrade, the CTM filler modules must be unseated before performing the software upgrade and stay unseated until the upgrade is completed.

For an interface module, allow at least 30 seconds to power down.

> **CAUTION**
> **Risk of equipment damage**
> You must re-equip the slot within three minutes as empty slots are not allowed.

14 Insert the module into the slot by lifting the edges of the faceplate and carefully guiding it into the slot guide grooves.

15 Push the module towards the back of the shelf until it engages with the backplane and then push on the faceplate to fully seat it.

You will see the latches click into place into the shelf as you push the faceplate towards the backplane.

Do not force the locking levers. If the levers do not close properly, remove the module and examine the connectors on the back of the module. Look for bent pins or damage to the module or shelf keys. Contact Ciena support group if the connectors are damaged.

16 Select your next step.

If you are reseating	**Then**
an interface module or a CTM	go to step 17
a filler module	this procedure is complete

17 Consider the following:

- During a module reseat, the port and Ethernet port status LEDs remain off.
- Once the green LED is steadily lit (after the software initialization), an auto-upgrade of the module may occur. During an auto-upgrade, the green LED remains steadily lit and the blue LED remains off (a Software Auto-Upgrade in progress alarm is raised and clears once the auto-upgrade is complete).

Copyright© 2019-2025 Ciena® Corporation

> **ATTENTION**
> Do not cold restart or reprovision wavelengths in the first 5 minutes after an upgrade is completed.

Wait until this sequence is complete before proceeding to the next step.

18 Ensure that the received input power of the optical interface does not exceed the overload value and the new module is recognized by the CTM. Refer to "Module descriptions, equipping rules, specifications" in *6500 RLS Planning Guide*, NTRN10WA

19 If you have reseated the CTM, verify that the date and time is correct. If necessary, reset the date and time.

If the Time Of Day (TOD) synchronization feature is enabled, you do not have to reprovision the date and time.

20 Change the equipment admin state of the module to "Enabled".

When the module is "Enabled", the blue LED turns on.

21 Change the admin states of all facilities on the module to "Enabled".

22 If applicable, return traffic to the module by releasing the protection switch. Refer to *Equipment/Facility Provisioning and Protection*, 323-2051-310.

23 Clear all alarms raised against the module. Refer to the "Alarms" section in this document.

Copyright© 2019-2025 Ciena® Corporation

Procedure 139 Replacing an R2, R4, R6-300, or R8-300 shelf

Use this procedure to replace an R2, R4, R6-300 or R8-300 shelf.

Requirements

To perform this procedure, you must:

- observe all safety requirements described in *6500 RLS Shelf Installation Guide*, 323-2051-201
- have the correct replacement shelf (the replacement Product Engineering Code [PEC] is the same as the current PEC)
- have protective caps for the patchcords

CAUTION
Risk of equipment damage
Electrostatic discharge (ESD) can damage electrostatic sensitive devices. You must use antistatic protection while unpacking and installing all Field-Replaceable Units (FRU) and cables.

Overview

Use this procedure to replace an R2 (NTK803DA), R4 (NTK803FA), R6-300, (NTK803PA) or R8-300 shelf (NTK803QA) in the equipment rack or cabinet. See Figure 16, Figure 17, Figure 18 and Figure 19 for an example of the shelves.

CAUTION
Service affecting procedure
Shelf replacement is service affecting. Ensure you have exhausted all other troubleshooting options before performing this procedure and if possible, re-route the traffic to minimize the traffic loss.

Steps

1. Perform a database-backup of the node and store the backup file found in "/var/opt/ap/pub/backups" in a remote location off the shelf (laptop used for the database-restore/database-commit). Refer to the Backup and restore section in *Licensing, Security, and Administration*, 323-2051-300.
2. Disable the Access Panel as described in Procedure 143, "Replacing an Access Panel in an R2 shelf", Procedure 144, "Replacing an Access Panel in an R4 shelf", Procedure 145, "Replacing an Access Panel in an R6-300 shelf", or Procedure 146, "Replacing an Access Panel in an R8-300 shelf".

Copyright© 2019-2025 Ciena® Corporation

3 Wear an appropriate ESD personal grounding device to dissipate electrostatic charges. If you are wearing an antistatic wrist strap, connect the cord to the ESD jack on the shelf installed and grounded in a grounded rack or clip to a suitable ground point.

4 Power down system by disconnecting power cable to AC power module or turning off power to DC power module from BIP or power distribution panel.

5 Disconnect power cables, optical fiber cables to the IM cards and any comms cables to the Access Panel.

6 If attached, remove shelf front cover and any Fiber Interconnect Modules (FIM).

7 Unseat and remove IM cards and fillers from their slots and store them safely.

8 Select your next step:

If you are replacing an	**Then** go to
R2 shelf	step 9
R4 shelf	step 12
R6-300 shelf	step 16
R8-300 shelf	step 19

Replacing an R2 shelf

9 Remove the fan modules from its slot. On an R2 shelf, fan module can be removed without removing CTM but removing a CTM also removes its attached fan module.

a. using a Phillips screwdriver, unfasten the retention screw on the module

b. pull the fan module using the handle until the module is fully disengaged from the backplane

c. remove the fan module using the fan handle and place it in a safe location

10 If still seated, unseat and remove CTMs from their slots.

a. open the latches of the CTM by squeezing the locks and rotating the latches outward

b. use the latches to pull and remove the CTM from the backplane and store it safely

11 Unseat and remove AP module from its slot.

a. disconnect the control and communication connectors and any wire wrap adapters (if being used) from the access panel

b. push the spring latch upward until disengages and pull to remove the panel from the shelf and store it safely

Go to step 22.

Replacing an R4 shelf

12 Unseat CTMs and/or filler modules from their slots and store them safely.

a. open the latches of the CTM by squeezing the locks and rotating the latches outward

Copyright© 2019-2025 Ciena® Corporation

b. use the latches to pull and remove the CTM from the backplane and store it safely

13 Remove the module carriers from the shelf guides.

14 Remove fan modules from their slots.

a. use a Phillips screwdriver to loosen the retaining thumbscrew on the module

b. gripping the pull handle, carefully pull the fan module out of slot. Grip the fan using two hands, being careful not to allow hands or fingers near the fan blades. Remove the fan module from the shelf and store it safely.

15 Unseat and remove AP module from its slot.

a. disconnect the control and communication connectors and any wire wrap adapters (if being used) from the access panel

b. using a Phillips screwdriver, unscrew the thumbscrew on left side to shelf wall of the panel. Pull out the access panel by sliding it out and disengaging it from the backplane and store it safely.

Go to step 22.

Replacing an R6-300 shelf

16 Unseat CTMs and/or filler modules from their slots and store safely.

a. open the latches of the CTM by squeezing the locks and rotating the latches outward

b. use the latches to pull and remove the CTM from the backplane and store it safely

17 Remove fan modules from their slots in the side panel.

a. using a Phillips screwdriver, unfasten the retention screw that holds the fan module to the left wall

b. gripping the pull handle, carefully pull the fan module out of the slot. Grip the fan using two hands, being careful not to allow hands or fingers near the fan blades. Remove the fan module from the shelf and store it safely.

18 Unseat and remove AP module from its slot.

a. disconnect the control and communication connectors and any wire wrap adapters (if being used) from the access panel.

b. Pull on the pll tabs both sides of the access panel to pull out the access panel by sliding it out and disengaging it from the backplane and store it safely.

Replacing an R8-300 shelf

19 Unseat CTMs and/or filler modules from their slots and store safely.

a. open the latches of the CTM by squeezing the locks and rotating the latches outward

b. use the latches to pull and remove the CTM from the backplane and store it safely

20 Remove fan modules from their slots in the side panel.

Copyright© 2019-2025 Ciena® Corporation

a. using a Phillips screwdriver, unfasten the retention screw that holds the fan module to the left wall

b. gripping the pull handle, carefully pull the fan module out of the slot. Grip the fan using two hands, being careful not to allow hands or fingers near the fan blades. Remove the fan module from the shelf and store it safely.

21 Unseat and remove AP module from its slot.

a. disconnect the control and communication connectors and any wire wrap adapters (if being used) from the access panel.

b. using a Phillips screwdriver, unscrew the captive screws on each side of the faceplate

c. use your thumbs to swing the latches on both sides of the access panel into the open position. Pull out the access panel by sliding it out and disengaging it from the backplane and store it safely.

22 Unscrew power connection screws from PIMs and slide out of assigned slot. Remove power cables from PIM.

23 Disconnect shelf ground from bay ground.

24 Detach fiber managers from shelf.

25 Detach the mounting brackets and the rack adapters. Shelf chassis should now be free to move and store away.

26 Install new 6500 RLS shelf (R2, R4, R6-300, or R8-300) as per 6*500 RLS Shelf Installation Guide*, 323-2051-201.

27 With a laptop containing the database backup, connect the laptop to the craft port by following the “Connecting a terminal to the R2 shelf”, Connecting a terminal to the R4 shelf, “Connecting a terminal to the R6-300 shelf, or “Connecting a terminal to the R8-300 shelf” procedure as documented in the *6500 RLS Shelf Installation Guide*, 323-2051-201.

28 With the Access Panel installed on the new shelf, continue the steps described in Procedure 143, “Replacing an Access Panel in an R2 shelf”, Procedure 144, “Replacing an Access Panel in an R4 shelf”, Procedure 145, “Replacing an Access Panel in an R6-300 shelf” or Procedure 146, “Replacing an Access Panel in an R8-300 shelf” procedures.

Note: The software load to be restored on the Access Panel must match the software load of the backup file.

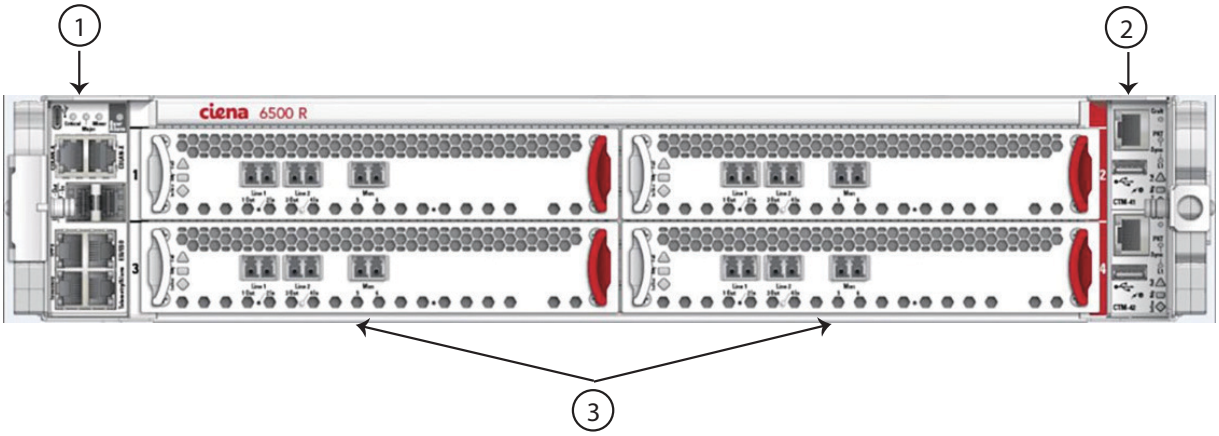
29 Set the shelf member name. Refer to “Set ciena-6500r-system:system id member” section of the *CLI Reference*, 323-2051-190. Perform a database-restore. Refer to the Backup and restore section of *Licensing, Security, and Administration*, 323-2051-300.

30 When you are replacing a shelf with Control Plane enabled, if you see the osrp-link in “Remote Node Unreachable” state, you must restart the CTMs at any neighbors connected by OSC. Refer to “Restarting an interface module or the CTM” on page 37 of this document.

31 Ensure there are no active alarms against the newly installed module(s).

Copyright© 2019-2025 Ciena® Corporation

Figure 16 Example of an R2 shelf (NTK803DA)—front view, equipped



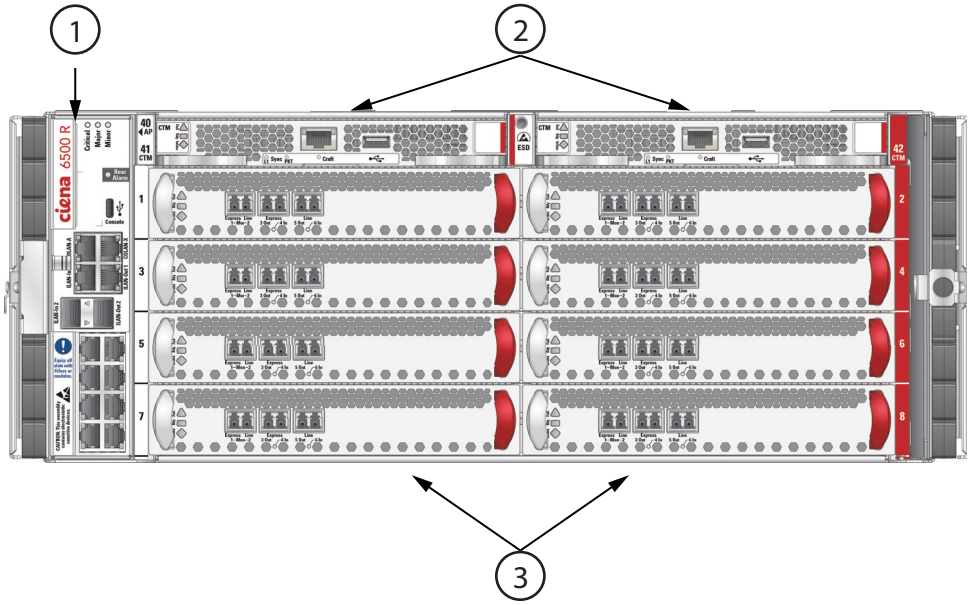
Legend

1 Access panel (slot 40)

2 Front panel for CTMs (slot 49)

3 Slots for Interface Modules (slots 1-4)

Figure 17 Example of an R4 shelf (NTK803FA)—front view, equipped



Legend

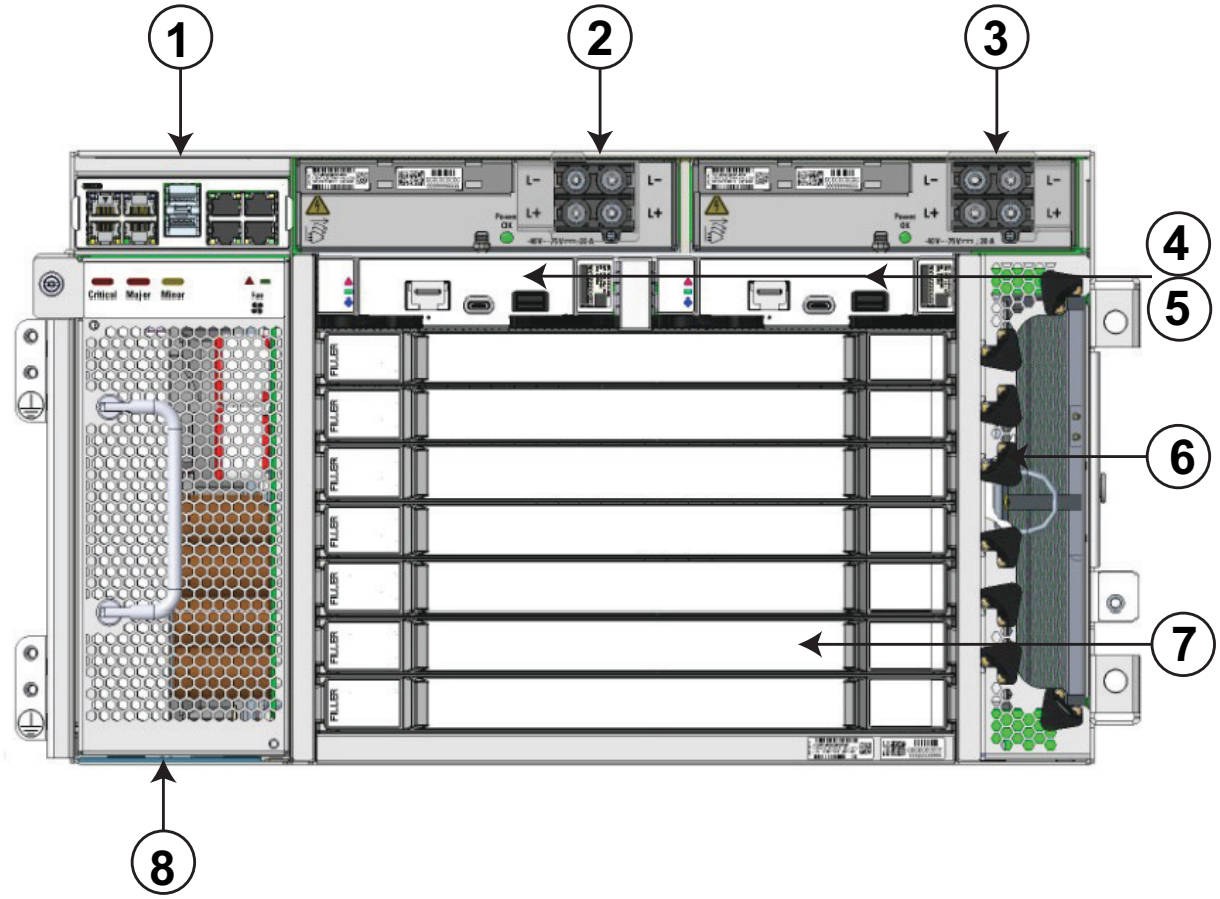
1 Access panel (slot 40)

2 Control and Timing Modules (slots 41 and 42)

3 Slots for Interface Modules

Copyright© 2019-2025 Ciena® Corporation

Figure 18 Example of an R6-300 shelf (NTK803PA)—front view, equipped

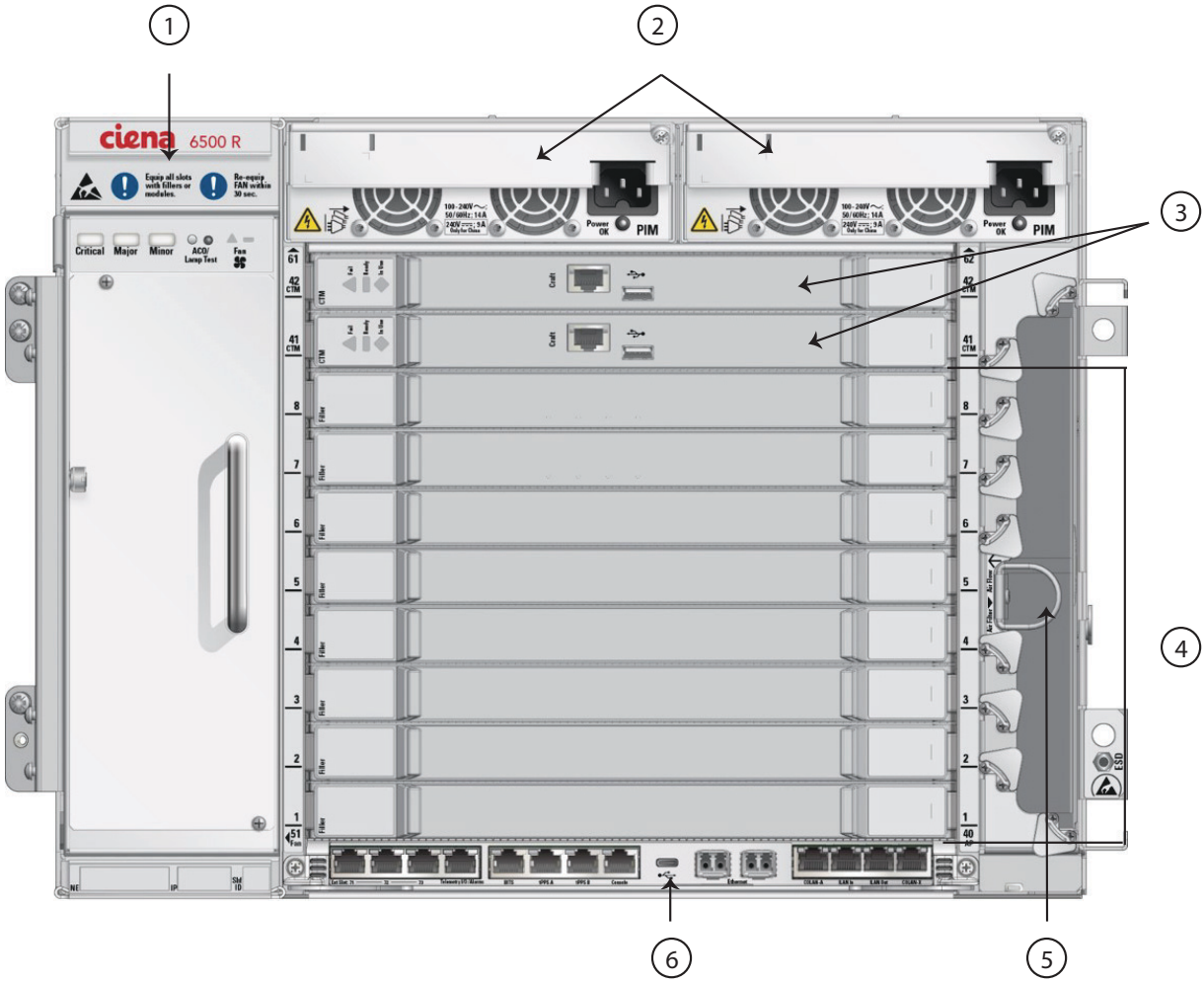


Legend

1	Access Panel (NTK805PA)	5	Air Filter Location (tab is part of air filter)(NTK807MP)
2	DC Power Input Modules Type 2 (NTK505UH)	6	Interface Modules
3	DC Power Input Modules Type2 (NTK505UH)	7	Cooling Fan module (NTK807PA
4	Control and Timing Modules (CTM) (NTK810PA)		

Copyright© 2019-2025 Ciena® Corporation

Figure 19 Example of an R8-300 shelf (NTK803QA) with AC PIMs—front view, equipped



Legend

1	Fan Module (NTK507QA)	4	Interface Module Slots (8)
2	AC Power Input Modules (NTK505RN)	5	Air Filter Location (tab is part of air filter)
3	Control and Timing Modules (CTM) (NTK810QA/QB)	6	Access Panel (NTK805QA)

Copyright© 2019-2025 Ciena® Corporation

Procedure 140 Replacing a Control and Timing Module (CTM)

Use this procedure to replace a Control and Timing Module (CTM) with the same model of CTM. Refer to the “Reconfiguring a Control and Timing Module (CTM) from 8G to 16G” procedure if you want to upgrade the CTMs from 8G to 16G.

Requirements

To perform this procedure, you must:

- have a replacement CTM module, review “Ordering Information” in *6500 RLS Planning Guide*, NTRN10WA to make sure you select the correct replacement part
- observe all safety requirements described in *6500 RLS Shelf Installation Guide,* 323-2051-201

CAUTION
Risk of equipment damage
Electrostatic discharge (ESD) can damage electrostatic sensitive devices. You must use antistatic protection while unpacking and installing all Field-Replaceable Units (FRU) and cables.

Overview

The following CTMs are supported:

- Control and Timing Module replacement for use in the R2 shelf.
  - NT810DA is replaced with NTK810DA
  - NT810DB is replaced with NTK810DB
- Control and Timing Module replacement for use in the R4 shelf.
  - NT810FA is replaced with NTK810FA
  - NT810FB is replaced with NTK810FB
- Control and Timing Module replacement for use in the R6-300 shelf.
  - NT810PA is replaced with NTK810PA
- Control and Timing Module replacement for use in the R8-300 shelf.
  - NT810QA is replaced with NTK810QA
  - NT810QB is replaced with NTK810QB

Copyright© 2019-2025 Ciena® Corporation

Note: When a CTM module is removed, it must be replaced with the identical model of CTM. Failure to do so will result in a “Circuit Pack Mismatch” and/or “Equipment Configuration Mismatch” alarm to be raised.

RLS supports both dual (also known as protected or duplex) and simplex (unprotected) operation for the Control and Timing Module (CTM). In a duplex operation, two (redundant) CTMs are installed in the shelf, in slot 41 and slot 42. One CTM is always active and controls the shelf while the other CTM is the standby CTM. By default, the admin or active CTM is the one equipped in slot 41. In a simplex operation, the CTM is in slot 41 and a CTM filler module is in slot 42.

Note: Do not replace the Access Panel and CTM simultaneously.

Steps

1 Retrieve all the active alarms and alarm details:

If you want to perform the procedure using	**Then** go to the
CLI commands	“CLI INTERFACE STEPS”
Node Essentials	See the Node Essential steps in “Retrieving the data for the active alarm object” on page 32 in this document. Then go to step 3.

CLI INTERFACE STEPS

2 The following step is performed using CLI commands.

```
show active-alarm <id> [name] [resource] [raise-time]
[raise-time] [cause] [condition-type] [direction]
[location] [severity] [service-impact] [additional-info]
[user-notes...]
```

The current alarms and alarm details will appear.

3 Wear an appropriate ESD personal grounding device to dissipate electrostatic charges. If you are wearing an antistatic wrist strap, connect the cord to the ESD jack on the shelf installed and grounded in a grounded rack or clip to a suitable ground point.

4 Change the equipment admin-state of the CTM to be replaced to “Disabled”.

If you want to perform the procedure using	**Then** go to the
CLI commands	“CLI INTERFACE STEPS”
Node Essentials	“NODE ESSENTIALS STEPS”

Copyright© 2019-2025 Ciena® Corporation

CLI INTERFACE STEPS

5 The following step is performed using CLI commands.

```
set slots <slot #> config circuit-pack admin-state
<Disabled>
```

6 Go to step 12.

NODE ESSENTIALS STEPS

7 Select **Facilities** from the Node Essentials navigation menu.

The Facilities menu opens.

8 From the **Equipment** grid, select the module to be replaced.

9 Click the **Pencil** icon (Edit Equipment).

10 Set the Admin state of the equipment to Disabled

11 Click **Confirm**.

12 When the equipment admin-state of the module to be replaced is “Disabled”, note the following:

The blue LED turns off when the module is set to “Disabled”. In a duplex operation, this can indicate which module to replace.

Note 1: In a duplex operation, only the idle (not active) CTM can be replaced. Otherwise, a CTM switch action is required.

Note 2: Ensure that the blue LED on the module faceplate is off before you remove the module from the backplane. If the blue LED is on, do not pull out the module.

13 If you are replacing the CTM in an R2 shelf, you must remove the R2 fan module first as follows:

a. using a Phillips screwdriver, unfasten the retention screw on the module

b. pull the fan module using the handle until the module is fully disengaged from the backplane

c. remove the fan module using the fan handle and place it in a safe location

CAUTION
Risk of equipment damage
Fan modules must be replaced within 30 seconds of removal to ensure adequate cooling of the shelf. Running the R2 shelf without sufficient cooling can result in equipment damage.

14 Open the latches of the CTM to be replaced by squeezing the locks and rotating the latches outward.

15 Use the latches to pull and unseat the CTM from the backplane.

16 Position the replacement CTM into the tracks of the slot, slide in until the backplane alignments pins are engaged, and then push on the faceplate to partially seat the CTM.

17 Push on both latch handles simultaneously until they rotate into a locked position where the latch catches snap closed to fully seat the CTM.

Copyright© 2019-2025 Ciena® Corporation

CAUTION
Risk of equipment damage
Do not close one latch at a time. Otherwise you risk damaging the connectors.

Do not use excessive force when pushing the lock/eject latches towards the faceplates. If the latches do not lock into place, remove the module and examine the connector at the back of the module. Look for bent pins or damage.

CAUTION
Risk of incorrect installation
Make sure that the CTM lock latches are locked into position. If the lock covers are not locked, the latch sensors on the CTM do not allow the shelf to identify the CTM and do not allow the CTM to autoprovision.

18 For the R2 shelf, install the fan module in the replacement CTM immediately after the CTM insertion. Refer to “Installing and testing fan modules in an R2 shelf” procedure in *6500 RLS Shelf Installation Guide,* 323-2051-201.

19 The red Fail, the green Ready and the blue In Use status LEDs on the front of the CTM go through the following sequence:

- The red LED turns on when the CTM is first inserted.
- After a few seconds, the red, green and blue LEDs turn on.
- After a few seconds, the red and blue LEDs turn off and the green LED flashes to indicate the software is initializing.
- When software initialization is complete, the green status LED turns on (does not flash).

Wait until this sequence is complete before you proceed to the next step.

Software initialization can take up to five minutes and is complete when the green status LED stops flashing and the green Ready LED turns on.

Do not remove the CTM if the green LED is flashing or the blue LED is on.

20 If the “Software Auto-Upgrade in Progress” alarm is active, wait until the alarm clears before continuing.

Note 1: It can take up to 15 minutes for this alarm to clear.

Note 2: The simplex CTM replacement can take up to 30 minutes to complete.

Note 3: If you perform a Secure Erase on the CTM and the secure erased module is returned to Ciena, there is no information remaining on the module that can be used for analysis or troubleshooting.

21 Change the equipment admin-state of the module to “Enabled”.

Copyright© 2019-2025 Ciena® Corporation

If you want to perform the procedure using	Then go to the
CLI commands	"CLI INTERFACE STEPS"
Node Essentials	"NODE ESSENTIALS STEPS"

CLI INTERFACE STEPS

22 The following step is performed using CLI commands.

```
set slots <slot #> config circuit-pack admin-state
<Enabled>
```

23 Go to step 29.

NODE ESSENTIALS STEPS

24 Select **Facilities** from the Node Essentials navigation menu.

The Facilities menu opens.

25 From the **Equipment** grid, select the module to be replaced.

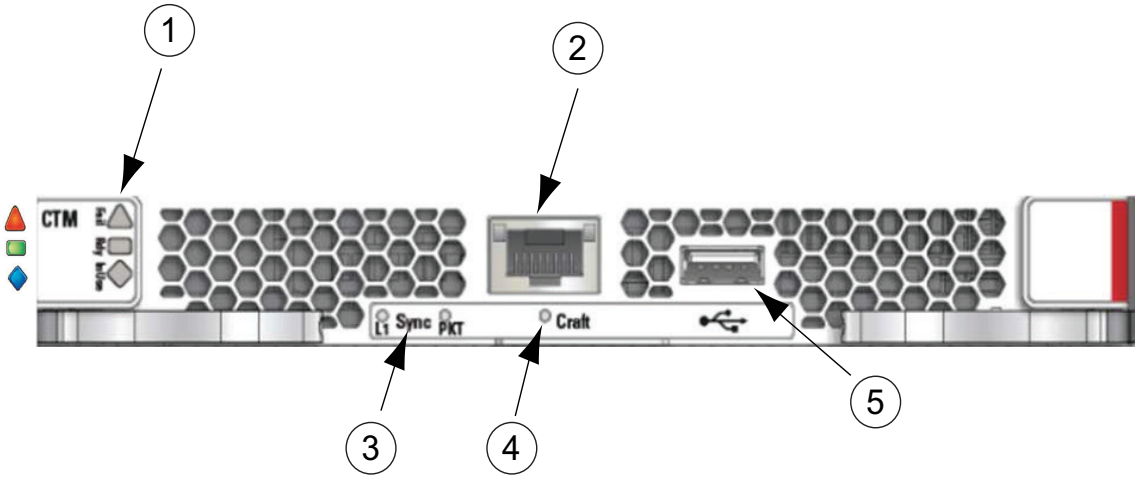
26 Click the **Pencil** icon (Edit Equipment).

27 Set the Admin state of the equipment to Enabled

28 Click **Confirm**.

29 Ensure there are no active alarms against the newly installed module(s).

Figure 20 R4 shelf CTM (NTK810FA or NTK810FB)

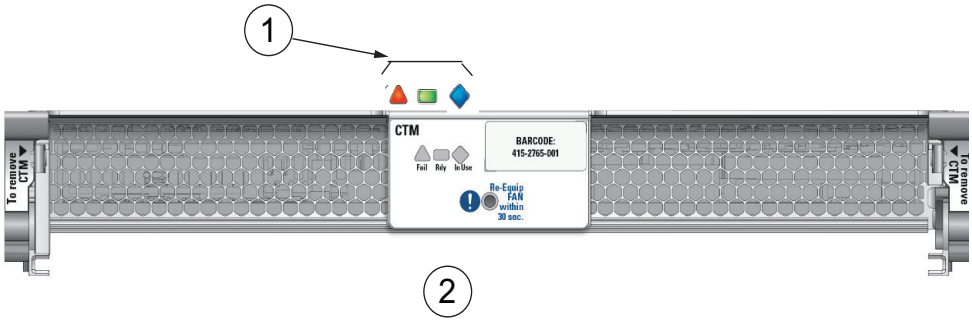


Legend

1	Module LEDs (red/green/blue)	4	Green circle (local craft interface status)
2	Local craft port (RJ45) and Green/Yellow squares (RJ45 Ethernet status indicators)	5	USB 2.0 port
3	Yellow/Green bi-color circle (Synchronization status LEDs)		

Copyright© 2019-2025 Ciena® Corporation

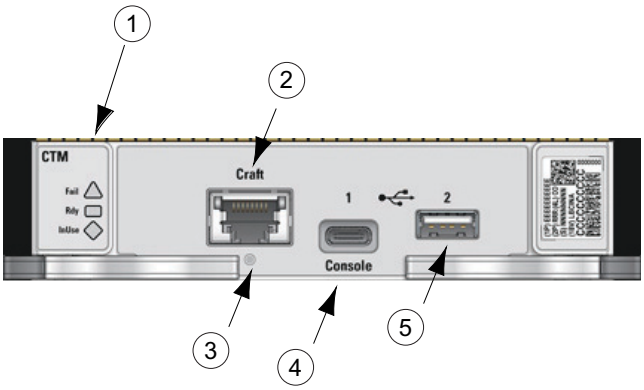
Figure 21 R2 shelf CTM (NTK810DA or NTK810DB)



Legend

1	Module LEDs (red/green/blue)	2	Note: The state of these LEDs for each equipped CTM is also reflected on the Front Panel for 2xCTM (NTK806DA) at the front of the R2 shelf.

Figure 22 R6-300 shelf CTM (NTK810PA)

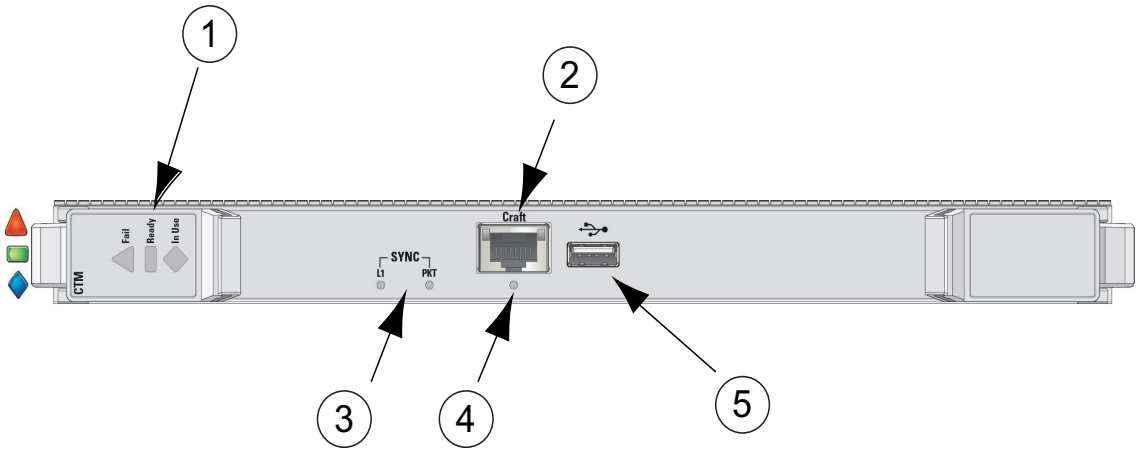


Legend

1	Module LEDS (Red/Green/ Blue)	4	USB-C:USB3.1/Console
2	Local Craft Port (RJ45) and Green/Yellow squares (RJ45 Ethernet status indicators)	5	USB 2.0 Port
3	Green circle (local craft interface status)		

Copyright© 2019-2025 Ciena® Corporation

Figure 23 R8-300 shelf CTM (NTK810QA or NTK810QB)



Legend

1	Module LEDS (Red/Green/ Blue)	4	Green circle (local craft interface status)
2	Local Craft Port (RJ45) and Green/Yellow squares (RJ45 Ethernet status indicators)	5	USB 2.0 Port
3	Yellow/Green bi-color circle (Synchronization status LEDs)		

Copyright© 2019-2025 Ciena® Corporation

Procedure 141 Replacing a CTM front panel on an R2 shelf

Use this procedure to replace the CTM front panel (NTK806DA). The CTM front panel is located in slot 49 on the rear of the R2 shelf.

Requirements

To perform this procedure, you must

- have a replacement CTM front panel. Review the “Ordering information” in *6500 RLS Planning Guide*, NTRN10WA to make sure you select the correct PEC as the replacement part for this product platform.
- observe all safety requirements described in *6500 RLS Shelf Installation Guide*, 323-2051-201

CAUTION
Risk of equipment damage
Electrostatic discharge (ESD) can damage electrostatic sensitive devices. You must use antistatic protection while unpacking and installing all Field-Replaceable Units (FRU) and cables.

Overview

CAUTION
Service affecting procedure
CTM front panel module replacement is service affecting. Ensure you have exhausted all other troubleshooting options before performing this procedure and if possible, re-route the traffic to minimize the traffic loss.

Steps

Removing the CTM front panel module

1 Wear an antistatic wrist strap or foot straps to protect the shelf from static damage. If using a wrist strap, connect the wrist strap to the ESD jack on the shelf.

2

CAUTION
Risk of damage to modules
Never disconnect an optical fiber that is connected to an active or powered up optical amplifier. To disconnect or reconnect an optical fiber, make sure the optical amplifier is “Disabled”.

Copyright© 2019-2025 Ciena® Corporation

Ensure that labels are applied to both ends of all cables and optical fiber patchcords.

3 Push the latch upwards until it disengages. Then pull the latch to remove the panel from the shelf. See Figure 24 on page 307.

4 Unseat and gently pull the CTM front panel until it is fully removed from the R2 shelf.

Installing the CTM front panel into the R2 shelf

5 Verify that the replacement PEC is the same as the current PEC.

6 Position the CTM front panel in the track of slot 49 of the shelf. Slide the CTM front panel in, engaging it into the backplane. See Figure 24 on page 307. Refer to “Installing the Control and Timing Module front panel on an R2 shelf” in *6500 RLS Shelf Installation Guide,* 323-2051-201.

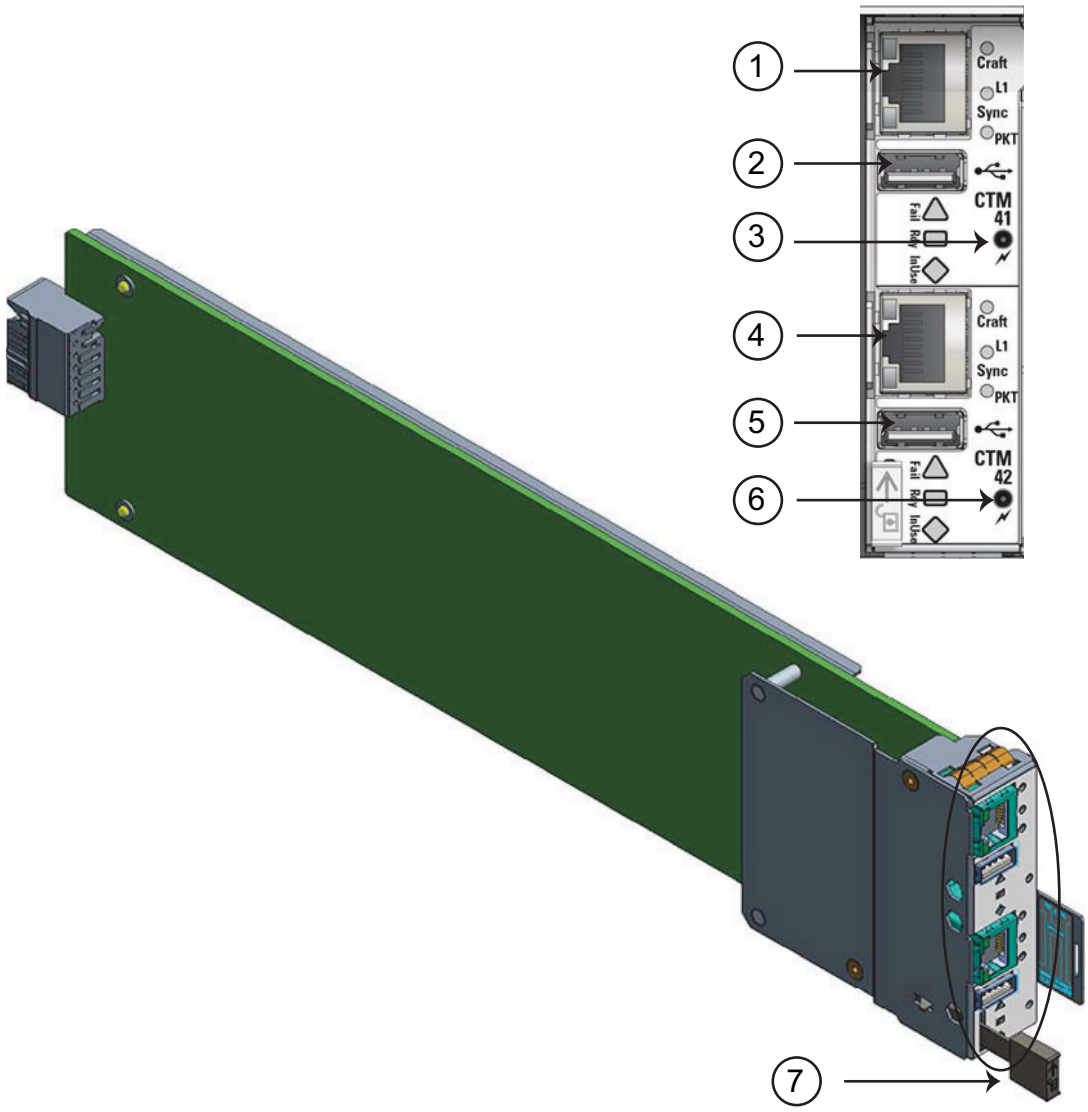
7 Press firmly on the faceplate handle until the spring latch engages and the handle moves down into the latched position.

8 Retrieve all the active alarms and alarm details.

9 Ensure there are no active alarms against the newly installed module(s)s.

Copyright© 2019-2025 Ciena® Corporation

Figure 24 CTM front panel in R2 shelf chassis



Legend

1	Craft port	5	USB
2	USB	6	Reset button
3	Reset button	7	Latch handle
4	Craft port		

Copyright© 2019-2025 Ciena® Corporation

Procedure 142 Reconfiguring a CTM with 8GB DDR memory (RAM) to a CTM with 16GB DDR memory

Use this procedure to reconfigure a Control and Timing Module (CTM) with 8GB DDR memory (RAM) to a CTM with 16GB DDR memory. Note that reconfiguration from 16GB to 8GB is not supported.

Requirements

To perform this procedure, you must:

- Observe all safety requirements described in *6500 RLS Shelf Installation Guide*, 323-2051-201.
- Have the required number of replacement CTM modules available. Review “Ordering Information” in *6500 RLS Planning Guide*, NTRN10WA to make sure you select the correct replacement part.

CAUTION
Risk of equipment damage
Electrostatic discharge (ESD) can damage electrostatic sensitive devices. You must use antistatic protection while unpacking and installing all Field-Replaceable Units (FRU) and cables.

Overview

The following CTM reconfigurations are supported.

- R2 Shelf
  - NTK810DA to NTK810DB
- R4 Shelf
  - NTK810FA to NTK810FB
- R8 Shelf
  - NTK810QA to NTK810QB

RLS supports both dual (also known as protected or duplex) and simplex (unprotected) operation for the Control and Timing Module (CTM). In a duplex operation, two (redundant) CTMs are installed in the shelf, in slot 41 and slot 42. One CTM is always active and controls the shelf while the other CTM is the standby CTM. By default, the admin or active CTM is the one equipped in slot 41. In a simplex operation, the CTM is in slot 41 and a CTM filler module is in slot 42.

Note: Do not replace the Access Panel and CTM simultaneously.

Copyright© 2019-2025 Ciena® Corporation

Steps

1 Retrieve all the active alarms and alarm details:

If you want to perform the procedure using	**Then** go to the
CLI commands	CLI INTERFACE STEPS
Node Essentials	See the Node Essential steps in "Retrieving the data for the active alarm object" on page 32 in this document. Then go to step 3.

CLI INTERFACE STEPS

2 The following step is performed using CLI commands.

```
show active-alarm <id> [name] [resource] [raise-time]
[raise-time] [cause] [condition-type] [direction]
[location] [severity] [service-impact] [additional-info]
[user-notes...]
```

The current alarms and alarm details will appear.

3 Wear an appropriate ESD personal grounding device to dissipate electrostatic charges. If you are wearing an antistatic wrist strap, connect the cord to the ESD jack on the shelf installed and grounded in a grounded rack or clip to a suitable ground point.

4 In a duplex configuration, identify which CTM is in idle state (not active).

If you want to perform the procedure using	**Then** go to the
CLI commands	CLI INTERFACE STEPS
Node Essentials	NODE ESSENTIALS STEPS

CLI INTERFACE STEPS

5 To identify which CTM is in idle state enter the following command.

```
show slots <name> inventory
```

6 In the slot inventory screen that appears, verify that the operational-state indicates "idle".

7 Go to step 9.

NODE ESSENTIALS STEPS

8 Click on the **Chassis** menu and select the module you want to retrieve the inventory for.

The inventory information appears on the right side of the screen.

9 Change the equipment admin-state of the module to be replaced to "Disabled". Refer to "Provisioning a circuit pack or pluggable" procedure in *Equipment/Facility Provisioning and Protection*, 323-2051-310.

The blue LED turns off when the module is set to "Disabled". In a duplex operation, this can indicate which module to replace.

Note 1: In a duplex configuration the idle CTM is replaced first.

Copyright© 2019-2025 Ciena® Corporation

Note 2: Ensure that the blue LED on the module faceplate is off before you remove the module from the backplane. If the blue LED is on, do not pull out the module.

10 If you are replacing the CTM in an R2 shelf, you must remove the R2 fan module first as follows:

a. using a Phillips screwdriver, unfasten the retention screw on the module

b. pull the fan module using the handle until the module is fully disengaged from the backplane

c. remove the fan module using the fan handle and place it in a safe location

CAUTION
Risk of equipment damage
Fan modules must be replaced within 30 seconds of removal to ensure adequate cooling of the shelf. Running the R2 shelf without sufficient cooling can result in equipment damage.

11 Open the latches of the CTM to be replaced by squeezing the locks and rotating the latches outward.

12 Use the latches to pull and unseat the CTM from the backplane.

13 Change the provisioned CTM PEC for the slot.

14 To change the PEC of the slot, you must delete and re-create the slot with the new PEC. Use the following commands:

```
delete slots <slot #> config
set slots <slot #> config circuit-pack pec <string>
```

Example: set slot 42 config circuit-pack pec NTK810FB

Note: There are no equivalent RLS Node Essentials steps for this release.

15 Position the replacement CTM into the tracks of the slot, slide in until the backplane alignments pins are engaged, and then push on the faceplate to partially seat the CTM.

16 Push on both latch handles simultaneously until they rotate into a locked position where the latch catches snap closed to fully seat the CTM.

CAUTION
Risk of equipment damage
Do not close one latch at a time. Otherwise you risk damaging the connectors.

Do not use excessive force when pushing the lock/eject latches towards the faceplates. If the latches do not lock into place, remove the module and examine the connector at the back of the module. Look for bent pins or damage.

Copyright© 2019-2025 Ciena® Corporation

CAUTION
Risk of incorrect installation
Make sure that the CTM lock latches are locked into position. If the lock covers are not locked, the latch sensors on the CTM do not allow the shelf to identify the CTM and do not allow the CTM to autoprovision.

17 For the R2 shelf, install the fan module in the replacement CTM immediately after the CTM insertion. Refer to “Installing and testing fan modules in an R2 shelf” procedure in *6500 RLS Shelf Installation Guide,* 323-2051-201.

18 The red Fail, the green Ready and the blue In Use status LEDs on the front of the CTM go through the following sequence:

- The red LED turns on when the CTM is first inserted.
- After a few seconds, the red, green and blue LEDs turn on.
- After a few seconds, the red and blue LEDs turn off and the green LED flashes to indicate the software is initializing.
- When software initialization is complete, the green status LED turns on (does not flash).

Wait until this sequence is complete before you proceed to the next step.

Software initialization can take up to five minutes and is complete when the green status LED stops flashing and the green Ready LED turns on.

Do not remove the CTM if the green LED is flashing or the blue LED is on.

19 If the “Software Auto-Upgrade in Progress” alarm is active, wait until the alarm clears before continuing.

Note 1: It can take up to 15 minutes for this alarm to clear.

Note 2: If you perform a Secure Erase on the CTM and the secure erased module is returned to Ciena, there is no information remaining on the module that can be used for analysis or troubleshooting.

20 Change the equipment admin-state of the module to “Enabled”. Refer to “Provisioning a circuit pack or pluggable” procedure in *Equipment/Facility Provisioning and Protection*, 323-2051-310.

In a simplex CTM configuration, the procedure is now completed.

21 In a duplex CTM configuration an “Equipment Configuration Mismatch” alarm will be raised as two different CTM types are now configured in the shelf.

22 Perform a CTM equipment switch from the currently active CTM (8GB) to the newly inserted standby CTM (16GB). Refer to “Protection configurations and CTM redundancy” section in *Equipment/Facility Provisioning and Protection*, 323-2051-310.

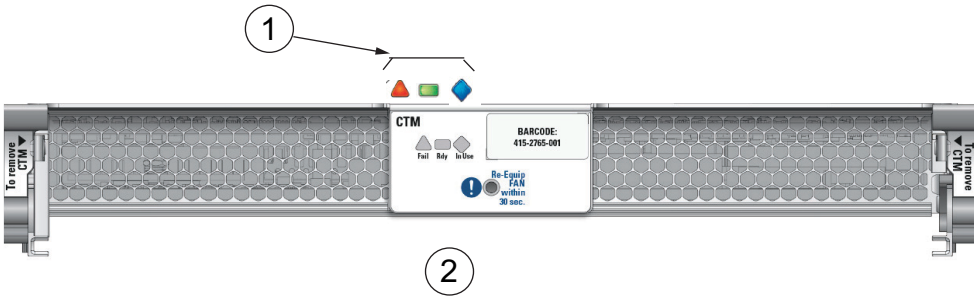
23 Following successful completion of the CTM equipment switch, repeat step 9 to step 20 on the standby CTM (8GB).

24 Following successful completion of the second CTM, the “Equipment Configuration Mismatch” alarm will be cleared.

25 Ensure there are no active alarms against the newly installed module(s).

Copyright© 2019-2025 Ciena® Corporation

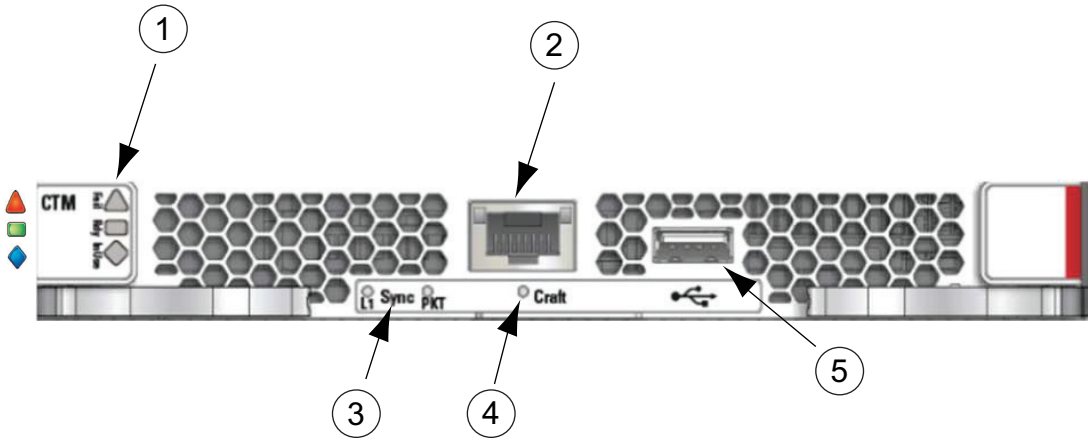
Figure 25 R2 shelf CTM (NTK810DA or NTK810DB)



Legend

1	Module LEDs (red/green/blue)	2	Note: The state of these LEDs for each equipped CTM is also reflected on the Front Panel for 2xCTM (NTK806DA) at the front of the R2 shelf.

Figure 26 R4 shelf CTM (NTK810FA or NTK810FB)

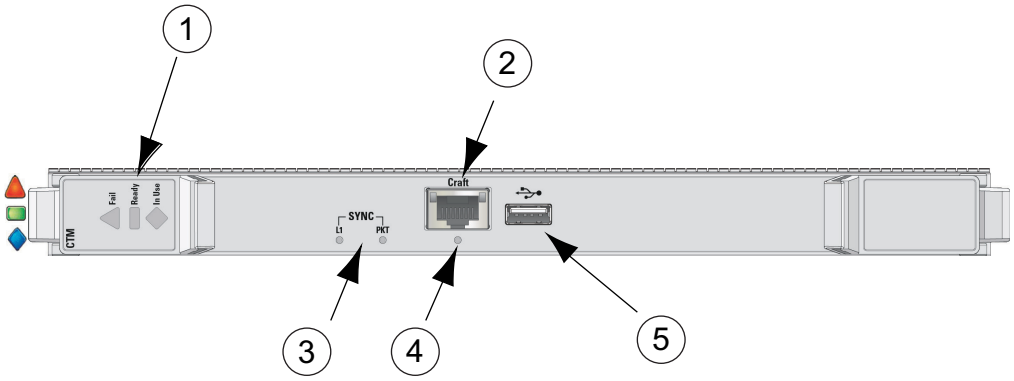


Legend

1	Module LEDs (red/green/blue)	4	Green circle (local craft interface status)
2	Local craft port (RJ45) and Green/Yellow squares (RJ45 Ethernet status indicators)	5	USB 2.0 port
3	Yellow/Green bi-color circle (Synchronization status LEDs)		

Copyright© 2019-2025 Ciena® Corporation

Figure 27 R8-300 shelf CTM (NTK810QA or NTK810QB)



Legend

1	Module LEDS (Red/Green/ Blue)	4	Green circle (local craft interface status)
2	Local Craft Port (RJ45) and Green/Yellow squares (RJ45 Ethernet status indicators)	5	USB 2.0 Port
3	Yellow/Green bi-color circle (Synchronization status LEDs)		

Copyright© 2019-2025 Ciena® Corporation

Procedure 143 Replacing an Access Panel in an R2 shelf

Use this procedure to replace the Access Panel (NTK805NA) in an R2 shelf

Requirements

To perform this procedure, you must:

- have one Access Panel
- review the “Ordering information” in *6500 RLS Planning Guide*, NTRN10WA to make sure you select the correct PEC as the replacement part for this product platform
- observe all safety requirements described in *6500 RLS Shelf Installation Guide*, 323-2051-201
- have one Phillips screwdriver

CAUTION
Risk of equipment damage
Electrostatic discharge (ESD) can damage electrostatic sensitive devices. You must use antistatic protection while unpacking and installing all Field-Replaceable Units (FRU) and cables.

CAUTION
Service affecting procedure
Setting the AP admin-state to “Disabled” will lock the file system on the AP. All other LAN ports or console/telemetry port are not impacted when the AP admin-state is “Disabled”. The CTM will no longer try to access the AP file system. If the AP admin-state is not set to “Disabled” prior to removing the AP, the CTM will continue to access the AP file system and when the AP is removed, the active CTM restarts.

Overview

The AP can be replaced with either a factory-fresh or previously used AP. Once the new AP is installed, it will backup the active CTMs configuration data. In a duplex CTM operation, if the AP fails, the primary CTM restarts, resulting in a switch-over. RLS shelves continue to carry services uninterrupted in case of AP failure or AP removal.

Note: Do not replace the Access Panel and CTM simultaneously.

Steps

1 Retrieve all the active alarms and alarm details:

Copyright© 2019-2025 Ciena® Corporation

If you want to perform the procedure using	**Then** go to the
CLI commands	"CLI INTERFACE STEPS"
Node Essentials	See the Node Essential steps in "Retrieving the data for the active alarm object" on page 32 in this document. Then go to step 3.

CLI INTERFACE STEPS

2 To retrieve all the active alarms and alarm details, enter:

```
show active-alarm <id> [name] [resource] [raise-time]
[raise-time] [cause] [condition-type] [direction]
[location] [severity] [service-impact] [additional-info]
[user-notes...]
```

The current alarms and alarm details will appear.

3 Ensure that there is no retrieve-log operation running by verifying that the "Log Collection In Progress" alarm is not active.

4 Retrieve upgrade state to ensure it is idle.

If you want to perform the procedure using	**Then** go to the
CLI commands	"CLI INTERFACE STEPS"
Node Essentials	"NODE ESSENTIALS STEPS"

CLI INTERFACE STEPS

5 To retrieve upgrade state to ensure it is idle, enter:

```
show software [active-version][committed-
version][component][last-operation][upgrade-operational-
state][upgrade-to-version]
```

6 Go to step 8.

NODE ESSENTIALS STEPS

7 From the **Configuration** menu, select Software maintenance.

The Software maintenance menu opens indicating the running and committed software version.

8 Provision the admin state of the module to "Disabled".

If you want to perform the procedure using	**Then** go to the
CLI commands	"CLI INTERFACE STEPS"
Node Essentials	"NODE ESSENTIALS STEPS"

CLI INTERFACE STEPS

9 The following step is performed using CLI commands.

```
set slots <40> config circuit-pack admin-state <Disabled>
```

10 Go to step 16.

Copyright© 2019-2025 Ciena® Corporation

NODE ESSENTIALS STEPS

11 Select **Facilities** from the Node Essentials navigation menu.

The Facilities menu opens.

12 From the **Equipment** grid, select the module to be replaced.

13 Click the **Pencil** icon (Edit Equipment).

14 Set the Admin state of the equipment to Disabled

15 Click **Confirm**.

16 Wear an antistatic wrist strap or foot straps to protect the shelf from static damage. If using a wrist strap, connect the wrist strap to the ESD jack on the shelf.

17 Disconnect the control and communication connectors and any wire wrap adapters (if being used) from the access panel.

18 Push the spring latch upward until disengages and pull to remove the panel from the shelf. See Figure 28, “R2 shelf Access Panel (NTK805NA)”.

Note: While the Access Panel is removed from the chassis, COLAN, ILAN, Console and Telemetry ports will not be operational.

19 Insert the new access panel carefully into the slot guide grooves and slide it in, engaging it into the backplane. Ensure that the access panel seats securely into the backplane. Refer to “Installing the access panel for the R2 shelf” procedure in the *6500 RLS Shelf Installation Guide, 323*-2051-201.

20 Connect the control and communication cables to the access panel.

21 Provision the admin state of the module to “Enabled”.

If you want to perform the procedure using	**Then** go to the
CLI commands	“CLI INTERFACE STEPS”
Node Essentials	“NODE ESSENTIALS STEPS”

CLI INTERFACE STEPS

22 The following step is performed using CLI commands.

```
set slots <40> config circuit-pack admin-state <Enabled>
```

23 Go to step 29.

NODE ESSENTIALS STEPS

24 Select **Facilities** from the Node Essentials navigation menu.

The Facilities menu opens.

25 From the **Equipment** grid, select the module to be replaced.

26 Click the **Pencil** icon (Edit Equipment).

27 Set the Admin state of the equipment to Enabled

28 Click **Confirm**.

29 Perform the following commands on ILAN ports that have an SFP installed:

```
set openconfig-interfaces:interfaces interface <ilan-in/
ilan-out> config enabled false
```


Copyright© 2019-2025 Ciena® Corporation

```
set openconfig-interfaces:interfaces interface <ilan-in/
ilan-out> config enabled true
```

For more information refer to *CLI Reference*, 323-2051-190.

Note: There are no equivalent RLS Node Essentials steps for this release.

30 Restore the software load to the new AP disk. Perform a shelf software delivery using the software load matching to the NE version by following this command:

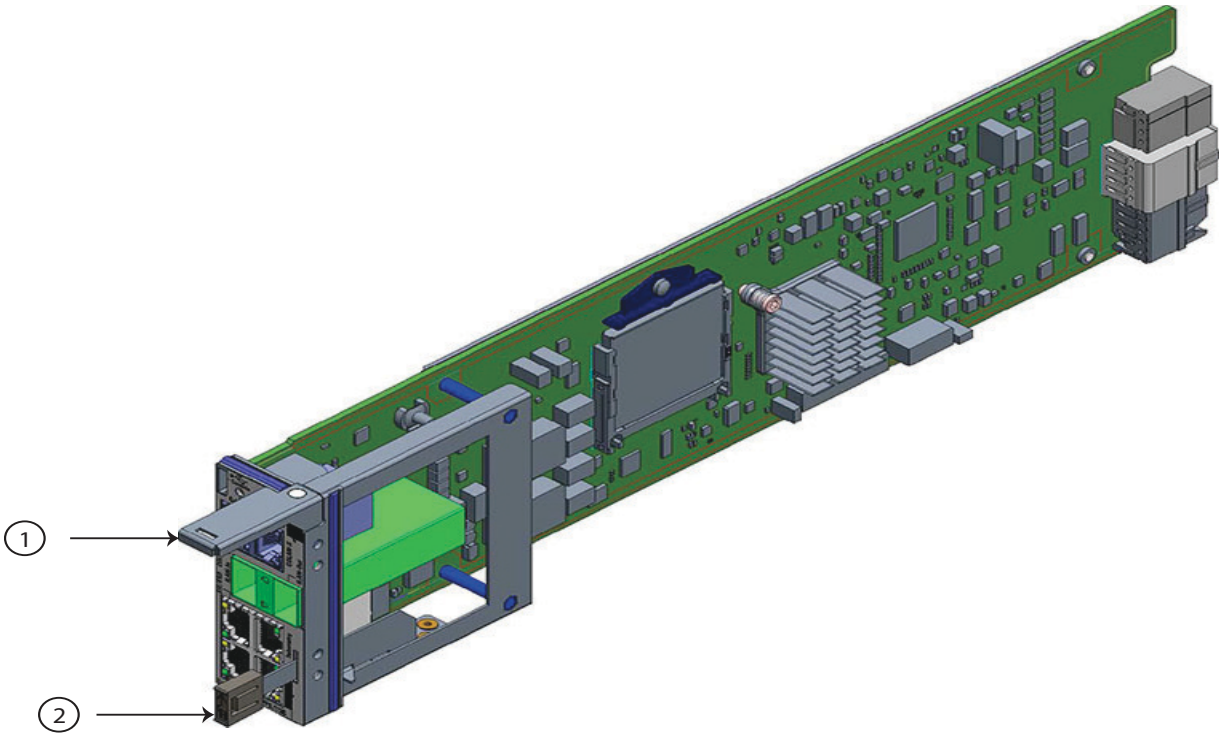
```
CLI# software-deliver uri <URI to committed-version.tgz>
```

This will restore the NE software load onto the disk of the newly inserted AP, and align the AP software load with the NE software load.

31 Ensure there are no active alarms against the newly installed module(s).

The following figure shows the Access Panels for the R2 shelf.

Figure 28 R2 shelf Access Panel (NTK805NA)



Legend

1	Faceplate handle	2	Module latch

Copyright© 2019-2025 Ciena® Corporation

Procedure 144 Replacing an Access Panel in an R4 shelf

Use this procedure to replace the R4 shelf Access Panels (NTK805MA/NTK805MB) or to reconfigure the R4 shelf Access Panel from NTK805MA to Type 2 Access Panel (NTK805MB).

Requirements

To perform this procedure, you must:

- have one Access Panel
- review the “Ordering information” in *6500 RLS Planning Guide*, NTRN10WA, to make sure you select the correct PEC as the replacement part for this product platform.
- observe all safety requirements described in *6500 RLS Shelf Installation Guide,* 323-2051-201
- have one Phillips screwdriver

CAUTION
Risk of equipment damage
Electrostatic discharge (ESD) can damage electrostatic sensitive devices. You must use antistatic protection while unpacking and installing all Field-Replaceable Units (FRU) and cables.

CAUTION
Service affecting procedure
Setting the AP admin-state to “Disabled” will lock the file system on the AP. All other LAN ports or console/telemetry port are not impacted when the AP admin-state is “Disabled”. The CTM will no longer try to access the AP file system. If the AP admin-state is not set to “Disabled” prior to removing the AP, the CTM will continue to access the AP file system and when the AP is removed, the active CTM restarts.

Overview

The following Access Panels are supported in the R4 shelf.

- Access Panel (NTK805MA)
- Access Panel Type 2 (NTK805MB)

Refer to “Access Panel (NTK805MA/MB, NTK805NA, NTK805QA)” in the *6500 RLS Planning Guide,*NTRN10WA for more details on the capabilities of each Access Panel.

Copyright© 2019-2025 Ciena® Corporation

Note: : Order and use Access Panel Type 2 (R4) (NTK805MB) if the application will require more than three external slot ports (such as used to connect to Fiber Interconnect Module (FIM) Type 4A, NTK504CX).

When removing and replacing the Access Panel in an R4 shelf, the same model of Access Panel should be used for the replacement.

- NTK805MA is replaced with NTK805MA
- NKT805MB is replaced with NTK805MB

If required, the RLS system will support a reconfiguration of the Access Panel in an R4 shelf as follows.

- R4 Access Panel (NTK805MA) to R4 Access Panel Type 2 (NTK805MB)

The AP can be replaced with either a factory-fresh or previously used AP. Once the new AP is installed, it will backup the active CTMs configuration data. In a duplex CTM operation, if the AP fails, the primary CTM restarts, resulting in a switch-over. RLS shelves continue to carry services uninterrupted in case of AP failure or AP removal.

Note: Do not replace the Access Panel and CTM simultaneously.

Steps

1 Retrieve all the active alarms and alarm details:

If you want to perform the procedure using	**Then** go to the
CLI commands	"CLI INTERFACE STEPS"
Node Essentials	See the Node Essential steps in "Retrieving the data for the active alarm object" on page 32 in this document. Then go to step 3.

CLI INTERFACE STEPS

2 To retrieve all the active alarms and alarm details, enter:

```
show active-alarm <id> [name] [resource] [raise-time]
[raise-time] [cause] [condition-type] [direction]
[location] [severity] [service-impact] [additional-info]
[user-notes...]
```

The current alarms and alarm details will appear.

3 Ensure that there is no retrieve-log operation running by verifying that the "Log Collection In Progress" alarm is not active.

4 Retrieve upgrade state to ensure it is idle. Refer to *CLI Reference*, 323-2051-190.

Copyright© 2019-2025 Ciena® Corporation

If you want to perform the procedure using	Then go to the
CLI commands	"CLI INTERFACE STEPS"
Node Essentials	"NODE ESSENTIALS STEPS"

CLI INTERFACE STEPS

5 To retrieve upgrade state, enter:

```
show software [active-version][committed-
version][component][last-operation][upgrade-operational-
state][upgrade-to-version]
```

6 Go to step 8.

NODE ESSENTIALS STEPS

7 From the **Configuration** menu, select Software maintenance.

The Software maintenance menu opens indicating the running and committed software version.

8 Provision the admin state of the module to "Disabled".

If you want to perform the procedure using	Then go to the
CLI commands	"CLI INTERFACE STEPS"
Node Essentials	"NODE ESSENTIALS STEPS"

CLI INTERFACE STEPS

9 The following step is performed using CLI commands.

```
set slots <40> config circuit-pack admin-state <Disabled>
```

10 Go to step 16.

NODE ESSENTIALS STEPS

11 Select **Facilities** from the Node Essentials navigation menu.

The Facilities menu opens.

12 From the **Equipment** grid, select the module to be replaced.

13 Click the **Pencil** icon (Edit Equipment).

14 Set the Admin state of the equipment to Disabled

15 Click **Confirm**.

16 Wear an antistatic wrist strap or foot straps to protect the shelf from static damage. If using a wrist strap, connect the wrist strap to the ESD jack on the shelf.

17 Disconnect the control and communication connectors from the access panel.

18 Using a Phillips screwdriver, unscrew the thumbscrew on left side to shelf wall of the panel. Pull out the access panel by sliding it out and disengaging it from the backplane. See Figure 29, "R4 shelf Access Panel (NTK805MA)/R4 shelf Access Panel Type 2 (NTK805MB)".

Copyright© 2019-2025 Ciena® Corporation

Note: While the Access Panel is removed from the chassis, COLAN, ILAN, Console and Telemetry ports will not be operational.

19 If the AP is being reconfigured from NTK805MA to NTK805MB, the provisioned PEC for the slot must be changed.

20 To change the provisioned PEC for the slot, use the following command:

```
set slots <slot #> config circuit-pack pec <string>
```

Example: set slots <40> config circuit-pack pec <NTK805MB>

Note: There are no equivalent RLS Node Essentials steps for this release.

21 Insert the new access panel carefully into the slot guide grooves and slide it in, engaging it into the backplane. Ensure that the access panel seats securely into the backplane. Refer to “Installing the access panel for the R4 shelf” procedure in the *6500 RLS Shelf Installation Guide,* 323-2051-201.

22 Tighten the thumbscrew on left side to shelf wall on the new access panel.

23 Connect the control and communication cables to the access panel.

Note: The configuration of the control and communication ports differ between the R4 Access Panel (NTK805MA) and the R4 Access Panel Type 2 (NTK805MB). Refer to “Access Panel (NTK805MA/MB, NTK805NA, NTK805QA) in the *6500 RLS Planning Guide*NTRN10WAf for more details on the supported ports and location on each Access Panel.

24 Choose your next step.

If	**Then** go to
you have replaced the AP with an AP of the same type (the same PEC code)	step 25
you have reconfigured the AP from NTK805MA to NTK805MB	step 33

25 Provision the admin state of the module to “Enabled”.

If you want to perform the procedure using	**Then** go to the
CLI commands	“CLI INTERFACE STEPS”
Node Essentials	“NODE ESSENTIALS STEPS”

CLI INTERFACE STEPS

26 The following step is performed using CLI commands.

```
set slots <40> config circuit-pack admin-state <Enabled>
```

27 Go to step 33.

NODE ESSENTIALS STEPS

28 Select **Facilities** from the Node Essentials navigation menu.

The Facilities menu opens.

29 From the **Equipment** grid, select the module to be replaced.

30 Click the **Pencil** icon (Edit Equipment).

Copyright© 2019-2025 Ciena® Corporation

31 Set the Admin state of the equipment to Enabled

32 Click **Confirm**.

33 Perform the following commands on ILAN ports that have an SFP installed:

```
set openconfig-interfaces:interfaces interface <ilan-in2/ilan-out2> config enabled false
```

```
set openconfig-interfaces:interfaces interface <ilan-in2/ilan-out2> config enabled true
```

For more information refer to *CLI Reference*, 323-2051-190.

Note: There are no equivalent RLS Node Essentials steps for this release.

34 Restore the software load to the new AP disk. Perform a shelf software delivery using the software load matching to the NE version by following this command:

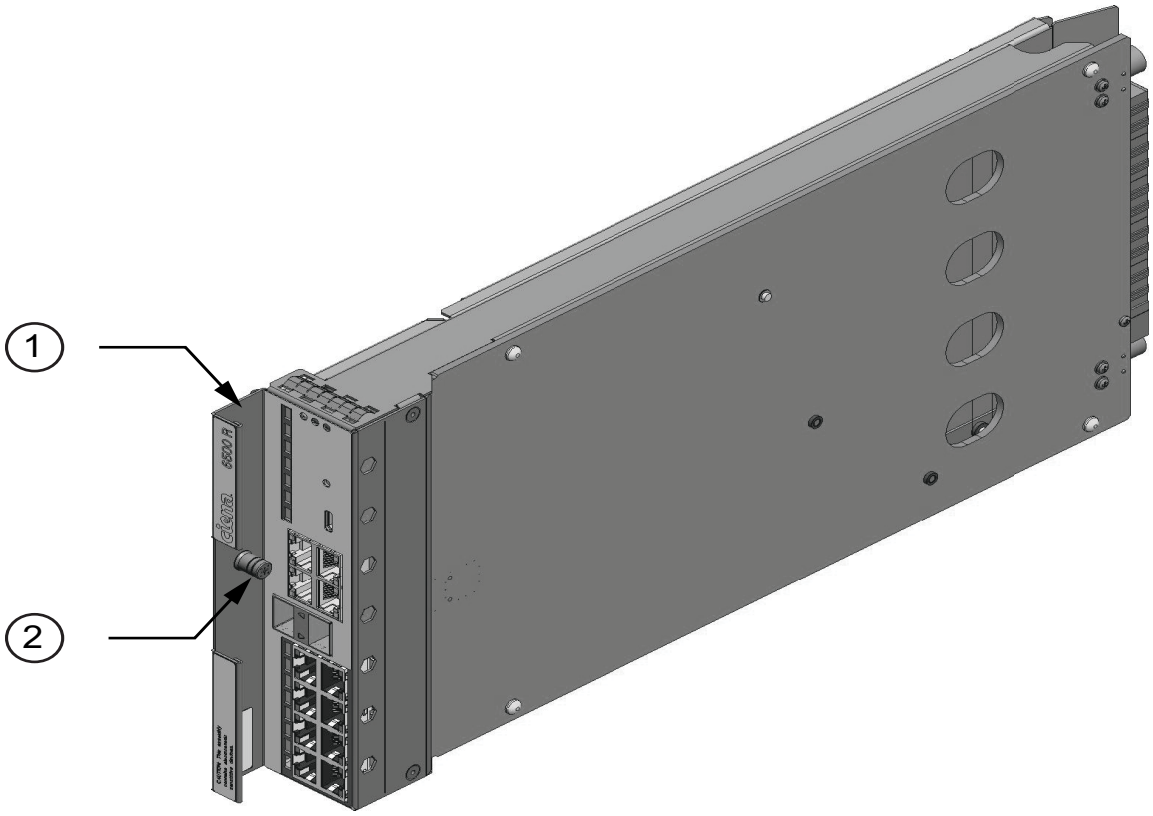
```
CLI# software-deliver uri <URI to committed-version.tgz>
```

This will restore the NE software load onto the disk of the newly inserted AP, and align the AP software load with the NE software load.

35 Ensure there are no active alarms against the newly installed module(s).

The following figure shows the Access Panel for R4 shelf.

Figure 29 R4 shelf Access Panel (NTK805MA)/R4 shelf Access Panel Type 2 (NTK805MB)



Copyright© 2019-2025 Ciena® Corporation

Legend

1	Faceplate handle
2	Retaining thumbscrew

Copyright© 2019-2025 Ciena® Corporation

Procedure 145 Replacing an Access Panel in an R6-300 shelf

Use this procedure to replace the Access Panel (NTK805PA) in an R6-300 shelf.

Requirements

To perform this procedure, you must:

- have one Access Panel
- review the “Ordering information” in *6500 RLS Planning Guide*, NTRN10WA to make sure you select the correct PEC as the replacement part for this product platform.
- observe all safety requirements described in *6500 RLS Shelf Installation Guide,* 323-2051-201

CAUTION
Risk of equipment damage
Electrostatic discharge (ESD) can damage electrostatic sensitive devices. You must use antistatic protection while unpacking and installing all Field-Replaceable Units (FRU) and cables.

CAUTION
Service affecting procedure
Setting the AP admin-state to “Disabled” will lock the file system on the AP. All other LAN ports or console/telemetry port are not impacted when the AP admin-state is “Disabled”. The CTM will no longer try to access the AP file system. If the AP admin-state is not set to “Disabled” prior to removing the AP, the CTM will continue to access the AP file system and when the AP is removed, the active CTM will restart.

Overview

The AP can be replaced with either a factory-fresh or previously used AP. Once the new AP is installed, it will backup the active CTMs configuration data. In a duplex CTM operation, if the AP fails, the primary CTM restarts, resulting in a switch-over. RLS shelves continue to carry services uninterrupted in case of AP failure or AP removal.

Note: Do not replace the Access Panel and CTM simultaneously.

Steps

1 Retrieve all the active alarms and alarm details:

Copyright© 2019-2025 Ciena® Corporation

If you want to perform the procedure using	Then go to the
CLI commands	CLI INTERFACE STEPS
Node Essentials	See the Node Essential steps in "Retrieving the data for the active alarm object" on page 32 in this document. Then go to step 3.

CLI INTERFACE STEPS

2 To retrieve all the active alarms and alarm details, enter:

```
show active-alarm <id> [name] [resource] [raise-time]
[raise-time] [cause] [condition-type] [direction]
[location] [severity] [service-impact] [additional-info]
[user-notes...]
```

The current alarms and alarm details will appear.

3 Ensure that there is no retrieve-log operation running by verifying that the "Log Collection In Progress" alarm is not active.

4 Retrieve upgrade state to ensure it is idle. Refer to *CLI Reference*, 323-2051-190.

If you want to perform the procedure using	Then go to the
CLI commands	CLI INTERFACE STEPS
Node Essentials	NODE ESSENTIALS STEPS

CLI INTERFACE STEPS

5 The following step is performed using CLI commands.

```
show software [active-version][committed-
version][component][last-operation][upgrade-operational-
state][upgrade-to-version]
```

6 Go to step 9.

NODE ESSENTIALS STEPS

7 The following steps are performed using Node Essentials.

Retrieving the software version and upgrade status

8 From the **Configuration** menu, select Software maintenance.

The Software maintenance screen opens indicating the running and committed software version.

Placing the module admin-state in Disabled status

9 Provision the admin state of the module to "Disabled".

If you want to perform the procedure using	Then go to the
CLI commands	CLI INTERFACE STEPS
Node Essentials	NODE ESSENTIALS STEPS

Copyright© 2019-2025 Ciena® Corporation

CLI INTERFACE STEPS

10 The following step is performed using CLI commands.

```
set slots <40> config circuit-pack admin-state <Disabled>
```

11 Click **Confirm**.

12 Go to step 18.

NODE ESSENTIALS STEPS

13 Select **Facilities** from the Node Essentials navigation menu.

The Facilities menu opens.

14 From the **Equipment** grid, select the module to be replaced.

15 Click the **Pencil** icon (Edit Equipment).

16 Set the Admin state of the equipment to Disabled

17 Click **Confirm**.

18 Wear an antistatic wrist strap or foot straps to protect the shelf from static damage. If using a wrist strap, connect the wrist strap to the ESD jack on the shelf.

19 Disconnect the control and communication connectors from the access panel.

20 Use your fingers to push the latch lever to the left, and pull the tab of the access panel to pull access panel by sliding it out and disengaging it from the backplane. See Figure 30 on page 327.

Note: While the Access Panel is removed from the chassis, COLAN, ILAN, Console and Telemetry ports will not be operational.

21 Insert the new access panel carefully into the slot guide grooves and slide it in, engaging it into the backplane. Ensure that the access panel seats securely into the backplane. Refer to “Installing the access panel for the R6-300” shelf procedure in the *6500 RLS Shelf Installation Guide,* 323-2051-201.

22 Connect the control and communication cables to the access panel.

23 Provision the admin state of the module to “Enabled”.

If you want to perform the procedure using	**Then** go to the
CLI commands	CLI INTERFACE STEPS
Node Essentials	NODE ESSENTIALS STEPS

CLI INTERFACE STEPS

24 The following step is performed using CLI commands.

```
set slots <40> config circuit-pack admin-state <Enabled>
```

25 Go to step 31.

NODE ESSENTIALS STEPS

26 Select **Facilities** from the Node Essentials navigation menu.

The Facilities menu opens.

27 From the **Equipment** grid, select the module to be replaced.

Copyright© 2019-2025 Ciena® Corporation

28 Click the **Pencil** icon (Edit Equipment).

29 Set the Admin state of the equipment to Enabled

30 Click **Confirm**.

31 Perform the following commands on ILAN ports that have an SFP installed:

```
set openconfig-interfaces:interfaces interface <ilan-in2/ilan-out2> config enabled false
```

```
set openconfig-interfaces:interfaces interface <ilan-in2/ilan-out2> config enabled true
```

For more information refer to *CLI Reference*, 323-2051-190.

Note: There are no equivalent RLS Node Essentials steps for this release.

32 Restore the software load to the new AP disk. Perform a shelf software delivery using the software load matching to the NE version **by following this command**:

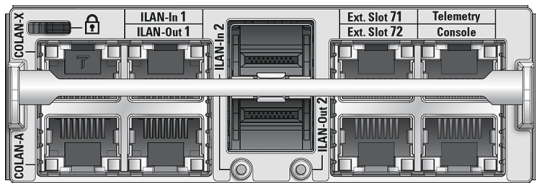
```
CLI# software-deliver uri <URI to committed-version.tgz>
```

This will restore the NE software load onto the disk of the newly inserted AP, and align the AP software load with the NE software load.

33 Ensure there are no active alarms against the newly installed module(s).

The following figure shows the Access Panel for the R6-300 shelf.

Figure 30 R6-300 shelf Access Panel (NTK805PA)



Copyright© 2019-2025 Ciena® Corporation

Procedure 146 Replacing an Access Panel in an R8-300 shelf

Use this procedure to replace the Access Panel (NTK805QA) in an R8-300 shelf.

Requirements

To perform this procedure, you must:

- have one Access Panel
- review the “Ordering information” in *6500 RLS Planning Guide*, NTRN10WA to make sure you select the correct PEC as the replacement part for this product platform.
- observe all safety requirements described in *6500 RLS Shelf Installation Guide,* 323-2051-201
- have one Phillips screwdriver

CAUTION
Risk of equipment damage
Electrostatic discharge (ESD) can damage electrostatic sensitive devices. You must use antistatic protection while unpacking and installing all Field-Replaceable Units (FRU) and cables.

CAUTION
Service affecting procedure
Setting the AP admin-state to “Disabled” will lock the file system on the AP. All other LAN ports or console/telemetry port are not impacted when the AP admin-state is “Disabled”. The CTM will no longer try to access the AP file system. If the AP admin-state is not set to “Disabled” prior to removing the AP, the CTM will continue to access the AP file system and when the AP is removed, the active CTM will restart.

Overview

The AP can be replaced with either a factory-fresh or previously used AP. Once the new AP is installed, it will backup the active CTMs configuration data. In a duplex CTM operation, if the AP fails, the primary CTM restarts, resulting in a switch-over. RLS shelves continue to carry services uninterrupted in case of AP failure or AP removal.

Note: Do not replace the Access Panel and CTM simultaneously.

Copyright© 2019-2025 Ciena® Corporation

Steps

1 Retrieve all the active alarms and alarm details:

If you want to perform the procedure using	**Then** go to the
CLI commands	"CLI INTERFACE STEPS"
Node Essentials	See the Node Essential steps in "Retrieving the data for the active alarm object" on page 32 in this document. Then go to step 3.

CLI INTERFACE STEPS

2 To retrieve all the active alarms and alarm details, enter:

```
show active-alarm <id> [name] [resource] [raise-time]
[raise-time] [cause] [condition-type] [direction]
[location] [severity] [service-impact] [additional-info]
[user-notes...]
```

The current alarms and alarm details will appear.

3 Ensure that there is no retrieve-log operation running by verifying that the "Log Collection In Progress" alarm is not active.

4 Retrieve upgrade state to ensure it is idle. Refer to *CLI Reference*, 323-2051-190.

If you want to perform the procedure using	**Then** go to the
CLI commands	"CLI INTERFACE STEPS"
Node Essentials	"NODE ESSENTIALS STEPS"

CLI INTERFACE STEPS

5 The following step is performed using CLI commands.

```
show software [active-version][committed-
version][component][last-operation][upgrade-operational-
state][upgrade-to-version]
```

6 Go to step 9.

NODE ESSENTIALS STEPS

7 The following steps are performed using Node Essentials.

Retrieving the software version

8 From the **Configuration** menu, select Software maintenance.

The Software maintenance screen opens indicating the running and committed software version.

9 Provision the admin state of the module to "Disabled".

Copyright© 2019-2025 Ciena® Corporation

If you want to perform the procedure using	**Then** go to the
CLI commands	"CLI INTERFACE STEPS"
Node Essentials	"NODE ESSENTIALS STEPS"

CLI INTERFACE STEPS

10 The following step is performed using CLI commands.

```
set slots <40> config circuit-pack admin-state <Disabled>
```

11 Go to step 17.

NODE ESSENTIALS STEPS

12 Select **Facilities** from the Node Essentials navigation menu.

The Facilities menu opens.

13 From the **Equipment** grid, select the module to be replaced.

14 Click the **Pencil** icon (Edit Equipment).

15 Set the Admin state of the equipment to Disabled

16 Click **Confirm**.

17 Wear an antistatic wrist strap or foot straps to protect the shelf from static damage. If using a wrist strap, connect the wrist strap to the ESD jack on the shelf.

18 Disconnect the control and communication connectors from the access panel.

19 Using a Phillips screwdriver, unscrew the captive screws on each side of the faceplate. See Figure 31, "R8-300 shelf Access Panel (NTK805QA)".

20 Use your thumbs to swing the latches on both sides of the access panel into the open position. Pull out the access panel by sliding it out and disengaging it from the backplane.

Note: While the Access Panel is removed from the chassis, COLAN, ILAN, Console and Telemetry ports will not be operational.

21 Insert the new access panel carefully into the slot guide grooves and slide it in, engaging it into the backplane. Ensure that the access panel seats securely into the backplane. Refer to "Installing the access panel for the R8-300" shelf procedure in the *6500 RLS Shelf Installation Guide,* 323-2051-201.

22 Connect the control and communication cables to the access panel.

23 Provision the admin state of the module to "Enabled".

If you want to perform the procedure using	**Then** go to the
CLI commands	"CLI INTERFACE STEPS"
Node Essentials	"NODE ESSENTIALS STEPS"

CLI INTERFACE STEPS

24 The following step is performed using CLI commands.

```
set slots <40> config circuit-pack admin-state <Enabled>
```


Copyright© 2019-2025 Ciena® Corporation

25 Go to step 31.

NODE ESSENTIALS STEPS

26 Select **Facilities** from the Node Essentials navigation menu.

The Facilities menu opens.

27 From the **Equipment** grid, select the module to be replaced.

28 Click the **Pencil** icon (Edit Equipment).

29 Set the Admin state of the equipment to Enabled

30 Click **Confirm**.

31 Perform the following commands on ILAN ports that have an SFP installed:

```
set openconfig-interfaces:interfaces interface <ilan-in2/ilan-out2> config enabled false
```

```
set openconfig-interfaces:interfaces interface <ilan-in2/ilan-out2> config enabled true
```

For more information refer to *CLI Reference*, 323-2051-190.

Note: There are no equivalent RLS Node Essentials steps for this release.

32 Restore the software load to the new AP disk. Perform a shelf software delivery using the software load matching to the NE version **by following this command**:

```
CLI# software-deliver uri <URI to committed-version.tgz>
```

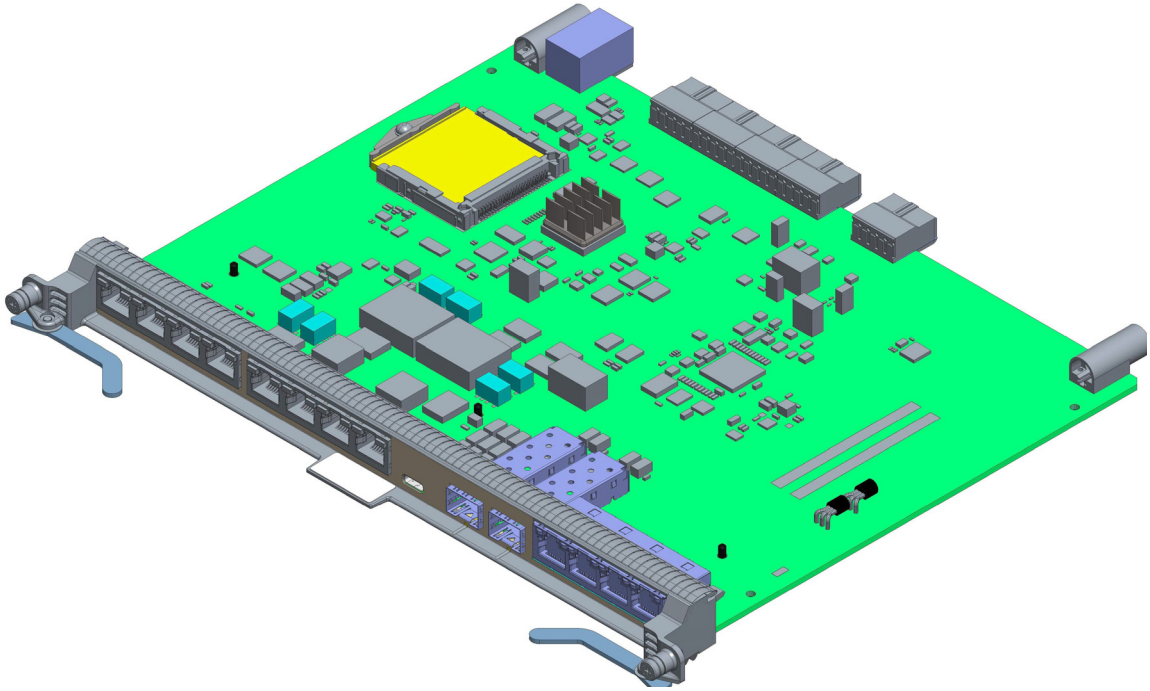
This will restore the NE software load onto the disk of the newly inserted AP, and align the AP software load with the NE software load.

33 Ensure there are no active alarms against the newly installed module(s).

The following figure shows the Access Panel for the R8-300 shelf.

Copyright© 2019-2025 Ciena® Corporation

Figure 31 R8-300 shelf Access Panel (NTK805QA)



Copyright© 2019-2025 Ciena® Corporation

Procedure 147 Replacing a pluggable module

Use this procedure to replace pluggable module.

Requirements

To perform this procedure, you must

- obtain a supported pluggable module. Review the Module descriptions, equipping rules, specifications in *6500 RLS Planning Guide*, NTRN10WA to make sure you select the correct PEC as the replacement part for this product platform
- ensure that you have all the documentation referenced in this procedure
- ensure that you have the LC fiber tool (174-0099-900)
- observe all safety requirements described in *6500 RLS Shelf Installation Guide*, 323-2051-201
- ensure that all alarms are enabled.
- use an account with admin privileges or higher

CAUTION
Risk of equipment damage
Electrostatic discharge (ESD) can damage electrostatic sensitive devices. You must use antistatic protection while unpacking and installing all Field-Replaceable Units (FRU) and cables.

Overview

CAUTION
Risk of loss of network reliability
Make sure that all optical connectors are cleaned before you make the connections (or re-connections) described in this procedure. For instructions on cleaning optical fiber, refer to *Optical Connector Inspection and Cleaning*, 323-1859-500.

CAUTION
Risk of personal injury
When inserted in a shelf slot, the optical interface module emits laser light that can blind. Keep all optical connectors on the optical interface modules capped when they are not connected to optical fiber cables. Never look directly into the end of an optical fiber.

Copyright© 2019-2025 Ciena® Corporation

ATTENTION
Keep the number of mating cycles of the SFP modules to the carrier modules below the maximum limit of 50 (to maintain the service life reliability of the interfaces).

Steps

1 Retrieve all the active alarms and alarm details:

If you want to perform the procedure using	**Then** go to the
CLI commands	"CLI INTERFACE STEPS"
Node Essentials	"NODE ESSENTIALS STEPS"

CLI INTERFACE STEPS

2 To retrieve all the active alarms and alarm details, enter:

```
show active-alarm <id> [name] [resource] [raise-time]
[raise-time] [cause] [condition-type] [direction]
[location] [severity] [service-impact] [additional-info]
[user-notes...]
```

The current alarms and alarm details will appear.

3 Go to step 5.

NODE ESSENTIALS STEPS

4 From the **Alarms** menu, select Current alarms.

The active alarm menu opens indicating the data for the active-alarm object.

5

If you are replacing a pluggable module in	**Then** go to
a protected configuration	step 6
an unprotected configuration	step 7

6 Switch traffic away from the pluggable module to be replaced. Perform a manual switch to verify the inactive path. Refer to the "Operating a manual TPS/TPS2 protection switch" procedure in *Equipment/Facility Provisioning and Protection*, 323-2051-310.

If traffic switches back autonomously to the active path or if the manual switch is denied, contact your next level of support or your Ciena support group.

7 Change the corresponding facility of the pluggable module to be replaced to "Disabled". Refer to the *Equipment/Facility Provisioning and Protection*, 323-2051-310.

8 Change the corresponding equipment of the pluggable module to be replaced to "Disabled".

Removing the pluggable from the module

9 Wear an antistatic wrist strap or foot straps to protect the shelf from static damage. If using a wrist strap, connect the wrist strap to the ESD jack on the shelf.

Copyright© 2019-2025 Ciena® Corporation

10 Disconnect the fiber-optic cable from the pluggable module.

You can use the LC fiber tool (174-0099-900) to install or remove LC fibers or to remove pluggable modules when space is restricted.

11 Remove the pluggable modules as follows:

- For the SFP pluggable modules, open the latch on the pluggable module by pressing the latch to the left.
- For OSC pluggable modules, pull down the latch to unseat the pluggable module.

12 Carefully pull the pluggable module out of its slot and install a protective dust cap on the module.

Inserting a replacement pluggable into the module

13 Remove the dust cap from the replacement pluggable module and make sure that connectors are properly cleaned. Refer to *Optical Connector Inspection and Cleaning*, 323-1859-500.

14 While holding the replacement pluggable module with the side where the electrical connections are exposed to your left, slide the pluggable module into the receptacle in the module faceplate. Ensure that the latch is closed (folded back in the pluggable module). An audible click indicates that the module is fully inserted.

15 Install the pluggable modules as follows:.

- For the SFP pluggable modules, close the latch on the pluggable module by pressing the latch to the right.
- For OSC pluggable modules, reseat the pluggable module and flip the latch up to lock it in place.

16 Reconnect the fiber-optic/cable you removed in step 10. Make sure that all fibers are properly cleaned before reconnection.

17 Change the equipment admin state of the pluggable module to “Enabled”. Refer to *Equipment/Facility Provisioning and Protection*, 323-2051-310.

18 Change the facility states to “Enabled” for all facilities on the pluggable module.

19 If applicable, return traffic to the module by releasing the protection switch that you performed in step 6.

20 Clear all alarms raised against the system. Refer to the alarm clearing procedures in this document.

Copyright© 2019-2025 Ciena® Corporation

Procedure 148 Replacing a shelf fan module

Use this procedure to replace a shelf fan module.

Requirements

To perform this procedure, you must:

- have a replacement shelf fan module for an RLS shelf. Review the “Ordering information” in *6500 RLS Planning Guide*, NTRN10WA to make sure you select the correct PEC as the replacement part for this product platform.
- have a Phillips or flathead screwdriver
- observe all safety requirements described in *6500 RLS Shelf* Installation Guide, 323-2051-201
- You have the appropriate personal grounding device to dissipate electrostatic charges

CAUTION
Risk of module failure
You must complete this procedure within 30 seconds to ensure that the modules equipped in the shelf do not overheat and fail while the fan module is being replaced. Never remove more than one fan module at the same time even if multiple fan modules require replacement. Have the replacement equipment ready before starting the procedure. Make sure to read and understand the entire procedure before starting.

CAUTION
Risk of equipment damage
Electrostatic discharge (ESD) can damage electrostatic sensitive devices. You must use antistatic protection while unpacking and installing all Field-Replaceable Units (FRU) and cables.

Overview

The following fan modules are supported:

- Shelf Fan Module (NTK807FA) for use in the R4 shelf
- Shelf Fan Module (NTK807DA) for use in the R2 shelf
- Shelf Fan Module (NTK507PA) for use in the R6-300 shelf
- Shelf Fan Module (NTK507QA) for use in the R8-300 shelf

RLS R2 and R4 shelves require two fan modules. Each shelf fan module contains two fans. In the event of a fan failure, the remaining fan will automatically adjust to compensate.

Copyright© 2019-2025 Ciena® Corporation

For additional fault-tolerance and power load balancing in RLS R2/R4 shelves, each pair of fans integrated into the fan modules is powered in a separate shelf power zone.

The individual fans integrated into the fan module are not field-replaceable and the entire shelf fan module must be replaced if one integrated fan fails.

The Rear Alarm LED on the Access Panel turns on if there is an alarm against the fan and/or PIM. If the LED is lit, determine the alarm(s) raised against the fan modules or PIMs and troubleshoot them accordingly (except “Software Auto-Upgrade in Progress” alarm).

Steps

1 Retrieve all the active alarms and alarm details:

If you want to perform the procedure using	**Then** go to the
CLI commands	“CLI INTERFACE STEPS”
Node Essentials	“NODE ESSENTIALS STEPS”

CLI INTERFACE STEPS

2 To retrieve all the active alarms and alarm details, enter:

```
show active-alarm <id> [name] [resource] [raise-time]
[raise-time] [cause] [condition-type] [direction]
[location] [severity] [service-impact] [additional-info]
[user-notes...]
```

The current alarms and alarm details will appear.

3 Go to step 5.

NODE ESSENTIALS STEPS

4 From the **Alarms** menu, select Current alarms.

The active alarm menu opens indicating the data for the active-alarm object.

5 Wear an antistatic wrist strap or foot straps to protect the shelf from static damage. If using a wrist strap, connect the wrist strap to the ESD jack on the shelf.

Copyright© 2019-2025 Ciena® Corporation

DANGER
Risk of personal injury
It can take up to 4 seconds for the fan blades to stop spinning after the fan module is disengaged from the backplane. During fan removal, the fan module will engage in a secondary stop position where a snap button will prevent the fan from being removed.

Do not attempt modify the equipment to defeat the snap button feature. You must leave the fan in this position for at least 4 seconds to ensure that it stops and never handle the fan in a manner that allows your hand or fingers to come in contact with the fan blades.

DANGER
Risk of eye injury
Wear eye protection such as safety goggles or safety glasses with side guards when you work with fan modules or in proximity to the shelf air exhaust.

Removing the fan module from the shelf

6 For the fan module in an R2 or R4 shelves, locate the fan module to be replaced in the back of the shelf. See Figure 32 on page 339 or Figure 33 on page 340.

7 If you are replacing the fan module in an R2 shelf, remove the fan module as follows:

a. using a Phillips screwdriver, unfasten the retention screw on the module

b. pull the fan module using the handle until the module is fully disengaged from the backplane

c. remove the fan module using the fan handle and place it in a safe location

d. Repeat the same steps to remove the second fan module from the CTM

8 If you are replacing the fan module in an R4 shelf, remove the fan module as follows:

a. Use a Phillips screwdriver to loosen the retaining thumbscrew on the module

b. Gripping the pull handle, carefully pull the fan module out of slot. Grip the fan using two hands, being careful not to allow hands or fingers near the fan blades. Remove the fan module from the shelf

9 If you are replacing the fan module in an R8-300 shelf, remove the fan module as follows:

a. Using a Phillips screwdriver, unfasten the retention screw that holds the fan module to the left wall. See Figure 35 on page 341.

b. Gripping the pull handle, carefully pull the fan module out of slot. Grip the fan using two hands, being careful not to allow hands or fingers near the fan blades. Remove the fan module from the shelf.

Copyright© 2019-2025 Ciena® Corporation

Installing the new shelf fan module

10 Firmly grip the replacement fan module, taking care not to touch the fan blades. Position the fan in front of the fan slot and slide the fan into the slot.

11 For the R2 shelf, push the plate between fans until the module is fully engaged with the backplane. Go to step 13.

12 For the R4 shelf, push the fan module using the handle or faceplate until the module is fully engaged with the backplane.

13 Use a Phillips screwdriver to fasten the retaining thumbscrew on the R4 shelf or the retention screw on the R2 shelf to a maximum torque of 5 lb-in. (0.56 N-m).

14 For the R8-300 shelf, fasten the fan module to the left wall using a Phillips screwdriver to a torque value between 0.45 N-m and 0.68 N-m (between 4 lb-in. and 6 lb-in.)

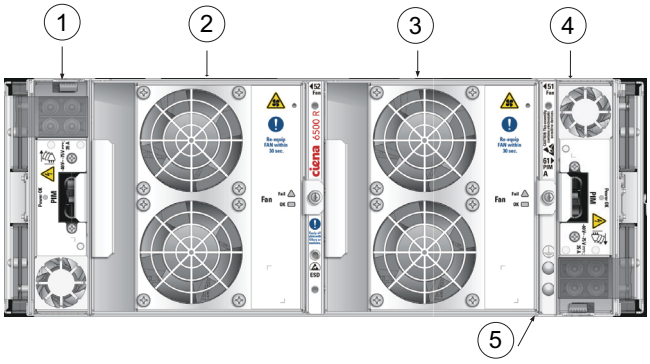
Confirming fan module operation

15 Ensure that the LED on the fan module is green and that the fan blades are operating by confirming that air is exhausting out the corresponding port on the rear of the shelf.

16 Clear all alarms raised against the system. Refer to the alarm clearing procedures in this document.

17 If an alarm does not clear, contact your next level of support or your Ciena support group.

Figure 32 RLS-R4 shelf fan module using DC PIMs

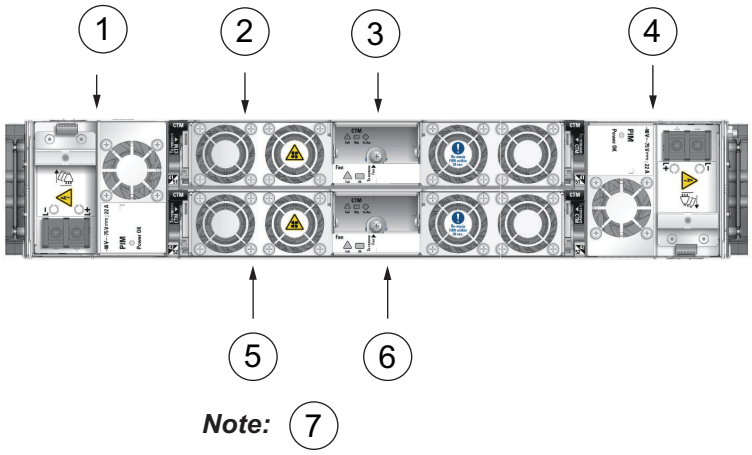


Legend

1	DC Power Input Module (PIM) (slot 62)	4	DC Power Input Module (PIM) (slot 61)
2	Shelf Fan Module (slot 52)	5	Shelf rear grounding point
3	Shelf Fan Module (slot 51)		

Copyright© 2019-2025 Ciena® Corporation

Figure 33 RLS-R2 shelf fan module using DC PIMs



Legend

1	DC Power Interface Module (PIM) (slot 62)	5	Shelf Fan Module (slot 52)
2	Shelf Fan Module (slot 51)	6	Control Timing Module (CTM) (slot 42)
3	Control Timing Module (CTM) (slot 41)	7	CTMs located behind Shelf Fan Modules.
4	DC Power Interface Module (PIM) (slot 61)		

Copyright© 2019-2025 Ciena® Corporation

Figure 34 RLS-R6-300 Shelf fan module (NTK507PA)

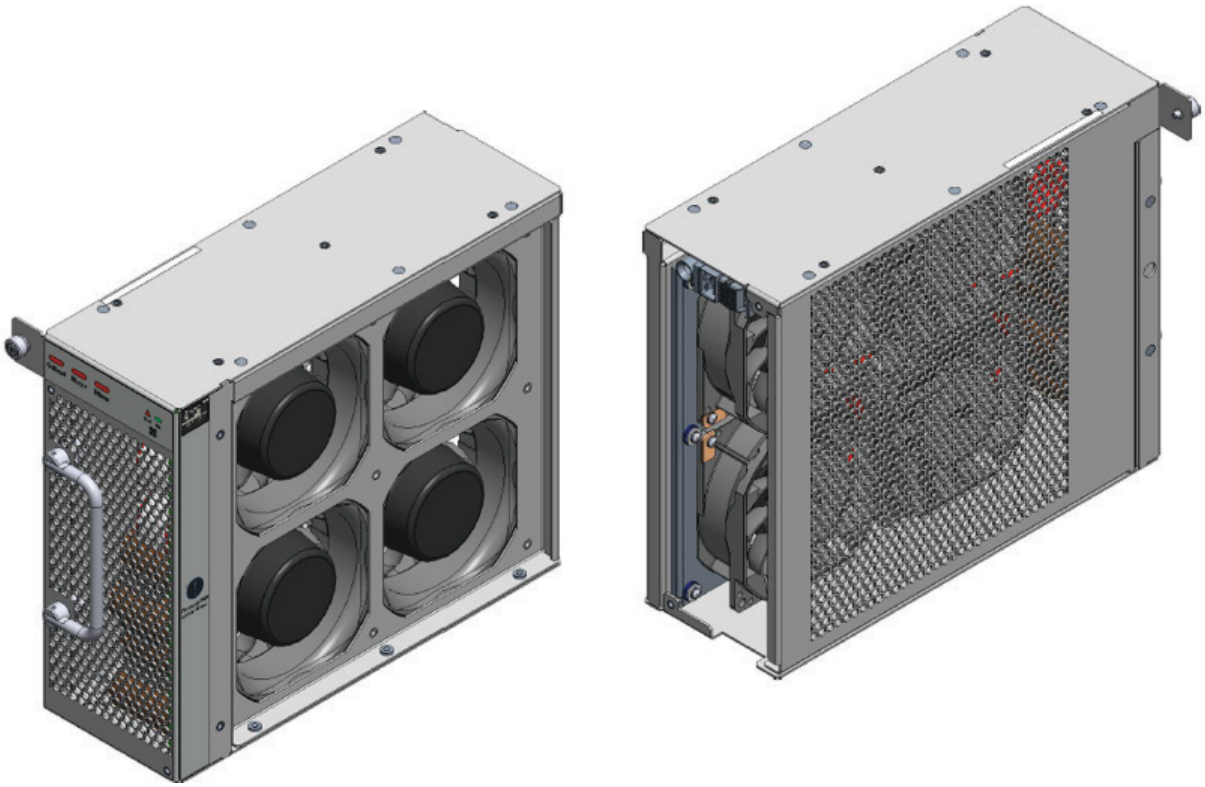
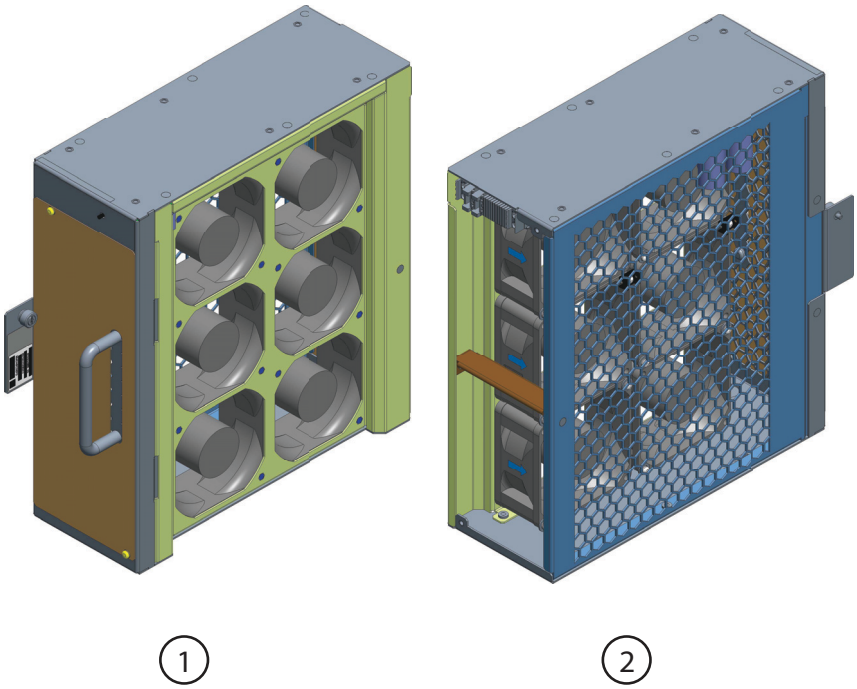


Figure 35 RLS-R8-300 shelf fan module



Copyright© 2019-2025 Ciena® Corporation

Legend

1	Fan Module (NTK507QA) - front view	2	Fan Module (NTK507QA) - rear view

Copyright© 2019-2025 Ciena® Corporation

Procedure 149 Replacing a shelf air filter in R2 or R4 shelf

Use this procedure to replace the shelf air filter in an R2 or R4 shelf.

Requirements

To perform this procedure, you must:

- have a replacement shelf air filter. Review the “Ordering information” in *6500 RLS Planning Guide*, NTRN10WA, to make sure you select the correct PEC as the replacement part for this product platform.
- have a Phillips screwdriver
- observe all safety requirements described in *6500 RLS Shelf Installation Guide*, 323-2051-201

CAUTION
Risk of equipment damage
Electrostatic discharge (ESD) can damage electrostatic sensitive devices. You must use antistatic protection while unpacking and installing all Field-Replaceable Units (FRU) and cables.

Overview

The following shelf air filters are supported:

- Shelf Air Filter (NTK807MF) for use in the R4 shelf.
- Shelf Air Filter (NTK807MD) for use in the R2 shelf.

The air filter is embedded within the shelf front cover. As a result, if air filtering is required, the shelf front cover is required. See examples of the shelf air filter at the end of this procedure. Use of the shelf front cover with air filter and side air blocking brushes is recommended for all applications and is required in Telcordia GR-63-CORE (NEBS) operating environments.

A working air filter must be equipped in order to help prevent dust and other airborne contaminants from entering the shelf enclosure. A blocked air filter will compromise the shelf cooling and could lead to the assertion of a “High Temperature Warning” alarm.

In controlled operating environments that are below the airborne contaminant levels listed in Telcordia GR-63-CORE (NEBS) and maintain an ambient temperature of 30°C or less, it is recommended that you inspect the air filter after 12 months of use and that you replace it if it has accumulated a layer of dust. You must discard and replace the air filter after 18 to 24 months of use. The recommended air filter replacement interval is six months when operating

Copyright© 2019-2025 Ciena® Corporation

in environments with higher ambient temperatures, with an unknown concentration of airborne contaminants or when the concentration is known to be in excess of Telcordia GR-63-CORE (NEBS) levels.

Steps

1 Retrieve all the active alarms and alarm details:

If you want to perform the procedure using	**Then** go to the
CLI commands	"CLI INTERFACE STEPS"
Node Essentials	"NODE ESSENTIALS STEPS"

CLI INTERFACE STEPS

2 To retrieve all the active alarms and alarm details, enter:

```
show active-alarm <id> [name] [resource] [raise-time]
[raise-time] [cause] [condition-type] [direction]
[location] [severity] [service-impact] [additional-info]
[user-notes...]
```

The current alarms and alarm details will appear.

3 Go to step 5.

NODE ESSENTIALS STEPS

4 From the **Alarms** menu, select Current alarms.

The active alarm menu opens indicating the data for the active-alarm object.

5 See the figures at the end of this procedure for an overview of the shelf air filter replacement for the R2 shelf and the R4 shelf.

DANGER
Risk of eye injury
Wear eye protection such as safety goggles or safety glasses with side guards when you work with fan modules, air filters or in proximity to the shelf air exhaust.

6 Wear an antistatic wrist strap or foot straps to protect the shelf from static damage. If using a wrist strap, connect the wrist strap to the ESD jack on the shelf.

7 Open the shelf front cover.

8 Detach the ground cable from the shelf front cover.

9 Remove the shelf front cover from the shelf.

10 Locate the Phillips screw on the bottom left of the filter frame. Using a Phillips screwdriver, unfasten the retention screw that secures the filter frame to the shelf front cover and holds the shelf air filters in place. Set the screw aside.

11 Slide the filter frame towards the left so that the standoff lines up with the opening of the keyholes and then lift the filter frame upwards to expose the filters.

Copyright© 2019-2025 Ciena® Corporation

12 Remove both air filters.

13 Insert the new air filters.

14 Place the filter frame over the air filters in the correct orientation. The numbers etched into the frame filter are up against the air filters.

15 Align the frame filter keyholes with the standoffs and slide the frame filter to the right to lock it into place.

16 Use a Phillips screwdriver to fasten the screw that secures the filter frame to the shelf front cover and holds the shelf air filters in place.

17 Attach the ground cable to the shelf front cover, and reinstall the shelf front cover to the shelf.

18 Close the shelf front cover.

19 Clear all alarms raised against the system. Refer to the alarm clearing procedures in the "Alarms" section in this document.

Figure 36 R2 shelf air filter—installed

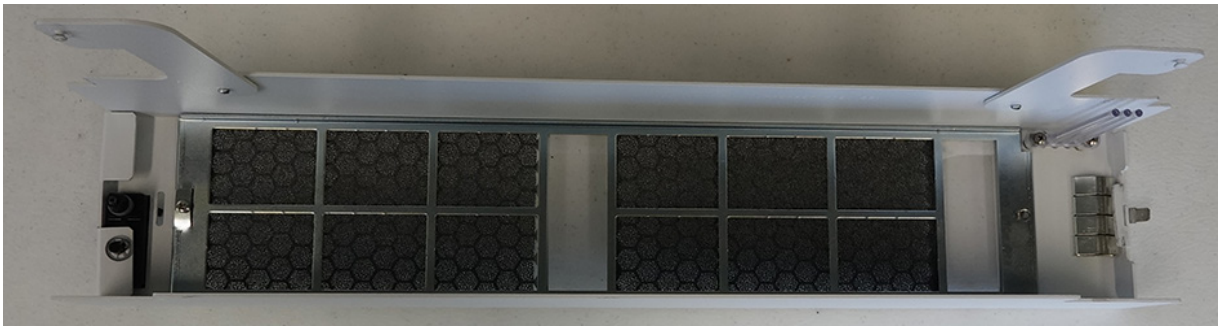


Figure 37 R2 shelf air filter—removing the filter frame

Copyright© 2019-2025 Ciena® Corporation

Figure 38 R2 shelf air filter—to replace

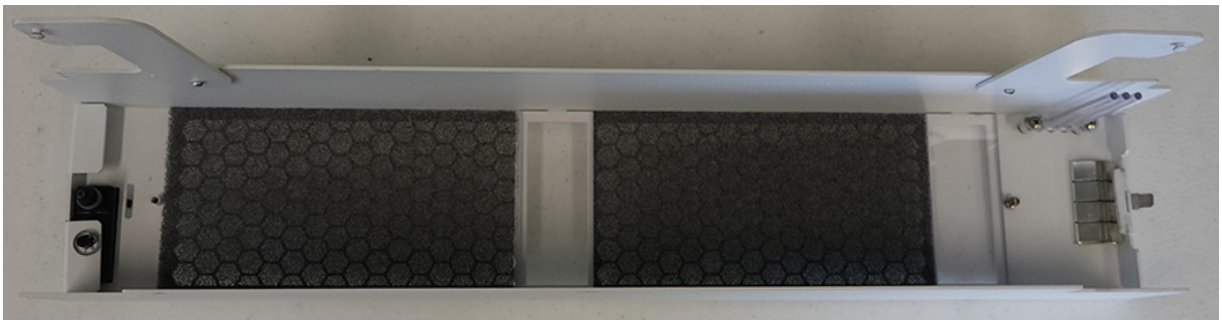
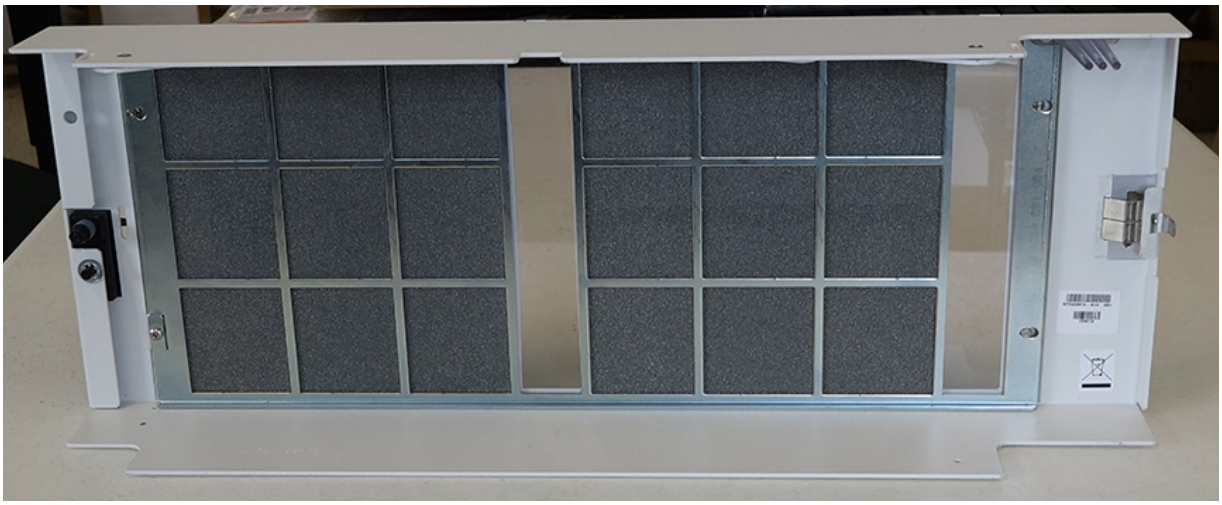


Figure 39 R2 shelf air filter—removed

Figure 40 R4 shelf air filter—installed



Copyright© 2019-2025 Ciena® Corporation

Figure 41 R4 shelf air filter—removing the filter frame

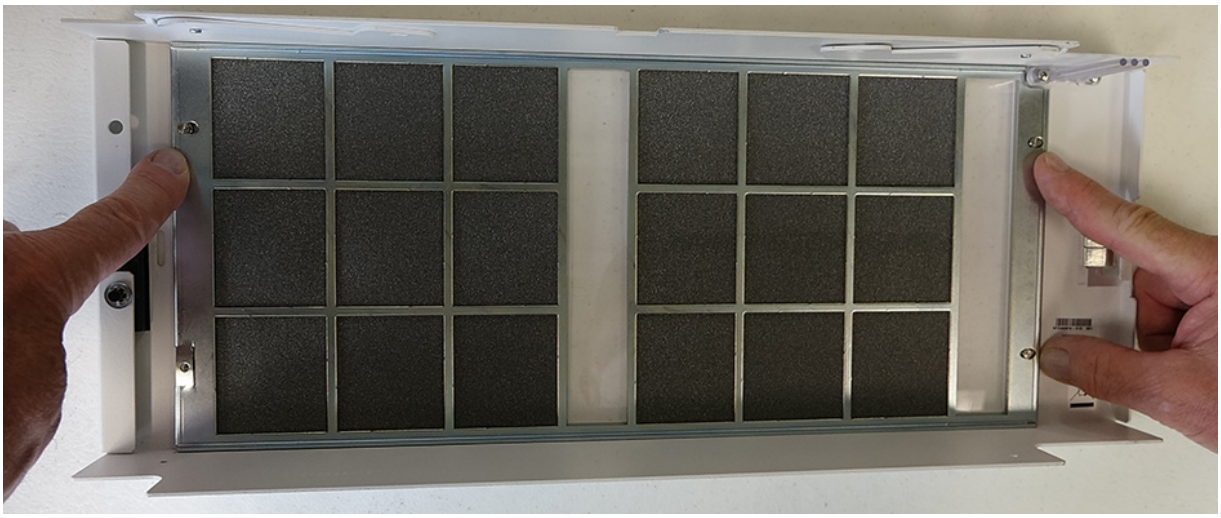
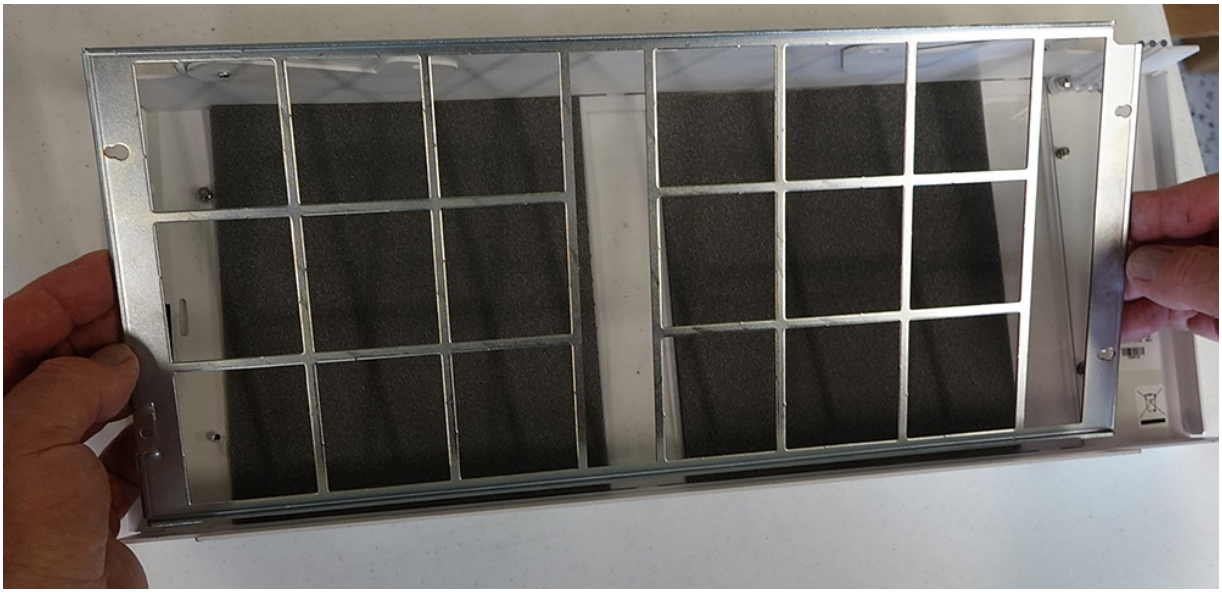
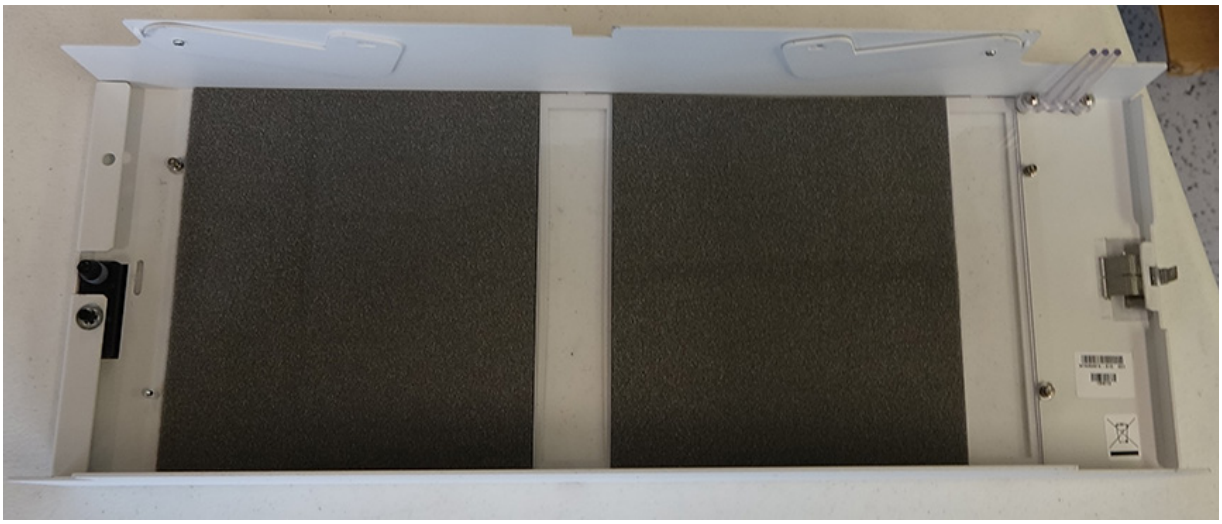


Figure 42 R4 shelf air filter—removing the filter frame



Copyright© 2019-2025 Ciena® Corporation

Figure 43 R4 shelf air filters—to remove



Copyright© 2019-2025 Ciena® Corporation

Procedure 150 Replacing a shelf air filter in an R6-300 or R8-300 shelf

Use this procedure to replace the shelf air filter (NTK807MP) in an R6-300 shelf or the shelf air filter (NTK509ER) in an R8-300 shelf.

Requirements

To perform this procedure, you must:

- have a replacement shelf air filter. Review the “Ordering information” in *6500 RLS Planning Guide*, NTRN10WA to make sure you select the correct PEC as the replacement part for this product platform.
- observe all safety requirements described in *6500 RLS Shelf Installation Guide,* 323-2051-201.

CAUTION
Risk of equipment damage
Electrostatic discharge (ESD) can damage electrostatic sensitive devices. You must use antistatic protection while unpacking and installing all Field-Replaceable Units (FRU) and cables.

Overview

The **R6-300 shelf or** R8-300 shelf assembly includes an air filter, which must be periodically replaced. A working air filter must be equipped to help prevent dust and other airborne contaminants from entering the shelf enclosure. A blocked air filter will compromise the shelf cooling and could lead to the assertion of a “High Temperature Warning” alarms.

A working air filter must be equipped in order to help prevent dust and other airborne contaminants from entering the shelf enclosure. A blocked air filter will compromise the shelf cooling and could lead to the assertion of a “High Temperature Warning” alarm.

Steps

1 Retrieve all the active alarms and alarm details:

If you want to perform the procedure using	**Then** go to the
CLI commands	“CLI INTERFACE STEPS”
Node Essentials	“NODE ESSENTIALS STEPS”

Copyright© 2019-2025 Ciena® Corporation

CLI INTERFACE STEPS

2 To retrieve all the active alarms and alarm details, enter:

```
show active-alarm <id> [name] [resource] [raise-time]
[raise-time] [cause] [condition-type] [direction]
[location] [severity] [service-impact] [additional-info]
[user-notes...]
```

The current alarms and alarm details will appear.

3 Go to step 5.

NODE ESSENTIALS STEPS

4 From the **Alarms** menu, select Current alarms.

The active alarm menu opens indicating the data for the active-alarm object.

5 Wear an antistatic wrist strap or foot straps to protect the shelf from static damage. If using a wrist strap, connect the wrist strap to the ESD jack on the shelf.

DANGER
Risk of eye injury
Wear eye protection such as safety goggles or safety glasses with side guards when you work with fan modules, air filters or in proximity to the shelf air exhaust.

6 Open the shelf front door (if equipped). Locate the shelf air filter on the right side of the shelf behind the fiber manager. Make sure that the D-shaped pull is perpendicular to the air filter. Grab the D-shaped pull with an index finger. Just to the right of the air filter location label, use your thumb to push inward against the front of the filter and then to the far right. This will push the air filter away from the hold-down tabs located at the top and bottom of the shelf.

7 Pull the old filter out of the shelf along the inside right face of the shelf using the D-shaped pull. Before inserting the replacement air filter, make sure that it is oriented in the correct direction. The D-shaped pull should be at the front and the air flow direction arrows on the side of filter frame should point to the left.

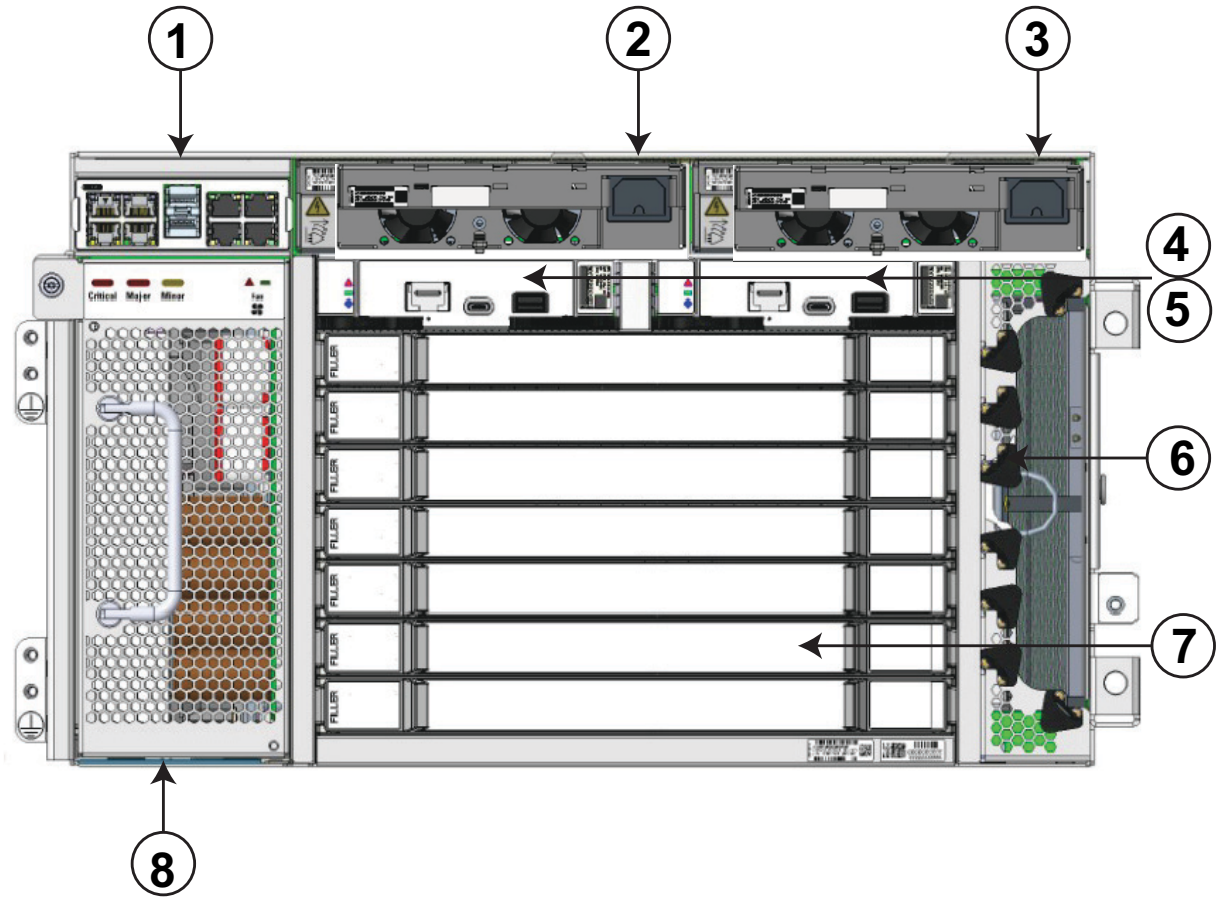
8 Insert the new replacement air filter until you feel a spring force. Press in and to the left to seat the filter past the hold-down tabs. See Figure 45.

9 Close the shelf front door (if equipped).

10 Clear all alarms raised against the system. Refer to the alarm clearing procedures in the “Alarms” section in this document.

Copyright© 2019-2025 Ciena® Corporation

Figure 44 R6-300 Shelf air filter location (number 6 in the figure below)

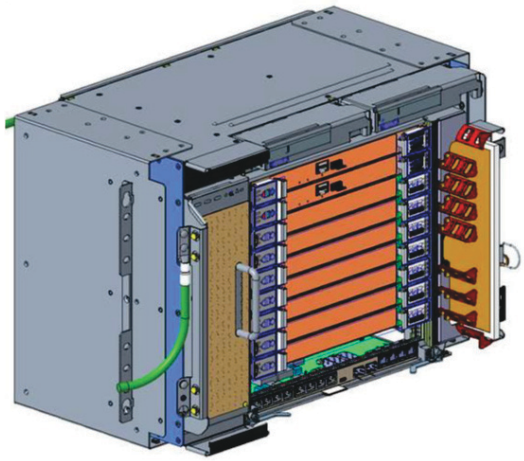


Legend

1	Access Panel (slot 40)	5	Control Timing Module (CTM-B) (slot 42)
2	DC Power Input Module (PIM A) (slot 61)	6	Fiber/Cable routing channel and air filter access port
3	DC Power Input Module (PIM B) (slot 62)	7	Interface Modules (IMs) (slots 1 to 7)
4	Control Timing Module (CTM-A) (slot 41)	8	Cooling Fan Module (slot 51)

Copyright© 2019-2025 Ciena® Corporation

Figure 45 R8-300 Shelf air filter



Copyright© 2019-2025 Ciena® Corporation

Procedure 151 Replacing a DC Power Input Module

Use this procedure to replace a DC Power Input Module (PIM).

Requirements

To perform this procedure, you must:

- have a replacement PIM. Review the “Ordering information” in *6500 RLS Planning Guide*, NTRN10WA to make sure you select the correct PEC as the replacement part for this product platform.
- observe all safety requirements described in *6500 RLS Shelf* Installation Guide, 323-2051-201
- have the following tools and material:
  - — digital voltmeter (DVM)
  - — Phillips screwdriver and torque flathead screwdrivers suitable for at least 2 N-m (18 lb-in.)
  - — antioxidant paste and a metric or imperial torque driver/socket set suitable for at least 3.4 N-m (30 lb-in.) (if working with lug-based power connections)

CAUTION
Risk of electrocution
Working with live circuits is dangerous. Before you continue, make sure that the shelf power is turned off at the power distribution panel and cannot be turned on by accident. Use a multimeter to verify that no potential exists.

Make sure that you have the appropriate personal grounding device to dissipate electrostatic charges.

CAUTION
Risk of equipment damage
Electrostatic discharge (ESD) can damage electrostatic sensitive devices. Use antistatic protection to avoid damaging modules.

Overview

The following power input modules are supported:

- DC Power Input Modules; PIM 22A (Breakerless Power Input Module) (NTK805DA)
- DC Power Input Modules; PIM 35A (Breakered Power Input Module) (NTK805FA)

Copyright© 2019-2025 Ciena® Corporation

- Power Input Module Type 2 (breakered) - 2-Wire D-Sub Input, Max 50A (NTK505QA)
- Power Input Module Type 2 (fused) - 2-wire D-Sub Input, Max 50A (NTK505QE)

For more information on power specifications, PIMs and power cables, refer to “Module descriptions, equipping rules, specifications” in *6500 RLS Planning Guide*, NTRN10WA.

Steps

1 Retrieve all the active alarms and alarm details:

If you want to perform the procedure using	**Then** go to the
CLI commands	“CLI INTERFACE STEPS”
Node Essentials	“NODE ESSENTIALS STEPS”

CLI INTERFACE STEPS

2 The following step is performed using CLI commands.

```
show active-alarm <id> [name] [resource] [raise-time]
[raise-time] [cause] [condition-type] [direction]
[location] [severity] [service-impact] [additional-info]
[user-notes...]
```

The current alarms and alarm details will appear.

3 Go to step 6.

NODE ESSENTIALS STEPS

4 The following steps are performed using Node Essentials.

Retrieving the active alarms

5 From the **Alarms** menu, select Current alarms.

The active alarm menu opens indicating the data for the active-alarm object.

6 Record the current state of the system.

7 Wear an appropriate ESD personal grounding device to dissipate electrostatic charges. If you are wearing an antistatic wrist strap, connect the cord to the ESD jack on the shelf installed and grounded in a grounded rack or clip to a suitable ground point.

8 If the shelf is currently “Enabled”, confirm that the cooling fan modules and equipped modules in the shelf are powered (green LEDs are on). See Figure 46 on page 357.

9 Locate the power to the PIM that is going to be replaced. Verify the modules affected by the replacement. Refer to “Shelf descriptions and technical specifications” in *6500 RLS Planning Guide*, NTRN10WA for information on the power configurations and affected modules.

Copyright© 2019-2025 Ciena® Corporation

10 Turn off the power of the PIM that is going to be replaced. Follow your company procedure for labeling and/or locking out each of the disconnected power sources in order to prevent any of the power sources from being re-energized before the procedure is completed.

CAUTION
Risk of traffic loss
If you are replacing a failed PIM and the Power failure alarm is already raised for the corresponding feed or feeds, the shelf may be operating without redundant power feeds. Special care should be taken when turning off the power at the source to ensure that the traffic is not impacted. You must ensure that one PIM remains equipped and is powered throughout the procedure.

11 Confirm that the green Power OK LED for the disconnected power feed is off.

A “Power Failure Fault” alarm should be raised against the affected PIM slot unless masked by another alarm such as “Circuit Pack Missing” or “Circuit Pack Unknown” against the slot.

12 Select your next step:

If the PIM you are replacing is	**Then** go to
breakered	step 13
breakerless	step 14
fused	step 16

13 Switch off the breaker(s) on the breakered PIM to be replaced.

14 Loosen the two screws (1/2 a turn each) on the plastic safety cover installed over the PIM wire connections.

15 Remove the plastic safety cover over the two screws of the PIM by sliding it to the left.

16 For the Power Input Card Type 2, 2-wire D-Sub (NTK505QA/NTK505QE), remove the tie wrap from the left and right routed 2W2 D-Sub power connectors.

17 Remove the nut/washer assembly and nut on each of the power cables.

18 Remove the DC power cable connectors from the port of the DC power input card.

19 Loosen the captive screws on the PIM to be replaced.

20 Remove the M4 screws and square washers from the power terminals of the PIM to be replaced.

21 Actuate the latch at the top of the R2 PIM before extracting the module.

22 Hold the PIM by the handle and pull on the PIM to disengage it from the backplane of the shelf.

Copyright© 2019-2025 Ciena® Corporation

Installing the replacement PIM into the shelf

23 Remove the plastic cover from the replacement PIM by loosening the two screws (1/2 a turn each) on the cover and sliding the plastic cover to the left and then outward.

24 On the breakerless PIMs, ensure the breakers feeding these circuits are all set to the OFF position.

25 On the breakered PIMs, ensure the breakers of the DC PIM are all set to the OFF position.

26 For the fused power input card (NTK505QE), if you are re-using the fuse from the replaced module, remove the fuse holder assembly from the replaced module using the optional fuse holder pull tool, inspect the fuse and install it in the replacement module. Refer to “Installing the Power Input Modules and connecting power cables” in *6500 RLS Shelf Installation Guide*, 323-2051-201 for information on removing, installing and choosing the correct type of fuse.

27 Hold the PIM by the handle and insert the PIM into the slot.

28 Press the PIM to fully engage it into the backplane.

Note: The NTK805FA PIM’s signal connector has flexibility of movement to allow for ease of connection to the backplane.

29 Hand tighten the captive screws on the PIM to the shelf pem nuts and then use a torque of 3 lbs-in. to complete securing the PIM to the shelf.

Installing the power cables

30 Connect the power cables as applicable. Refer to “Installing the Power Input Modules and connecting power cables” in 6500 RLS Shelf Installation Guide, 323-2051-201.

31 Reinstall the nut/washer assembly and nut on each of the power cables. Verify that the torque is 20 lb-in. (2.26 N-m) using a torque driver. (If required, lightly coat non-oxidizing compound on the terminals, two-hole lugs, and the contact surface of any jumpers.)

CAUTION
Risk of equipment damage and electrical shock
When routing power cables over metallic edges, wrap and secure an insulating sheet fiber (such as Nomex® or Formex™) around the power cables to protect them against damage and to prevent personal injury from electrical shock.

32 Reinstall the plastic safety cover over the two screws of each of the PIMs and slide the plastic cover to the right.

33 Secure the plastic covers into place by tightening the two screws (1/2 a turn each) if applicable.

34 Turn on the power source for the PIM you are replacing.

35 Turn on the breaker on the breakered DC PIM you are replacing.

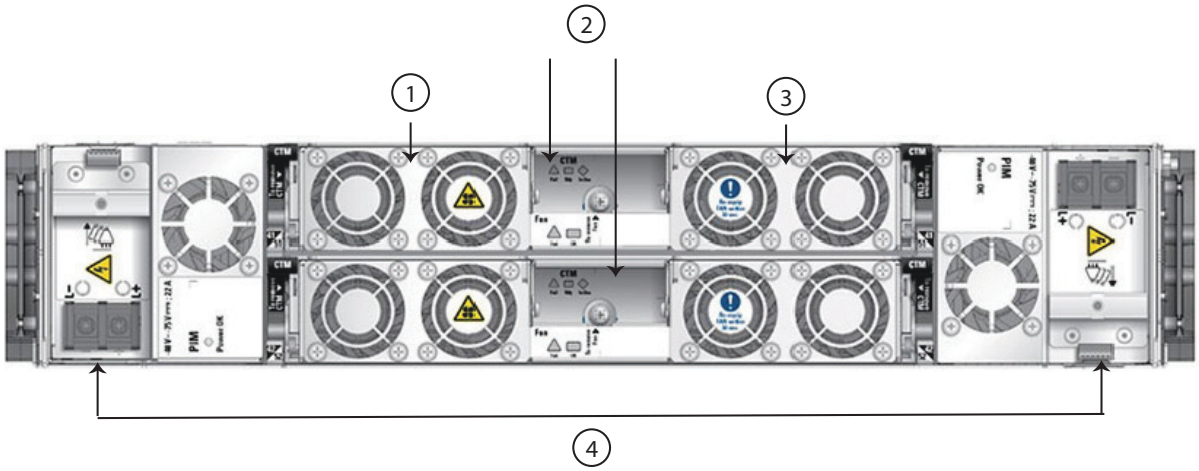
36 Check that the POWER OK LEDs on the PIM turn on.

Copyright© 2019-2025 Ciena® Corporation

If the LED does not turn on, possible causes are ground short-circuit or reverse polarity. You must power down the system, then remove the power cable before you troubleshoot further.

37 Clear all alarms raised against the system. Refer to the "Alarms" procedures in this document.

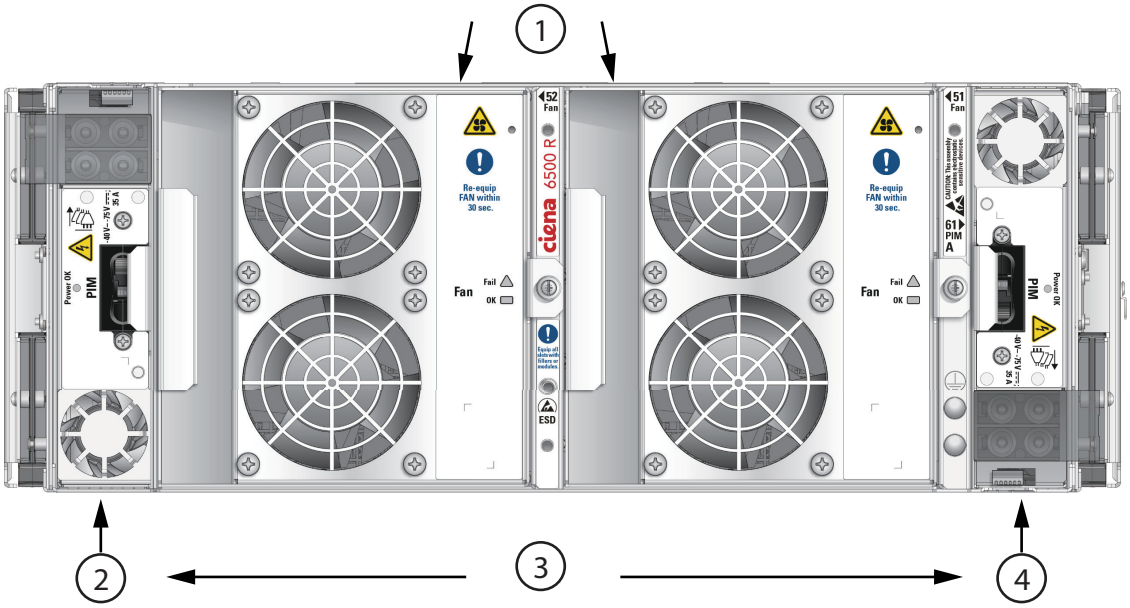
Figure 46 DC Power Input Modules; PIM 22A (Breakerless) (NTK805DA)



Legend

1	Shelf Fan Module (NTK807DA)	3	Shelf Fan Module (NTK807DA)
2	Control and Timing Modules (CTM) (NTK810DA/ NTK810DB)	4	Power Input Modules (NTK805DA)

Figure 47 DC Power Input Modules; PIM 35A (Breakered) (NTK805FA)



Copyright© 2019-2025 Ciena® Corporation

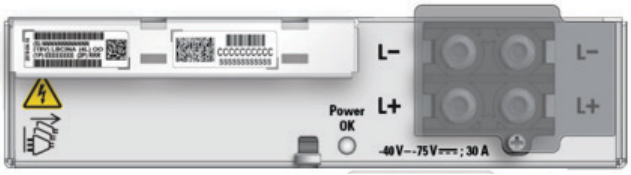
Legend

1	Shelf Fan Modules (NTK807FA)	3	DC Power Input Modules (PIM) breakered (NTK805FA)
2	PIM B (slot 62)	4	PIM A (slot 61)

Figure 48 Power Input Card Type 2 (breakered) (NTK505QA)

Figure 49 Power Input Card Type 2 (fused) (NTK505QE)

Figure 50 Power Input Card TYPE 2 (Breakerless PIM, MAX 30A) (NTK505UH)



Copyright© 2019-2025 Ciena® Corporation

Procedure 152 Replacing an AC Power Input Module

Use this procedure to replace a Power Input Module (PIM).

Requirements

To perform this procedure, you must

- have a replacement PIM. Review the “Ordering information” in *6500 RLS Planning Guide*, NTRN10WA to make sure you select the correct PEC as the replacement part for this product platform.
- have a Phillips or small flathead screwdriver
- have a torque driver
- observe all safety requirements described in *6500 RLS Shelf* Installation Guide, 323-2051-201

ATTENTION

All AC inputs to an AC-powered shelf or to any rectifier supplying DC power to a shelf must be equipped with an external Surge Protection Device (SPD not supplied) to meet the Telcordia criteria for lightning criteria for equipment interfacing with AC power port(s).

CAUTION

Risk of electrocution

Working with live circuits is dangerous. Before you continue, make sure that the shelf power is turned off at the power distribution panel and cannot be turned on by accident. Use a multimeter to verify that no potential exists.

Make sure that you have the appropriate personal grounding device to dissipate electrostatic charges.

CAUTION

Risk of equipment damage

Electrostatic discharge (ESD) can damage electrostatic sensitive devices. Use antistatic protection to avoid damaging modules.

Overview

The following power input modules are supported:

- AC Power Input Modules; PIM 100V-240V AC (NTK805SA)
- AC Power Input Modules; PIM 100V-240V AC (NTK805RA)
- AC Power Input Module; PIM 100-240V AC (NTK505UN)
- AC Type 3 Power Input Module PIM 100V-240V AC (NTK505RN)

Copyright© 2019-2025 Ciena® Corporation

For more information on power specifications, PIMs and power cables, refer to “Module descriptions, equipping rules, specifications” in *6500 RLS Planning Guide*, NTRN10WA.

Steps

1 Retrieve all the active alarms and alarm details:

If you want to perform the procedure using	**Then** go to the
CLI commands	“CLI INTERFACE STEPS”
Node Essentials	“NODE ESSENTIALS STEPS”

CLI INTERFACE STEPS

2 To retrieve all the active alarms and alarm details, enter:

```
show active-alarm <id> [name] [resource] [raise-time]
[raise-time] [cause] [condition-type] [direction]
[location] [severity] [service-impact] [additional-info]
[user-notes...]
```

The current alarms and alarm details will appear.

3 Go to step 5.

NODE ESSENTIALS STEPS

4 From the **Alarms** menu, select Current alarms.

The active alarm menu opens indicating the data for the active-alarm object.

5 Record the current state of the system.

6 Wear an appropriate ESD personal grounding device to dissipate electrostatic charges. If you are wearing an antistatic wrist strap, connect the cord to the ESD jack on the shelf installed and grounded in a grounded rack or clip to a suitable ground point.

7 If the shelf is currently “Enabled”, confirm that the cooling fan modules and equipped modules in the shelf are powered (green LEDs are on).

8 Locate the power to the PIM that is going to be replaced. Verify the modules affected by the replacement. Refer to “Shelf descriptions and technical specifications” in *6500 RLS Planning Guide*, NTRN10WA, for information on the power configurations and affected modules.

9 Optionally, turn off the power of the AC PIM that is going to be replaced or unplug the AC cable from the power source. Follow your company procedure for labeling and/or locking out each of the disconnected power sources in order to prevent any of the power sources from being re-energized before the procedure is completed.

Copyright© 2019-2025 Ciena® Corporation

CAUTION
Risk of traffic loss
If you are replacing a failed PIM and the Power failure alarm is already raised for the corresponding feed or feeds, the shelf may be operating without redundant power feeds. Special care should be taken when turning off the power at the source to ensure that the traffic is not impacted. You must ensure that one PIM remains equipped and is powered throughout the procedure.

10 Remove the AC power cables from the PIM to be replaced.

11 Confirm that the green Power OK LED for the PIM with the disconnected power feed is off. A “Power Failure Fault” alarm should be raised against the affected PIM slot unless masked by another alarm such as “Circuit Pack Missing” or “Circuit Pack Unknown” against the slot.

12 For the NTK505RNor NTK505UN AC PIM, loosen the captive screw with a Phillips or flathead screwdriver.

13 For the R2/R4/R6 shelves, unlatch the AC PIM from the shelf.

14 Hold the PIM by the handle and pull on the PIM to disengage it from the backplane of the shelf.

Installing the replacement PIM into the shelf

15 Hold the PIM by the handle and insert the PIM into the slot in the same orientation as the one that was removed.

16 Push the handles toward the back of the shelf until it is fully engaged into the backplane.

Note: The NTK805RA PIM’s signal connector has flexibility of movement to allow for ease of connection to the backplane. Refer to “Installing the Power Input Modules and connecting power cables” in 6500 RLS Shelf Installation Guide, 323-2051-201.

17 If you are installing an NTK505RN AC PIM into an R8-300 shelf, or NTK505UN AC PIM into an R6-300 shelf, insert the PIM into the shelf, and latch the PIM.

CAUTION
Risk of power brownout
Make sure the power input cards are fully seated and secured before applying power. When applying power, the Power OK LED will be activated even if the power input card is not fully seated.

Installing the power cables

18 Connect the power cables as applicable. Refer to “Installing the Power Input Modules and connecting power cables” in 6500 RLS Shelf Installation Guide, 323-2051-201.

Copyright© 2019-2025 Ciena® Corporation

19 Make sure that the other end of the AC cord for the PIM that you are replacing is plugged into the power source and that the power is turned on.

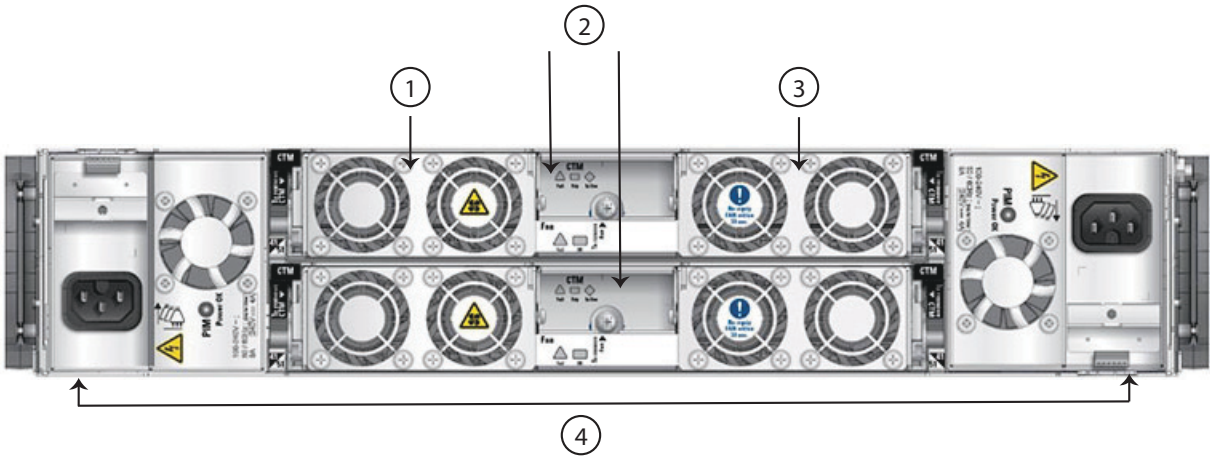
20 Check that the POWER OK LEDs on the PIM turn on.

If the LED does not turn on, possible causes are no power at the source or a faulty AC cable assembly. You must power down the system, then remove the power cable before you troubleshoot further.

21 Clear all alarms raised against the system. Refer to the "Alarms" procedures in this document.

22 Ensure there are no active alarms against the newly installed module(s).

Figure 51 AC Power Input Modules; PIM 100V-240V AC (NTK805SA)

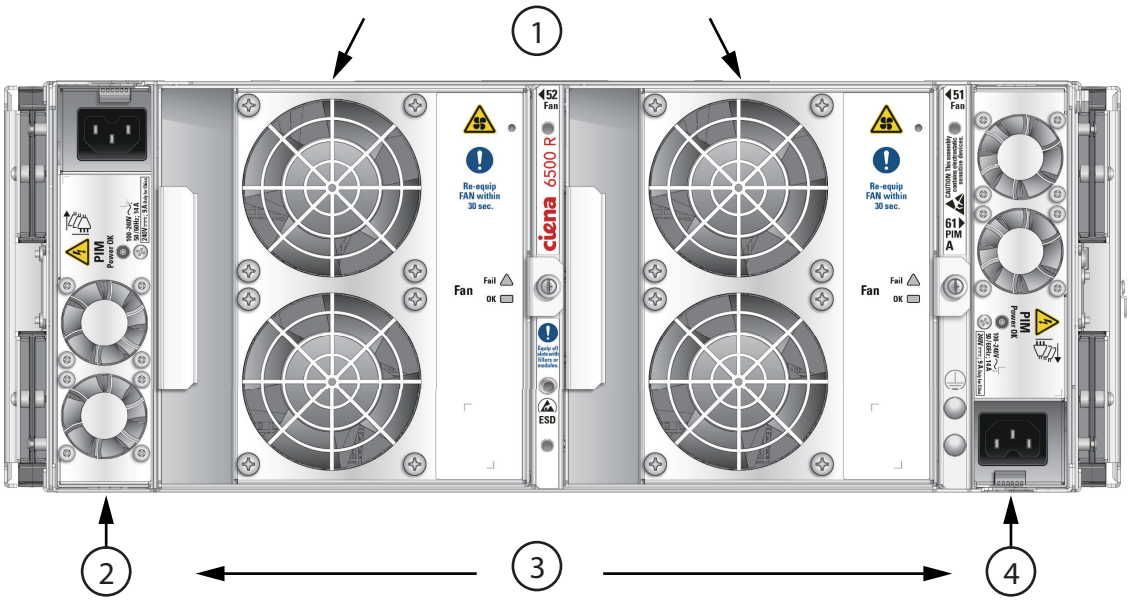


Legend

1	Shelf Fan Module (NTK807DA)	3	Shelf Fan Module (NTK807DA)
2	Control and Timing Modules (CTM)(NTK810DA/NTK810DB)	4	Power Input Modules (NTK805SA)

Copyright© 2019-2025 Ciena® Corporation

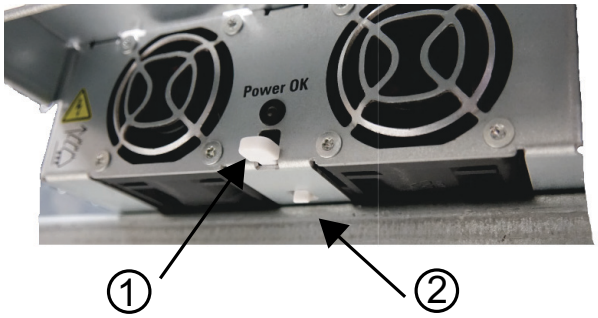
Figure 52 AC Power Input Modules; PIM 100V-240V AC (NTK805RA)



Legend

1	Shelf Fan Modules (NTK807FA)	3	AC Power Input Modules (PIM) (NTK805RA)
1	PIM B (slot 62)	4	PIM A (slot 61)

Figure 53 AC Power Input Card (100-240 V AC PIM) (NTK505UN)



Legend

1 latch

2 tab

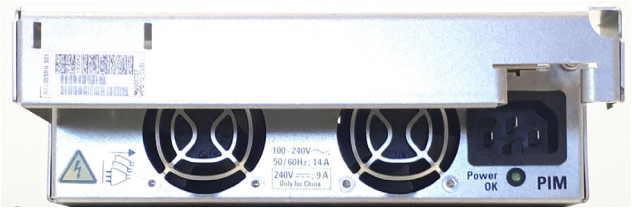
To install, push the power input card (AC or DC) into its slot. As you do so, the spring-loaded latch moves down. The power input card is inserted correctly when the latch is down and the tab engages with the hole in the shelf. You will hear a click.

Copyright© 2019-2025 Ciena® Corporation

(This example shows an AC Power Input Card being installed. When a power input card is fully inserted, the tab will no longer be visible: it will be engaged with the hole in the shelf.)

Note: This same latch and tab mechanism applies to the DC Power Input Card (NTK505UH).

Figure 54 AC Power Input Card Type 3 (100-240V AC PIM) (NTK505RN)



Copyright© 2019-2025 Ciena® Corporation

Procedure 153 Replacing a DLM, TLM C-Band module

Use this procedure to replace the DLM C-Band 2xSFP module (Dual Line Monitor), TLM C-Band 1xSFP Module (Terminal Line Monitor) modules:

Requirements

- observe all safety requirements described in *6500 RLS Shelf* Installation Guide, 323-2051-201
- have the correct replacement module (the replacement Product Engineering Code [PEC] is the same as the current PEC)
- have protective caps for the patchcords

CAUTION
Risk of equipment damage
Electrostatic discharge (ESD) can damage electrostatic sensitive devices. You must use antistatic protection while unpacking and installing all Field-Replaceable Units (FRU) and cables.

Overview

CAUTION
Service affecting procedure
Amplifier replacement is service affecting. Ensure you have exhausted all other troubleshooting options before performing this procedure and if possible, re-route the traffic to minimize the traffic loss.

You can perform this procedure while Device Controller “Enabled”. However, Device Controller will raise some alarms at the Device Controller network element. (for details on alarms, see Alarm Clearing section in this document. These alarms occur because Device Controller detects changes in the system topology. To ensure correct operation, Device Controller only attempts equalization when the system topology is stable and determined to be accurate. To avoid the alarm generation, set the Device Controller to “Disabled” at the beginning of this procedure. Make sure to return the Device Controller state to “Enabled”, as indicated at the end of this procedure.

Steps

1 Check the date and time of the last backup and check whether a data backup is required.

Copyright© 2019-2025 Ciena® Corporation

2 Set all Device Controller within this domain to “Disabled”. Refer to *Equipment/ Facility Provisioning and Protection*, 323-2051-310.

Note: Device Controller(s) managing other domains will not be able to optimize or add/delete channels traversing the domain whose Device Controller is in a “Disabled” state.

3 Verify the current alarm conditions on the network element. Depending on the configuration of the node where this procedure is to be performed the following alarms can appear throughout the network during this procedure:

- Automatic Power Reduction Active
- Automatic Shutoff
- Circuit Pack Missing
- Shutoff Threshold Crossed

4 Verify that the replacement Product Engineering Code (PEC) is the same as the current PEC.

Removing the module

5 Switch traffic away from this optical link by performing a protection switch at the service layer to prevent traffic loss. Refer to *Equipment/Facility Provisioning and Protection*, 323-2051-310 section in this document.

6 Wear an antistatic wrist strap to protect the equipment from static damage. Connect the wrist strap to the ESD jack on the shelf or module.

CAUTION
Risk of laser radiation exposure
Do not look directly into the optical beam. Invisible light can severely damage your eyes.

CAUTION
Risk of damage to modules
Never disconnect an optical fiber that is connected to an active or powered up optical amplifier. To disconnect or reconnect an optical fiber, make sure the optical amplifier is “Disabled”.

7 Remove the amplifier facilities connected to the module being replaced from service. Refer to *Equipment/Facility Provisioning and Protection*, 323-2051-310 for information on removing optical facilities from service.

8 Ensure that labels are applied to both ends of all cables and optical fiber patchcords.

9 Disconnect all connectors from the DLM or TLM module. See Figure 55 on page 369 or Figure 62 on page 375.

10 Put protective caps on the ends of the patchcords to protect them from contamination and damage.

11 Make sure that the blue LED on the module faceplate is off. If the blue LED is on, do not pull out the module.

Copyright© 2019-2025 Ciena® Corporation

12 Pull and hold the locks to unlock the latches.

13 Pull the lock/eject latches of the module faceplate to their completely extended positions.

The module connector disengages from the backplane.

14 Pull the module out of the slot.

Installing the module

15 Lift the replacement module by the edges of the faceplate.

16 Carefully guide the back end of the module into the required slot, while making sure that the edges of the module enter the slot guide rails.

17 Push the module into the shelf until 75% of the length of the module is in the shelf.

18 Pull the lock/eject latches of the replacement module faceplate to their completely extended positions.

19 Push the module towards the back of the shelf until it engages with the backplane and then push on the faceplate to partially seat it. At this time, the lock/eject latches will slip into the grooves at the top and bottom edges of the slot rack.

20 Push the lock/eject latches towards the module faceplate. Make sure that the locks are back to their place when the latches snap into the locked position.

Do not use excessive force when pushing the lock/eject latches towards the faceplates. If the latches do not lock into place, remove the module and examine the connector at the back of the module. Look for bent pins or damage.

21 You can retrieve the inventory data for the module you inserted.

If you want to perform the procedure using	**Then** go to the
CLI commands	“CLI INTERFACE STEPS”
Node Essentials	“NODE ESSENTIALS STEPS”

CLI INTERFACE STEPS

22 To rretrieve the inventory data for the module, enter:.

```
show slots <name> inventory circuit-pack
```

23 Go to step 25.

NODE ESSENTIALS STEPS

24 Click on the **Chassis** menu and select the module you want to retrieve the inventory for.

The inventory information appears on the right side of the screen.

25 Clean all connectors disconnected from the module in step 9 and reconnect them to the appropriate ports on the replacement module. For instructions on inspecting and cleaning optical fiber, refer to *Optical Connector Inspection and Cleaning*, 323-1859-500.

26 Wait for the software initialization to complete.

Copyright© 2019-2025 Ciena® Corporation

Software download and initialization can take up to five minutes and is complete when the green status LED stops flashing and the green Ready LED turns on.

27 If the auto-equipping feature is turned on or if the equipment is already provisioned for the respective slot, the module is “Enabled” and the blue LED turns on after the green LED.

When the green LED is steadily lit (after the software initialization), an auto-upgrade of the module may occur. During an auto-upgrade, the green LED remains steadily lit and the blue LED remains off (a Software Auto-Upgrade in progress alarm is raised and clears after the auto-upgrade is complete).

Do not remove the module if the green LED is flashing, if the blue LED is on, or if the module is auto-upgrading (check for the Software Auto-Upgrade in progress alarm).

28 Wait for the module to start.

29 Restore the amplifier facilities connected to the new module back to “Enabled”. Refer to *Equipment/Facility Provisioning and Protection*, 323-2051-310 section in this document for information on restoring facilities to service.

30 Retrieve all the active alarms and alarm details:

If you want to perform the procedure using	**Then** go to the
CLI commands	“CLI INTERFACE STEPS”
Node Essentials	“NODE ESSENTIALS STEPS”

CLI INTERFACE STEPS

31 The following step is performed using CLI commands.

```
show active-alarm <id> [name] [resource] [raise-time]
[raise-time] [cause] [condition-type] [direction]
[location] [severity] [service-impact] [additional-info]
[user-notes...]
```

The current alarms and alarm details will appear.

32 Go to step 35.

NODE ESSENTIALS STEPS

33 The following steps are performed using Node Essentials.

Retrieving the active alarms

34 From the **Alarms** menu, select Current alarms.

The active alarm menu opens indicating the data for the active-alarm object.

35 If the “Software Auto-Upgrade in Progress” alarm is active, wait until the alarm clears before continuing.

Note: It can take up to 15 minutes for this alarm to clear.

36 If “Autoprovisioning Mismatch” alarm is active, a problem with provisioning the module has been detected. Refer to the “Alarms” section in this document.

Copyright© 2019-2025 Ciena® Corporation

37 Undo any traffic switches performed in step 5.

38 Put both Device Controllers back to “Enabled”. Performing a manual re-optimization of both Device Controllers is recommended. Refer to *Equipment/ Facility Provisioning and Protection*, 323-2051-310.

39 Update the user label with the current shelf and slot number.

40 Ensure there are no active alarms against the newly installed module(s).

Figure 55 DLM C-Band 2xSFP module

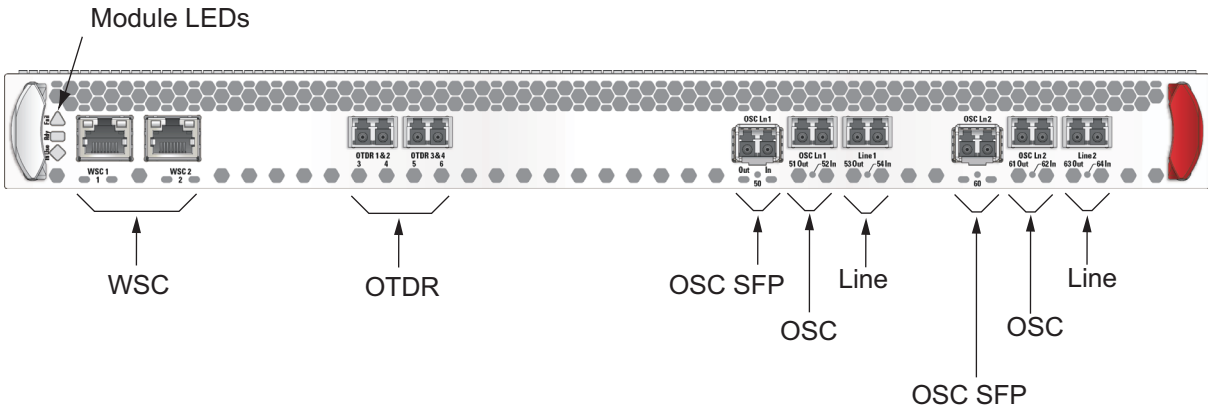
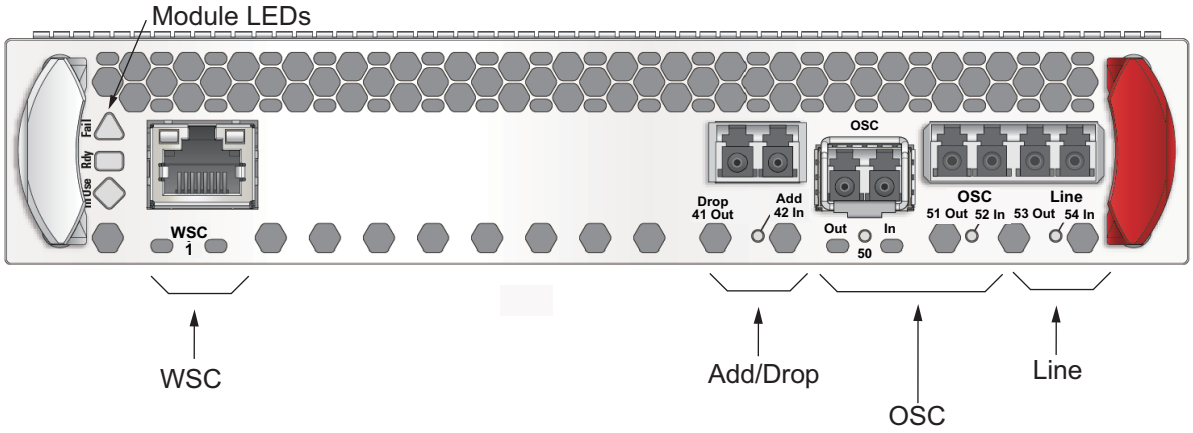


Figure 56 TLM C-Band 1xSFP module



Copyright© 2019-2025 Ciena® Corporation

Procedure 154 Replacing a CMD, CCMD, or SSM module

Requirements

To perform this procedure, you must:

- observe all safety requirements described in *6500 RLS Shelf* Installation Guide, 323-2051-201
- have the correct replacement module (the replacement Product Engineering Code [PEC] is the same as the current PEC)
- have protective caps for the patchcords

CAUTION
Risk of equipment damage
Electrostatic discharge (ESD) can damage electrostatic sensitive devices. You must use antistatic protection while unpacking and installing all Field-Replaceable Units (FRU) and cables.

Overview

Use this procedure to replace one of the following modules:

- CMD24 200 GHz C-Band Module (CMD24 200GHz C-Band) (NTT862QA)
- CMD32 150 GHz C-Band module (NTT862PA)
- CMD32 150 GHz C-Band Type 2 module (NTT862PB)
- CMD42 C-Band module (NTT862NA)
- CMD48 100 GHz C-Band module (NTT862MA)
- CMD64 75 GHz C-Band module (NTT862JA)
- CMD64 75 GHz Type 2 C-Band module (NTT862JB)
- CCMD 8x24 C-Band module (NTK843BA)
- CCMD 8x24 L-Band module (NTK843BE)
- CCMD16 C-Band module (NTT834AA)
- CCMD16 L-Band module (NTT834AE)
- CCMD16 C-Band Module (16-Channel Colorless Mux/Demux, RLS-300) (CCMD16) (NTK874AA)
- CCMD 16x24 C-Band module (NTK843AA)
- CCMD 16x24 L-Band module (NTK843AE)
- SSM C-Band Module (Shared Spectrum Monitor) (NTK835NA)

Copyright© 2019-2025 Ciena® Corporation

See Figure 58 on page 375

Figure 60 on page 375, Figure 61 on page 375, Figure 62 on page 375, Figure 63 on page 376, Figure 64 on page 376,Figure 65 on page 376, Figure 66 on page 376, Figure 67 on page 377, or Figure 68 on page 377.

CAUTION
Service affecting procedure
Module replacement is service affecting. Ensure you have exhausted all other troubleshooting options before performing this procedure and if possible, re-route the traffic to minimize the traffic loss.

Steps

Removing the module

1. Check the date and time of the last backup and check whether a data backup is required. Refer to *Licensing, Security, and Administration*, 323-2051-300 for details on how to view the current backup state and how to save provisioning data.
2. Provision the admin state of the module to “Disabled”.

If you want to perform the procedure using	**Then** go to the
CLI commands	“CLI INTERFACE STEPS”
Node Essentials	“NODE ESSENTIALS STEPS”

CLI INTERFACE STEPS

3. The following step is performed using CLI commands.

```
set slots <slot #> config circuit-pack admin-state
<Disabled>
```

4. Go to step 10.

NODE ESSENTIALS STEPS

5. Select **Facilities** from the Node Essentials navigation menu.

   The Facilities menu opens.
6. From the **Equipment** grid, select the module to be replaced.
7. Click the **Pencil** icon (Edit Equipment).
8. Set the Admin state of the equipment to Disabled
9. Click **Confirm**.

Copyright© 2019-2025 Ciena® Corporation

10 Verify the current alarm conditions on the network element. Depending on the configuration of the node where this procedure is to be performed, the following alarms can appear throughout the network during this procedure:

- Automatic Power Reduction Active
- Automatic Shutoff
- Circuit Pack Missing
- Shutoff Threshold Crossed
- Loss Of Signal
- Connection Validation Data Missing

11 Verify that the replacement Product Engineering Code (PEC) is the same as the current PEC.

12

CAUTION
Risk of laser radiation exposure
Do not look directly into the optical beam. Invisible light can severely damage your eyes.

CAUTION
Risk of damage to modules
Never disconnect an optical fiber that is connected to an active or powered up optical amplifier. To disconnect or reconnect an optical fiber, make sure the optical amplifier is “Disabled”.

CAUTION
Risk of damage to modules
Wear an antistatic wrist strap to protect the equipment from static damage. Connect the wrist strap to the ESD jack on the shelf or module.

Ensure that labels are applied to both ends of all cables and optical fiber patchcords.

13 Disconnect all optical connectors from the module to be replaced.

14 Put protective caps on the ends of the patchcords to protect them from contamination and damage.

15 Unseat and remove the module from the slot.

16 Gently pull the module until it is fully removed from the shelf.

Installing the module

17 Install the replacement module into the corresponding slot and press the latches to close. For complete equipping rules and module slot numbering, refer to “Module descriptions, equipping rules, specifications” in *6500 RLS Planning Guide*, NTRN10WA.

Copyright© 2019-2025 Ciena® Corporation

Note: Some modules such as CMD42 have a sliding feature. You can slide the module towards the front of the rack and secure it in a position that provides easier access for connecting and disconnecting fiber cables. To achieve this, pull out the plunger on the right-hand side of the CMD chassis, pull the chassis toward the front of the rack, and release the plunger to secure the chassis in the frontmost position.

18 Wait for the module to start.

Note: While the module is removed or rebooting, the lost channels are replaced with ASE. After recovery, the channel controller re-evaluates relevant in/out profile deltas and re-adjusts WSS attenuation accordingly for traffic channels.

19 You can retrieve the inventory data for the module you inserted.

If you want to perform the procedure using	**Then** go to the
CLI commands	"CLI INTERFACE STEPS"
Node Essentials	"NODE ESSENTIALS STEPS"

CLI INTERFACE STEPS

20 The following step is performed using CLI commands.

```
show slots <name> inventory circuit-pack
```

21 Go to step 24.

NODE ESSENTIALS STEPS

22 Click on the **Chassis** menu and select the module you want to retrieve the inventory for.

The inventory information appears on the right side of the screen.

23 Wait until the upgrade is complete and the upgrade-operation-state of the CCMD8x24 is "idle". Run the following command:

```
show software component <affected IM slot number>
```

24 Provision the admin state of the module to "Enabled".

If you want to perform the procedure using	**Then** go to the
CLI commands	"CLI INTERFACE STEPS"
Node Essentials	"NODE ESSENTIALS STEPS"

CLI INTERFACE STEPS

25 The following step is performed using CLI commands.

```
set slots <slot #> config circuit-pack admin-state
<Enabled>
```

26 Go to step 32.

NODE ESSENTIALS STEPS

27 Select **Facilities** from the Node Essentials navigation menu.

The Facilities menu opens.

Copyright© 2019-2025 Ciena® Corporation

28 From the **Equipment** grid, select the module to be replaced.

29 Click the **Pencil** icon (Edit Equipment).

30 Set the Admin state of the equipment to Enabled

31 Click **Confirm**.

32 Clean all fiber connectors disconnected from the ports in step 13 and reconnect them to the appropriate ports on the module. For instructions on inspecting and cleaning optical fiber, refer to *Optical Connector Inspection and Cleaning*, 323-1859-500.

33 Retrieve all the active alarms and alarm details:

If you want to perform the procedure using	**Then** go to the
CLI commands	"CLI INTERFACE STEPS"
Node Essentials	"NODE ESSENTIALS STEPS"

CLI INTERFACE STEPS

34 The following step is performed using CLI commands.

```
show active-alarm <id> [name] [resource] [raise-time]
[raise-time] [cause] [condition-type] [direction]
[location] [severity] [service-impact] [additional-info]
[user-notes...]
```

The current alarms and alarm details will appear.

35 Go to step 38.

NODE ESSENTIALS STEPS

36 The following steps are performed using Node Essentials.

Retrieving the active alarms

37 From the **Alarms** menu, select Current alarms.

The active alarm menu opens indicating the data for the active-alarm object.

38 If the "Software Auto-Upgrade in Progress" alarm is active, wait until the alarm clears before continuing.

Note: It can take up to 15 minutes for this alarm to clear.

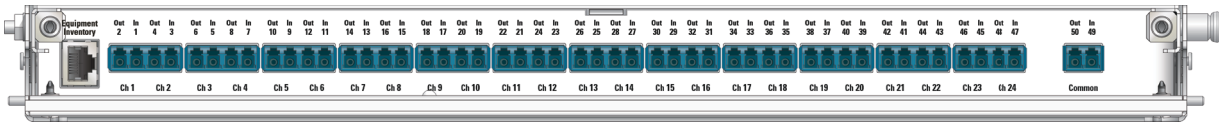
39 If "Autoprovisioning Mismatch" alarm is active, a problem with provisioning the module has been detected.

40 Check and clean fibers if there are "Loss Of Signal" alarms active.

Note: "Connection Validation Data Missing" alarms might take up to 60 minutes to clear.

41 Ensure there are no active alarms against the newly installed module(s).

Figure 57 CMD24 200 GHz C-Band module



Copyright© 2019-2025 Ciena® Corporation

Figure 58 CMD32 C-Band module

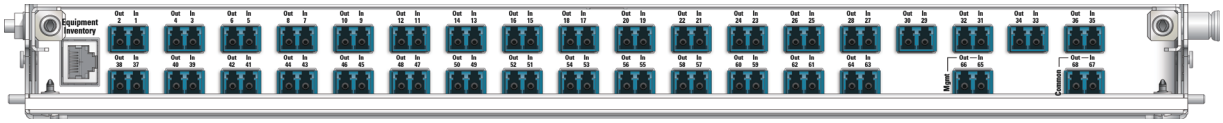


Figure 59 CMD32 Type 2 C-Band module

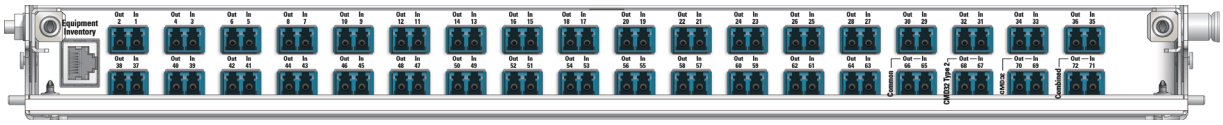


Figure 60 CMD42 C-Band module

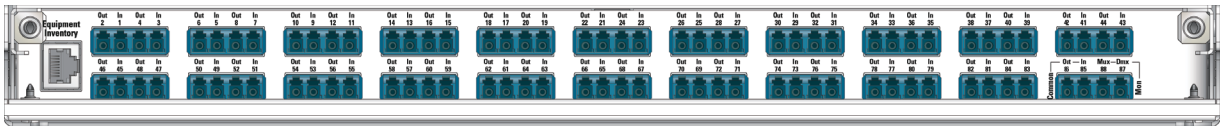


Figure 61 CMD48 C-Band module

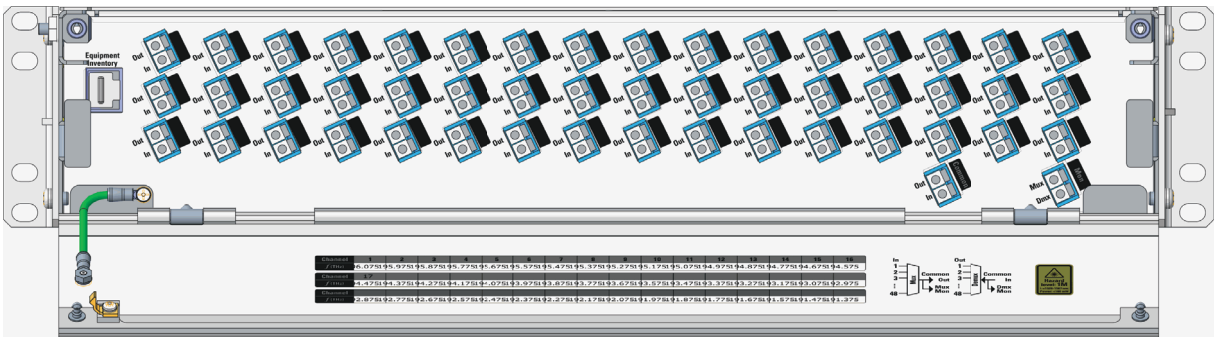
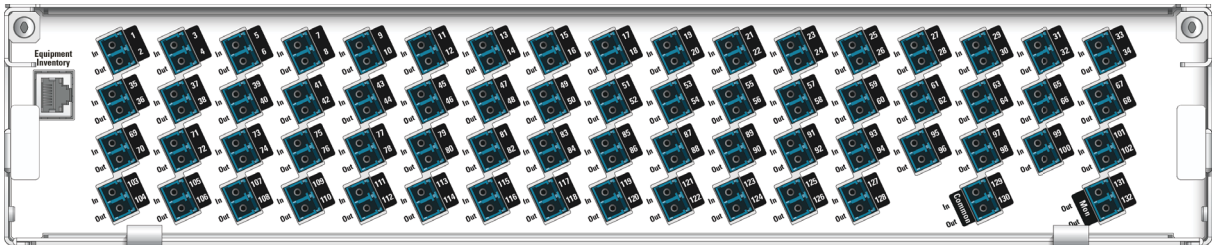


Figure 62 CMD64 C-Band module



Copyright© 2019-2025 Ciena® Corporation

Figure 63 CMD64 Type 2 C-Band module

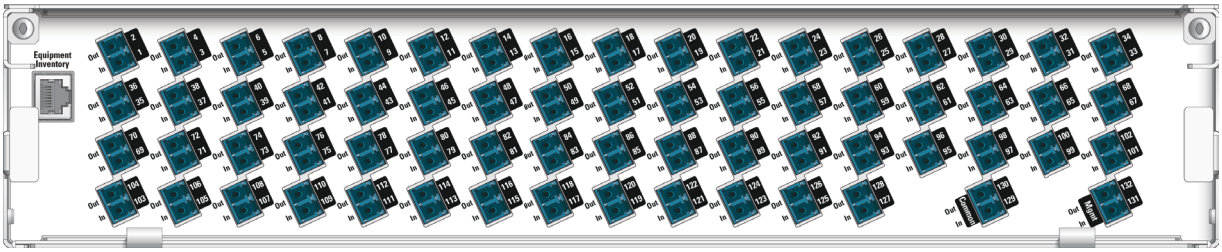


Figure 64 CCMD 8x24 C-Band/CCMD 8x24 L-Band module

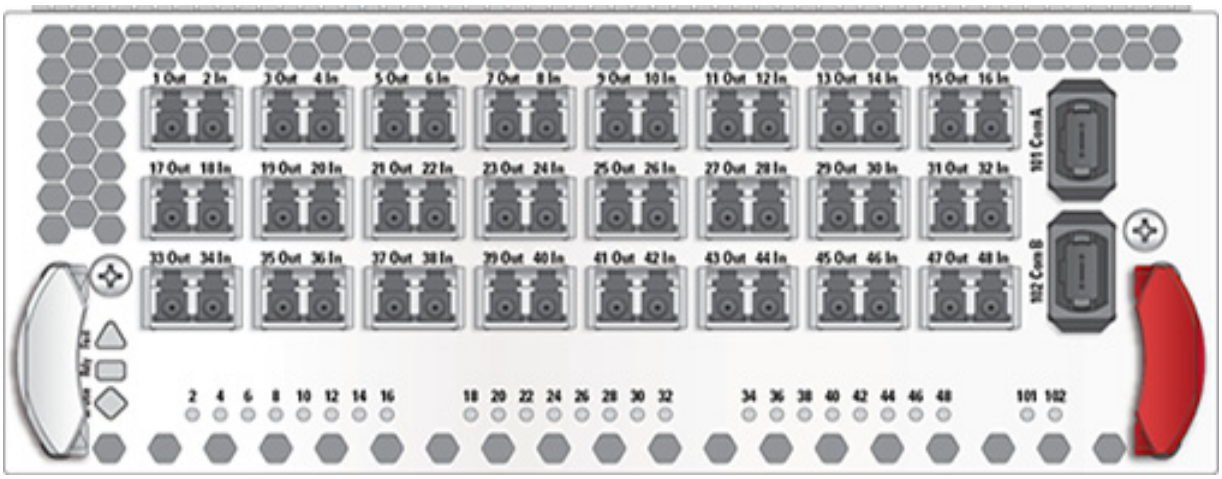


Figure 65 CCMD 16 C-Band module

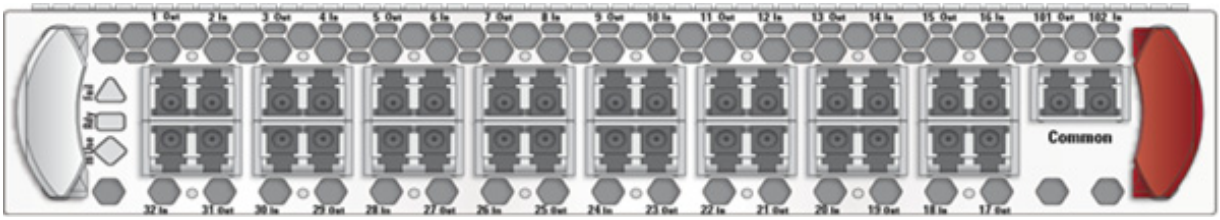
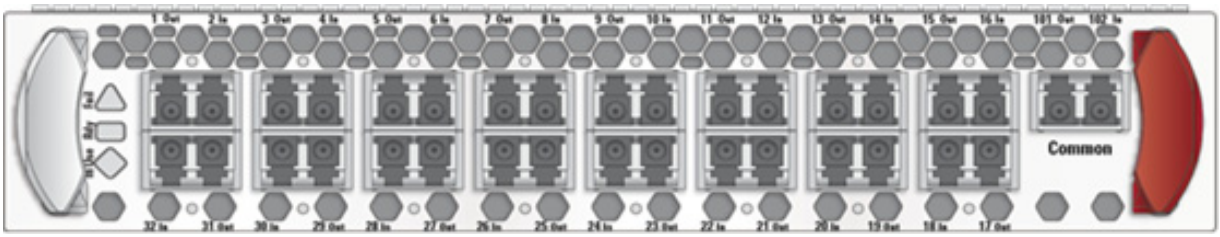


Figure 66 CCMD 16 L-Band module



Copyright© 2019-2025 Ciena® Corporation

Figure 67 CCMD 16x24 C-Band/CCMD 16x24 L-Band Module

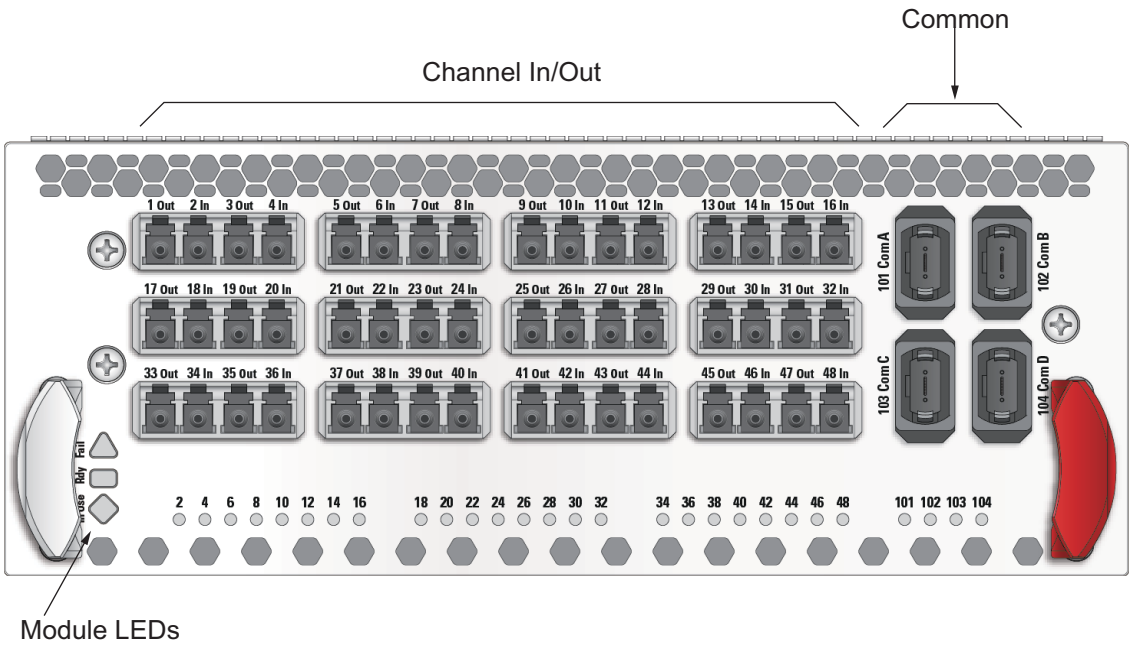
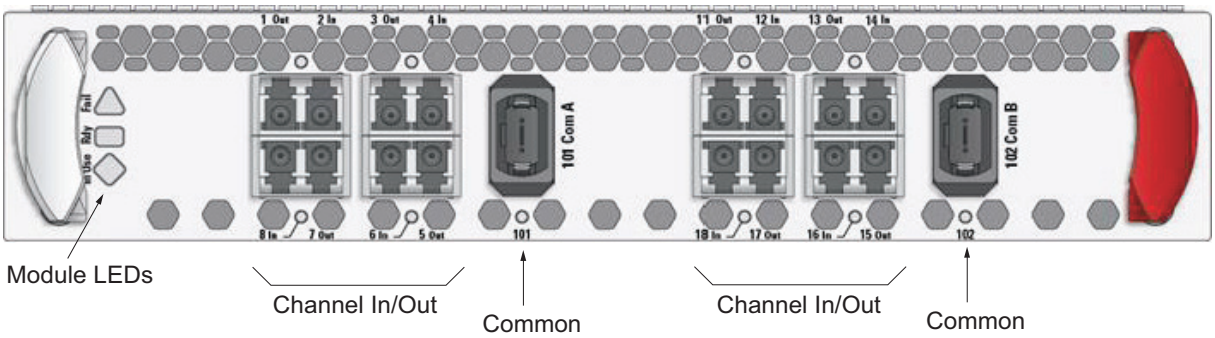


Figure 68 SSM C-Band module



Copyright© 2019-2025 Ciena® Corporation

Procedure 155 Replacing a CFIM, UCS, or MonCS in an OMC2 chassis

Requirements

To perform this procedure, you must

- have a replacement CFIM. Review the “Ordering information” in *6500 RLS Planning Guide*, NTRN10WA to make sure you select the correct PEC as the replacement part for this product platform.
- observe all safety requirements described in *6500 RLS Shelf Installation Guide,* 323-2051-201

CAUTION
Risk of equipment damage
Electrostatic discharge (ESD) can damage electrostatic sensitive devices. You must use antistatic protection while unpacking and installing all Field-Replaceable Units (FRU) and cables.

Overview

Use this procedure to replace the following modules:

- Compact Fiber Interconnect Module Type 1 (CFIM1) (NTK504QA)
- Compact Fiber Interconnect Module Type 2 (CFIM2) (NTK504QB)
- Compact Fiber Interconnect Module Type 3 (CFIM3) (NTK504QC)
- Upgrade Coupler/Splitter (UCS) Module (NTK504PL)
- Monitor Coupler/Splitter (MonCS) Module (NTK504PN)

CAUTION
Service affecting procedure
CFIM module replacement is service affecting. Ensure you have exhausted all other troubleshooting options before performing this procedure and if possible, re-route the traffic to minimize the traffic loss.

Steps

Removing the module

1. Identify the failed module or the module to be replaced.
2. Wear an antistatic wrist strap or foot straps to protect the shelf from static damage. If using a wrist strap, connect the wrist strap to the ESD jack on the shelf.

Copyright© 2019-2025 Ciena® Corporation

3

CAUTION
Risk of laser radiation exposure
Do not look directly into the optical beam. Invisible light can severely damage your eyes.

CAUTION
Risk of damage to modules
Never disconnect an optical fiber that is connected to an active or powered up optical amplifier. To disconnect or reconnect an optical fiber, make sure the optical amplifier is “Disabled”.

Ensure that labels are applied to both ends of all cables and optical fiber patchcords.

4 Switch traffic away from the optical link by performing a protection switch to prevent traffic loss. Refer to *Equipment/Facility Provisioning and Protection*, 323-2051-310.

5 Disconnect all optical connectors from the module to be replaced.

6 Put protective caps on the ends of the patchcords to protect them from contamination and damage.

7 Unfasten the captive screws on the faceplate of the module and remove the faceplate. See Figure 69 on page 380.

8 Unseat and gently pull the CFIM, UCS, or MonCS until it is fully removed from the OMC2 chassis.

Installing the CFIM1, CFIM2, CFIM3, UCS, or MonCS into the OMC2 chassis

9 Verify that the replacement PEC is the same as the current PEC.

10 Insert the module into the OMC2 in Slot 1 (left slot) or Slot 2 (right slot). Secure the faceplate to the module and OMC2 using the captive screws. See Figure 69 on page 380 for an example of a module installation in Slot 1. Refer to “Installing an OMC2 chassis and associated modules” in *6500 RLS Shelf Installation Guide,* 323-2051-201. After completing all the steps for installing the module into the OMC2, go to the next step.

11 Clean all fiber connectors disconnected from the ports in step 4 and reconnect them to the appropriate ports on the module. For instructions on inspecting and cleaning optical fiber, refer to *Optical Connector Inspection and Cleaning*, 323-1859-500.

12 Wait for the module to start.

13 Retrieve all the active alarms and alarm details:

If you want to perform the procedure using	**Then** go to the
CLI commands	“CLI INTERFACE STEPS”
Node Essentials	“NODE ESSENTIALS STEPS”

Copyright© 2019-2025 Ciena® Corporation

CLI INTERFACE STEPS

14 To retrieve all the active alarms and alarm details, enter:

```
show active-alarm <id> [name] [resource] [raise-time]
[raise-time] [cause] [condition-type] [direction]
[location] [severity] [service-impact] [additional-info]
[user-notes...]
```

The current alarms and alarm details will appear.

15 Go to step 17.

NODE ESSENTIALS STEPS

16 From the **Alarms** menu, select Current alarms.

The active alarm menu opens indicating the data for the active-alarm object.

17 If the “Software Auto-Upgrade in Progress” alarm is active, wait until the alarm clears before continuing.

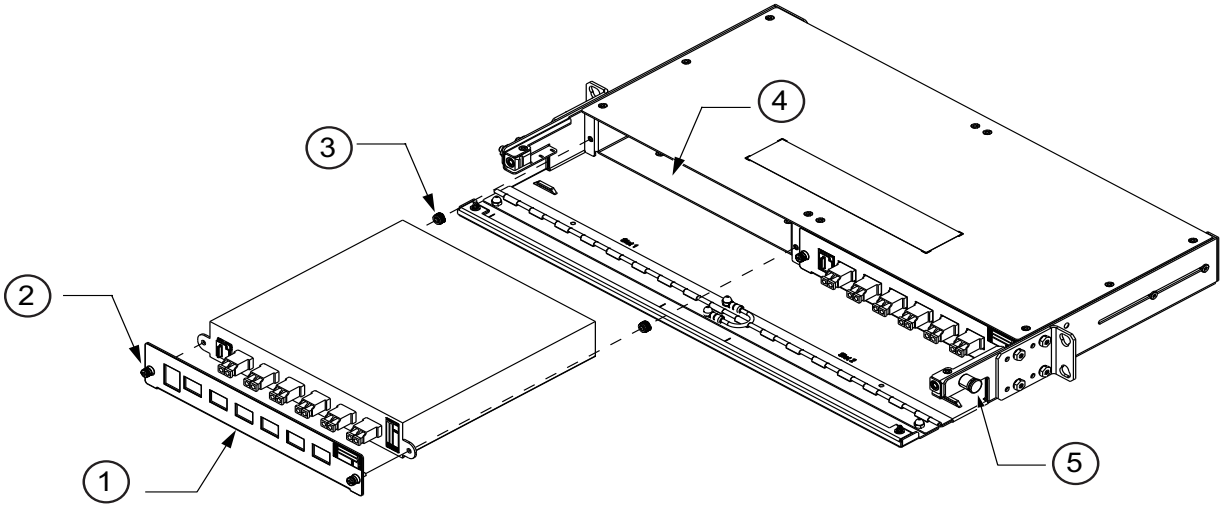
Note: It can take up to 15 minutes for this alarm to clear.

18 Undo any traffic switches invoked in step 4.

19 Put the facilities back in-service. Refer to *Equipment/Facility Provisioning and Protection*, 323-2051-310.

20 Ensure there are no active alarms against the newly installed module(s).

Figure 69 CFIM replacement in OMC2 chassis



Legend

1	Module faceplate	4	Chassis slot
2	Captive screw (2 places)	5	Plunger
3	Thumb nut (2 places)		

Copyright© 2019-2025 Ciena® Corporation

Procedure 156 Replacing the WSS 32x1 C-Band Module

Use this procedure to replace the Wavelength Selective Switch (WSS) 32x1 C-Band (NTK852LA) Module.

Requirements

To perform this procedure, you must:

- observe all safety requirements described in *6500 RLS Shelf Installation Guide,* 323-2051-201
- have the correct replacement module (the replacement Product Engineering Code [PEC] is the same as the current PEC)
- have protective caps for the patchcords
- obtain optical port dust caps from current or replacement circuit pack. Dust caps are required to prevent damage to circuit pack's optical ports

CAUTION
Risk of equipment damage
Electrostatic discharge (ESD) can damage electrostatic sensitive devices. You must use antistatic protection while unpacking and installing all Field-Replaceable Units (FRU) and cables.

Overview

Make sure the MPO ports and MPO fibers are clean when connected to the replaced WSS 32x1 C-Band module. For instructions on inspecting and cleaning optical fiber, refer to *Optical Connector Inspection and Cleaning*, 323-1859-500.

CAUTION
Service affecting procedure
WSS 32x1 module replacement is service affecting. Ensure you have exhausted all other troubleshooting options before performing this procedure and if possible, re-route the traffic to minimize the traffic loss.

Steps

1. Check the date and time of the last backup and check whether a data backup is required. Refer to *6500 RLS ZTP and Manual Commissioning*, 323-2051 220 for details on how to view the current backup state and how to save provisioning data.
2. Perform a manual switch on the port to verify the inactive path. Refer to *Equipment/Facility Provisioning and Protection*, 323-2051-310.

Copyright© 2019-2025 Ciena® Corporation

If traffic switches back autonomously to the active path or if the manual switch is denied, contact your next level of support or your Ciena support group.

3 Change the admin states of all facilities on the module to “Disabled”. Refer to *Equipment/Facility Provisioning and Protection*, 323-2051-310.

4 Change the equipment admin state of the module to “Disabled”. Refer to “Provisioning a circuit pack or pluggable” procedure in *Equipment/Facility Provisioning and Protection*, 323-2051-310.

5 Verify the current alarm conditions on the network element. Depending on the configuration of the node where this procedure is to be performed, the following alarms can appear throughout the network during this procedure:

- Automatic Power Reduction Active
- Automatic Shutoff
- Circuit Pack Missing
- Loss Of Signal
- Shutoff Threshold Crossed

6 Verify that the replacement Product Engineering Code (PEC) is the same as the current PEC.

7 Wear an antistatic wrist strap or foot straps to protect the shelf from static damage. If using a wrist strap, connect the wrist strap to the ESD jack on the shelf.

8 Ensure that labels are applied to both ends of all cables and optical fiber patchcords.

9 Disconnect all optical connectors from the WSS 32x1 module.

10 Place protective caps on the ends of the patchcords to protect them from contamination and damage.

11 Unseat and remove the WSS module from the slot.

12 Install the replacement WSS module into the corresponding slot and press the latches to close.

13 Clean all fiber connectors disconnected from the WSS 32x1 ports in step 9 and reconnect them to the appropriate ports on the WSS 32x1 module. For instructions on inspecting and cleaning optical fiber, refer to *Optical Connector Inspection and Cleaning*, 323-1859-500.

14 Wait for the WSS 32x1 module to start.

During a power up, LEDs on the front of the module go through a sequence. Wait until this sequence is complete before proceeding to the next step

15 Change the admin states of all facilities on the module to “Enabled”. Refer to *Equipment/Facility Provisioning and Protection*, 323-2051-310.

16 Wait for the WSS or SMD circuit pack to start.

17 Change the equipment admin state of the module to “Enabled”.

18 If the “Upgrade in Progress” alarm is active, wait until the alarm clears before continuing. It can take up to 15 minutes for this alarm to clear.

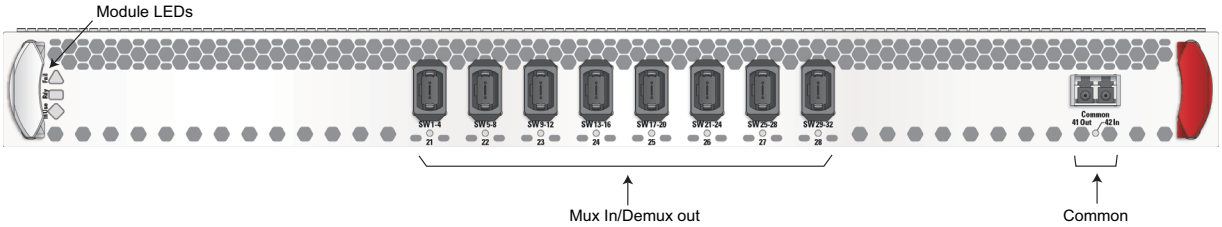
Copyright© 2019-2025 Ciena® Corporation

19 If “Autoprovisioning Mismatch” alarm is active, a problem with provisioning the module has been detected. Refer to the “Alarms”section in this document.

20 If applicable, return traffic to the module by releasing the protection switch invoked in step 2

21 Ensure there are no active alarms against the newly installed module(s).

Figure 70 WSS 32x1 C-Band module



Copyright© 2019-2025 Ciena® Corporation

Procedure 157 Replacing a Fiber Interconnect Module Type 4 (FIM4)/FIM4A

Use this procedure to replace the Fiber Interconnect Module Type 4 (FIM4) (NTK504CD)/FIM4A (NTK504CX).

Requirements

To perform this procedure, you must:

- observe all safety requirements described in *6500 RLS Shelf Installation Guide,* 323-2051-201
- have the correct replacement module (the replacement Product Engineering Code [PEC] is the same as the current PEC)
- have protective caps for the patchcords

CAUTION
Risk of equipment damage
Electrostatic discharge (ESD) can damage electrostatic sensitive devices. You must use antistatic protection while unpacking and installing all Field-Replaceable Units (FRU) and cables.

Overview

Any FIM connector not equipped with a loopback module or fiber patch cord must be equipped with a dust cap. The FIM tray assembly includes a bag of dust caps that must be put on any loopback module that is being removed and saved for future use. Removing the loopback and replacing with a simple dust cap in FIMs could result in hfl (High Fiber Loss).

CAUTION
Service affecting procedure
FIM4 module replacement is service affecting. Ensure you have exhausted all other troubleshooting options before performing this procedure and if possible, re-route the traffic to minimize the traffic loss.

Steps

Removing the module

1 Identify the failed module or the module to be replaced.

2 Wear an antistatic wrist strap or foot straps to protect the shelf from static damage. If using a wrist strap, connect the wrist strap to the ESD jack on the shelf.

3 Ensure that labels are applied to all MPO/LC cables on the module faceplate.

Copyright© 2019-2025 Ciena® Corporation

4 Disconnect all MPO/LC cables from the module to be replaced.

5 Place protective dust caps on the ends of the MPO/LC cables and MPO/LC ports to protect them from contamination and damage.

Note: If you disconnect a cable from an external slot and want to insert the same cable or another cable in the same external port, wait a few seconds before reconnecting (wait for the green LED to turn off) to allow the shelf inventory to update.

6 Using a screwdriver and an open wrench, unscrew the ground connection on the left side of the FIM. Remove the screws on both sides of the panel securing the FIM to the frame, while holding the module.

7 Remove the module from the frame and store it in a safe place.

Installing the module

8 Insert the replacement module into the frame.

9 Insert screws on each side of the FIM to secure the module to the frame while holding the module.

10 Re-connect the ground cable and secure the nuts on the left side of the replacement FIM.

11 Remove the protection dust caps of the MPO cables along with the required protection dust caps and MPO loopback plugs ports before reconnecting.

12 Use optical scope to inspect the MPO/LC ports on the FIM and the MPO/LC cables. Clean and reconnect them to the replacement module faceplate as per labels. Refer to *Optical Connector Inspection and Cleaning*, 323-1859-500.

13 Ensure there are no active alarms against the newly installed module(s).

Figure 71 FIM Type 4 module

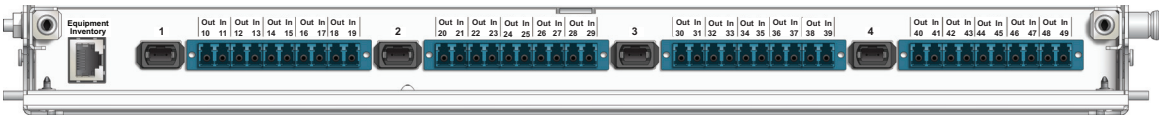
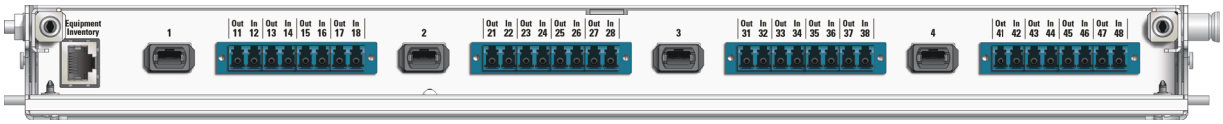


Figure 72 FIM Type 4A module



Copyright© 2019-2025 Ciena® Corporation

Procedure 158 Replacing an RLA module

Requirements

To perform this procedure, you must:

- observe all safety requirements described in *6500 RLS Shelf Installation Guide,* 323-2051-201
- have the correct replacement module (the replacement Product Engineering Code [PEC] is the same as the current PEC)
- have protective caps for the patchcords

CAUTION
Risk of equipment damage
Electrostatic discharge (ESD) can damage electrostatic sensitive devices. You must use antistatic protection while unpacking and installing all Field-Replaceable Units (FRU) and cables.

Overview

Use this procedure to replace one of the following modules:

- RLA 32x1 C-Band 1xSFP Module (NTK852AA)
- RLA 32x1 C&L-Band 1xSFP Module (NTK852AC)
- RLA 32x1 iC&L-Band 1xSFP Module (NTK852AH)
- RLA 64x1 iC&L-Band 1xSFP Module (NTK862AH)
- RLA 12x1 C-Band 1xSFP Module (NTK852BA)
- RLA 12x1 C&L-Band Module (NTK852BC)
- RLA 12x1 C-Band 1xSFP module (NTK892BA)
- RLA 12x1 C&L-Band 1xSFP module (NTK892BC)

CAUTION
Service affecting procedure
RLA module replacement is service affecting. Ensure you have exhausted all other troubleshooting options before performing this procedure and if possible, re-route the traffic to minimize the traffic loss.

Copyright© 2019-2025 Ciena® Corporation

Steps

Removing the module

1. Check the date and time of the last backup and check whether a data backup is required. Refer to *Licensing, Security, and Administration*, 323-2051-300 for details on how to view the current backup state and how to save provisioning data.
2. Retrieve and save the system logs on the RLS shelf. Refer to *Logs and PMs*, 323-2051-520.
3. Verify the current alarm conditions on the network element. Depending on the configuration of the node where this procedure is to be performed, the following alarms can appear throughout the network during this procedure:
   - Automatic Power Reduction Active
   - Automatic Shutoff
   - Circuit Pack Missing
   - Shutoff Threshold Crossed
   - Optical Line Fail
4. Verify that the replacement Product Engineering Code (PEC) is the same as the current PEC.
5. Switch traffic away from this optical link by performing a protection switch at the service layer to prevent traffic loss. Refer to the “Protection configurations and CTM redundancy” procedure in *Equipment/Facility Provisioning and Protection*, 323-2051-310.
6. Change the admin state of the Pre-AMP and the booster AMP facility to “Disabled”.

If you want to perform the procedure using	**Then** go to the
CLI commands	“CLI INTERFACE STEPS”
Node Essentials	“NODE ESSENTIALS STEPS”

CLI INTERFACE STEPS

7. To place the alarmed Pre-AMP and the booster AMP facility to “Disabled”, enter the following command:

   ```
   set slots <SlotNum> config amps <name> [admin-state
   <Disabled>]
   ```

   Note: This command requires confirmation as it might impact traffic. Type Y to confirm.
8. Go to step 14.

NODE ESSENTIALS STEPS

9. Select **Facilities** from the Node Essentials navigation menu.

   The Facilities menu opens.
10. From the **Equipment** grid, select the module with the alarmed AMP facility.

    The bottom part of screen becomes populated.

Copyright© 2019-2025 Ciena® Corporation

11 Select AMP facility from Facility navigator.

The AMP Facilities grid opens.

12 Select the alarmed AMP facility by Row selector from the AMP Facilities grid.

13 Click the **Pencil** icon.

The related Edit AMP dialog opens.

14 Edit the Admin state of the Pre-AMP and the booster AMP facility to Disabled.

15 Click **Confirm**.

16 Provision the admin state of the module to “Disabled”.

If you want to perform the procedure using	**Then** go to the
CLI commands	“CLI INTERFACE STEPS”
Node Essentials	“NODE ESSENTIALS STEPS”

CLI INTERFACE STEPS

17 The following step is performed using CLI commands.

```
set slots <slot #> config circuit-pack admin-state
<Disabled>
```

18 Go to step 24.

NODE ESSENTIALS STEPS

19 Select **Facilities** from the Node Essentials navigation menu.

The Facilities menu opens.

20 From the **Equipment** grid, select the module to be replaced.

21 Click the **Pencil** icon (Edit Equipment).

22 Set the Admin state of the equipment to Disabled

23 Click **Confirm**.

24 Ensure that the blue LED on the module faceplate is off.

25

CAUTION
Risk of laser radiation exposure
Do not look directly into the optical beam. Invisible light can severely damage your eyes.

CAUTION
Risk of damage to modules
Never disconnect an optical fiber that is connected to an active or powered up optical amplifier. To disconnect or reconnect an optical fiber, make sure the optical amplifier is “Disabled”.

Copyright© 2019-2025 Ciena® Corporation

CAUTION
Risk of damage to modules
Wear an antistatic wrist strap to protect the equipment from static damage. Connect the wrist strap to the ESD jack on the shelf or module.

Ensure that labels are applied to both ends of all cables and optical fiber patchcords.

26 Unseat the module to ensure that power is off. Push outwards on both pull tabs simultaneously and pull the module out far enough so that the power is off to the module and LEDs are turned off. Refer to Procedure 138, “Reseating a module” in this document.

27 Disconnect all optical connectors from the module to be replaced.

28 Put protective caps on the ends of the patchcords to protect them from contamination and damage.

29 Gently pull the module until it is fully removed from the shelf.

Installing the module

30 Install the replacement module into the corresponding slot and press the latches to close. For complete equipping rules and module slot numbering, refer to “Module descriptions, equipping rules, specifications” in *6500 RLS Planning Guide*, NTRN10WA.

31 Wait a few minutes for the card to initialize, before viewing the inventory data.

32 You can retrieve the inventory data for the module you inserted.

If you want to perform the procedure using	**Then** go to the
CLI commands	“CLI INTERFACE STEPS”
Node Essentials	“NODE ESSENTIALS STEPS”

CLI INTERFACE STEPS

33 The following step is performed using CLI commands.

```
show slots <SlotNum> inventory circuit-pack [pec]
[hardware-release] [common-language-equipment-
identifier][serial-number] [manufacturing date] [power]
[diagnostic] [current-temperature] [average-
temperature]
```

34 Go to step 38.

NODE ESSENTIALS STEPS

35 Click on the **Chassis** menu and select the module you want to retrieve the inventory for.

The inventory information appears on the right side of the screen.

36 Clean all fiber connectors disconnected from the ports in step 27 and reconnect them to the appropriate ports on the module. For instructions on inspecting and cleaning optical fiber, refer to *Optical Connector Inspection and Cleaning*, 323-1859-500.

Copyright© 2019-2025 Ciena® Corporation

37 Wait for the module to start.

38 Change the admin state of the facilities back to “Enabled”.

39 Provision the admin state of the module back to “Enabled”.

If you want to perform the procedure using	**Then** go to the
CLI commands	“CLI INTERFACE STEPS”
Node Essentials	“NODE ESSENTIALS STEPS”

CLI INTERFACE STEPS

40 The following step is performed using CLI commands.

```
set slots <slot #> config circuit-pack admin-state
<Enabled>
```

41 Go to step 46.

NODE ESSENTIALS STEPS

42 Select **Facilities** from the Node Essentials navigation menu.

The Facilities menu opens.

43 From the **Equipment** grid, select the module to be replaced.

44 Click the **Pencil** icon (Edit Equipment).

45 Click **Confirm**.

46 Ensure that the blue LED on the module faceplate is on.

47 Retrieve all the active alarms and alarm details.

48 Clear any unexpected alarms by following the appropriate trouble clearing procedure in this document.

49 If the “Software Auto-Upgrade in Progress” alarm is active, wait until the alarm clears before continuing.

Note: It can take up to 15 minutes for this alarm to clear.

50 If the “Autoprovisioning Mismatch” alarm is active, a problem with provisioning the module has been detected.

If the alarm does not clear, Contact your next level of support or your Ciena support group.

51 Undo any traffic switches invoked in step 5.

52 Ensure there are no active alarms against the newly installed module(s).

Copyright© 2019-2025 Ciena® Corporation

Figure 73 RLA 32x1 C-Band 1xSFP module (NTK852AA)

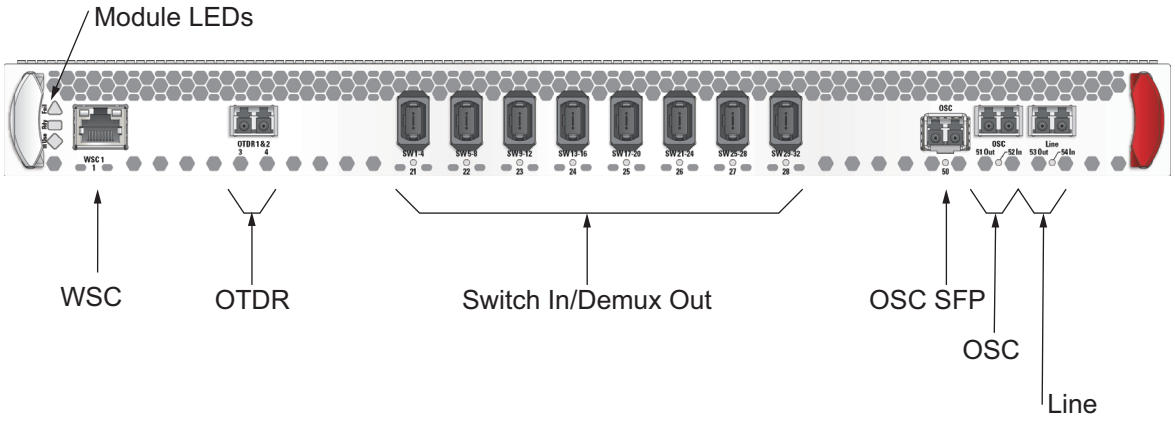


Figure 74 RLA 12x1 C-Band 1xSFP module (NTK852BA)

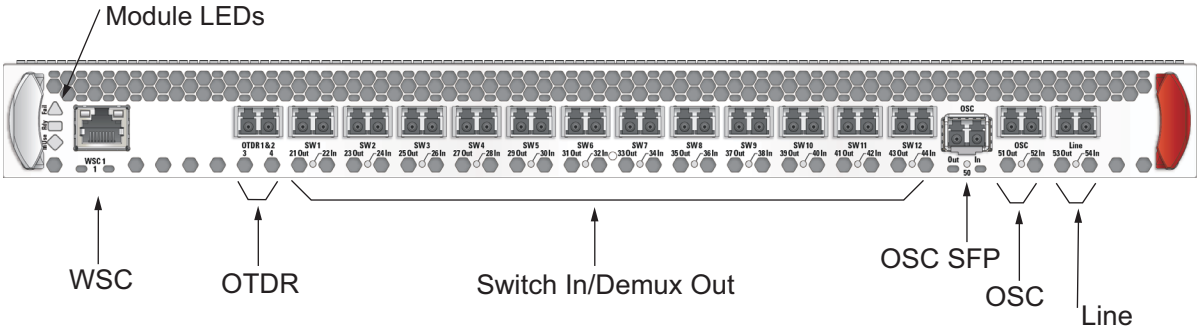
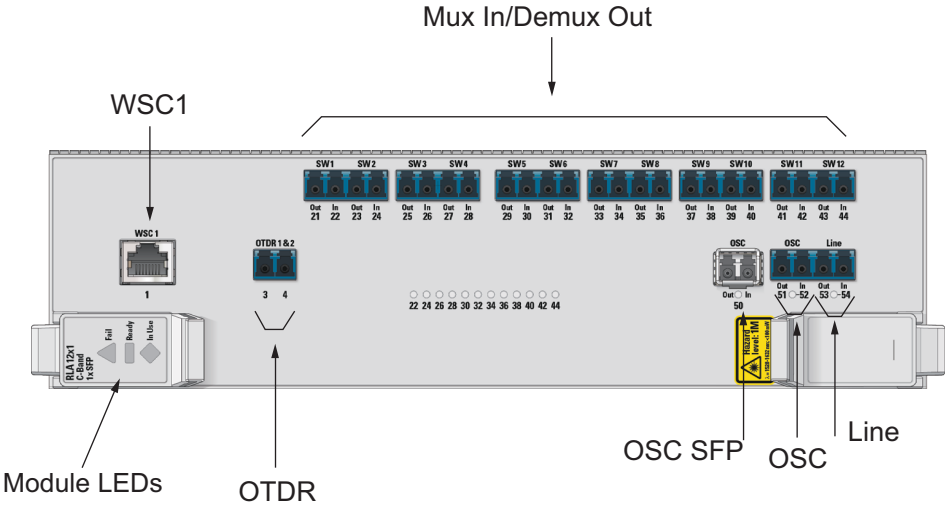


Figure 75 RLA 12x1 C-Band 1xSFP module (NTK892BA)



Copyright© 2019-2025 Ciena® Corporation

Figure 76 RLA 12x1 C&L-Band Module (NTK852BC)

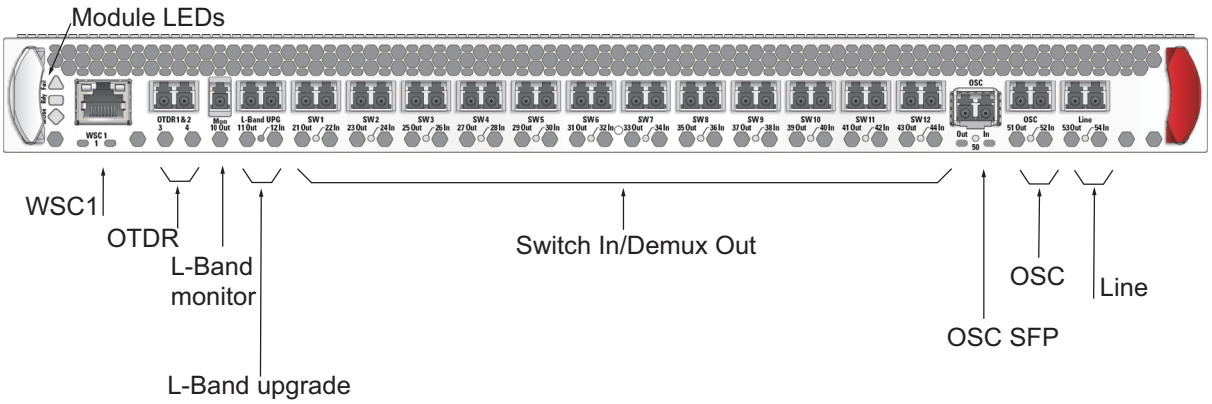


Figure 77 RLA 12x1 C&L-Band module (NTK892BC)

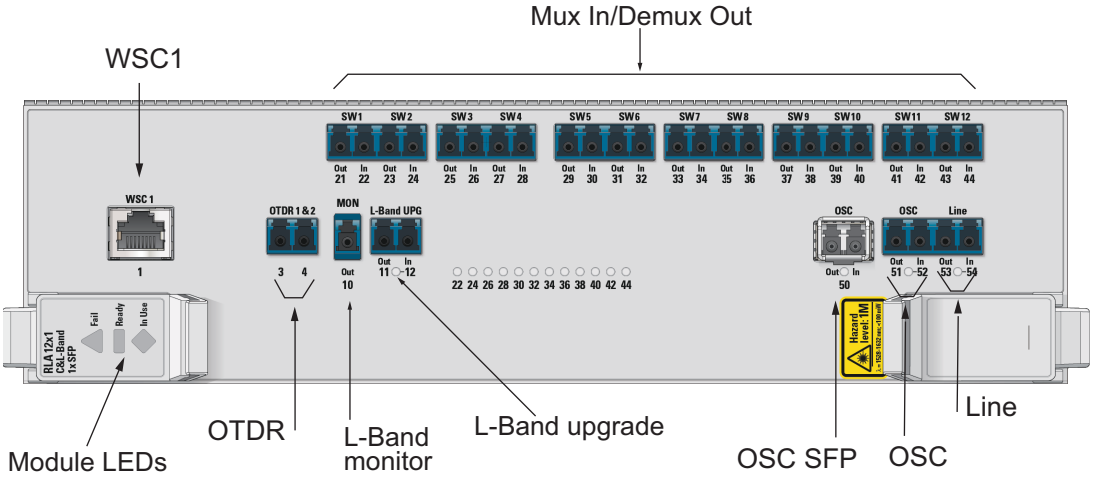
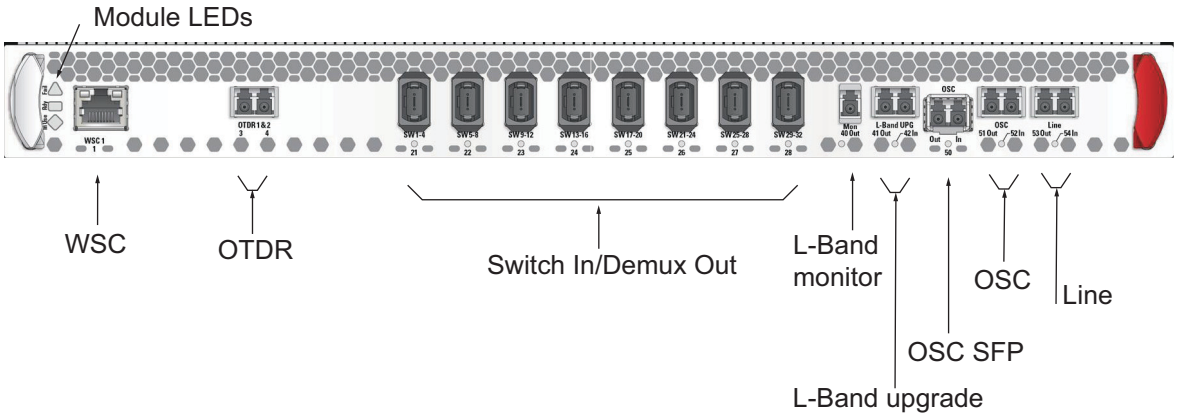


Figure 78 RLA 32x1 C&L-Band 1xSFP module (NTK852AC)



Copyright© 2019-2025 Ciena® Corporation

Figure 79 RLA 32x1 iC&L-Band Module - faceplate (NTK852AH)

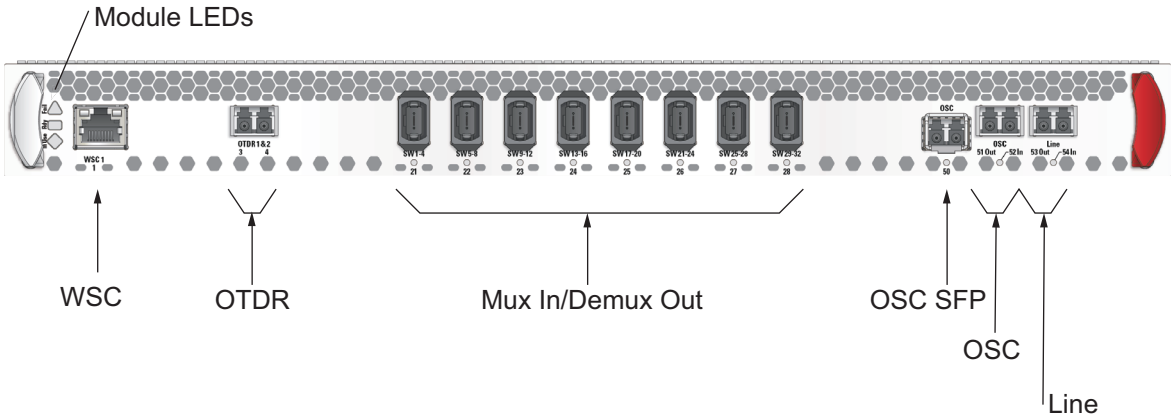
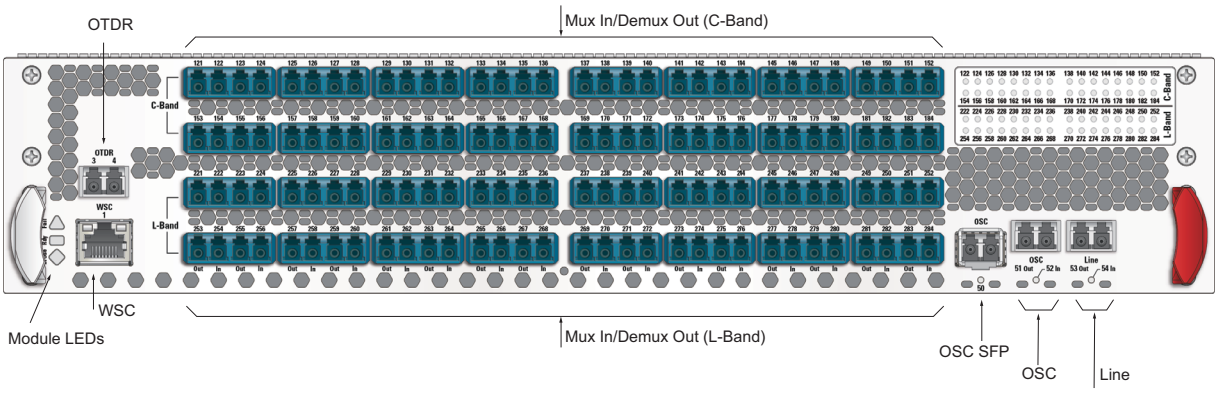


Figure 80 RLA 64x1 iC&L-Band 1xSFP Module - faceplate (NTK862AH)



Copyright© 2019-2025 Ciena® Corporation

Procedure 159 Replacing LRU module

Requirements

To perform this procedure, you must:

- observe all safety requirements described in *Installation – 6500 RLS Shelf,* 323-2051-201
- have the correct replacement module (the replacement Product Engineering Code [PEC] is the same as the current PEC)
- have protective caps for the patchcords

CAUTION
Service affecting procedure
LRU module replacement is service affecting. Ensure you have exhausted all other troubleshooting options before performing this procedure and if possible, re-route the traffic to minimize the traffic loss.

CAUTION
Risk of equipment damage
Electrostatic discharge (ESD) can damage electrostatic sensitive devices. You must use antistatic protection while unpacking and installing all Field-Replaceable Units (FRU) and cables.

Overview

Use this procedure to replace the following module.

- L-Band ROADM Upgrade (LRU) module NTK852NA

Steps

Removing the LRU

1 Check the date and time of the last backup and check whether a data backup is required. Refer to *Licensing, Security, and Administration*, 323-2051-300 section in this document for details on how to view the current backup state and how to save provisioning data.

Copyright© 2019-2025 Ciena® Corporation

2 Verify the current alarm conditions on the network element. Depending on the configuration of the node where this procedure is to be performed, the following alarms can appear throughout the network during this procedure:

- Automatic Power Reduction Active
- Automatic Shutoff
- Circuit Pack Missing
- Shutoff Threshold Crossed
- High Fiber Loss
- Fiber Break detected
- Connection Validation Data Missing

3 Verify that the replacement Product Engineering Code (PEC) is the same as the current PEC.

4 Switch traffic away from this optical link by performing a protection switch at the service layer to prevent traffic loss. Refer to *Equipment/Facility Provisioning and Protection*, 323-2051-310.

5 Ensure that the blue LED on the module faceplate is off.

6

CAUTION
Risk of laser radiation exposure
Do not look directly into the optical beam. Invisible light can severely damage your eyes.

CAUTION
Risk of damage to modules
Never disconnect an optical fiber that is connected to an active or powered up optical amplifier. To disconnect or reconnect an optical fiber, make sure the optical amplifier is “Disabled”.

CAUTION
Risk of damage to modules
Wear an antistatic wrist strap to protect the equipment from static damage. Connect the wrist strap to the ESD jack on the shelf or module.

Ensure that labels are applied to both ends of all cables and optical fiber patchcords.

7 Disconnect all optical connectors from the module to be replaced.

8 Put protective caps on the ends of the patchcords to protect them from contamination and damage.

9 Push outwards on both pull tabs simultaneously and pull the module out of the slot.

10 Gently pull the module until it is fully removed from the module.

Copyright© 2019-2025 Ciena® Corporation

Installing the LRU chassis

11 Verify that the replacement PEC is the same as the current PEC.

12 Install the replacement module into the corresponding slot and press the latches to close. For complete equipping rules and module slot numbering, refer to “Module descriptions, equipping rules, specifications” in *6500 RLS Planning Guide*, NTRN10WA.

13 You can retrieve the inventory data for the module you inserted.

If you want to perform the procedure using	**Then** go to the
CLI commands	“CLI INTERFACE STEPS”
Node Essentials	“NODE ESSENTIALS STEPS”

CLI INTERFACE STEPS

14 The following step is performed using CLI commands.

```
show slots <SlotNum> inventory circuit-pack [pec]
[hardware-release] [common-language-equipment-
identifier][serial-number] [manufacturing date] [power]
[diagnostic] [current-temperature] [average-
temperature]
```

15 Go to step 17.

NODE ESSENTIALS STEPS

16 Click on the **Chassis** menu and select the module you want to retrieve the inventory for.

The inventory information appears on the right side of the screen.

17 Clean all fiber connectors disconnected from the ports in step 7 and reconnect them to the appropriate ports on the module. For instructions on inspecting and cleaning optical fiber, refer to *Optical Connector Inspection and Cleaning*, 323-1859-500.

18 Wait for the module to start.

Note: While LRU is removed or rebooting, RLA replaces lost L-Band ASE with its own L-Band ASE source to meet the L-Band launch power profile. After recovery, the channel controller re-evaluates relevant in/out profile deltas and re-adjusts WSS attenuation accordingly for traffic channels.

19 Retrieve all the active alarms and alarm details:

If you want to perform the procedure using	**Then** go to the
CLI commands	“CLI INTERFACE STEPS”
Node Essentials	“Retrieving the data for the active alarm object” on page 32 in this document. Then go to step 21.

Copyright© 2019-2025 Ciena® Corporation

CLI INTERFACE STEPS

20 The following step is performed using CLI commands.

```
show active-alarm <id> [name] [resource] [raise-time]
[raise-time] [cause] [condition-type] [direction]
[location] [severity] [service-impact] [additional-info]
[user-notes...]
```

The current alarms and alarm details will appear.

21 If the “Software Auto-Upgrade in Progress” alarm is active, wait until the alarm clears before continuing.

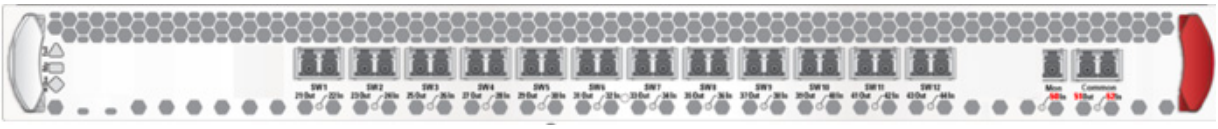
Note: It can take up to 15 minutes for this alarm to clear.

22 Undo any traffic switches invoked in step 4.

23 Update the user label with the current shelf and slot number.

24 Ensure there are no active alarms against the newly installed module(s).

Figure 81 LRU Module (NTK852NA)



Copyright© 2019-2025 Ciena® Corporation

Procedure 160 Replacing an SRA module

Requirements

To perform this procedure, you must:

- observe all safety requirements described in *6500 RLS Shelf Installation Guide,* 323-2051-201
- have the correct replacement module (the replacement Product Engineering Code [PEC] is the same as the current PEC)
- have protective caps for the patchcords
- have the cleaning supplies to clean the optical ports
- ensure the SRA circuit pack and all its facilities are all provisioned and available in the CLI (Blue and Green LED lit)
- ensure that the required fiber connection spacing is respected for proper Raman go-nogo analysis as per the 6500 *RLS Planning Guide*, NTRN10WA
- first attempt to clear non OTDR/SRA related alarms using the alarm clearing procedures in the "Alarms" section in this document
- verify that the reported span losses are as expected. Ensure Telemetry and OSC facilities are receiving power and reporting the similar span loss in both directions (< 2dB tolerance).
- verify that the line-fiber link is reporting expected span losses in both directions and the "TELEMETRY" loss type is being reported. If any issues with span loss value (Field value vs PlannerPlus), then fix span loss by verifying patch panels and site fibering (using OTDR traces) or contact your next level support if needed. If field values are different from PlannerPlus, it is recommended to re-run PlannerPlus with actual field data.
- if dispatching someone to site, make sure they have a spare SRA circuit pack or verify that the site has a known good SRA circuit pack that can be swapped if needed

CAUTION
Risk of equipment damage
Electrostatic discharge (ESD) can damage electrostatic sensitive devices. You must use antistatic protection while unpacking and installing all Field-Replaceable Units (FRU) and cables.

- make sure that you perform the steps in the SRA troubleshooting process as illustrated in the following flow chart.

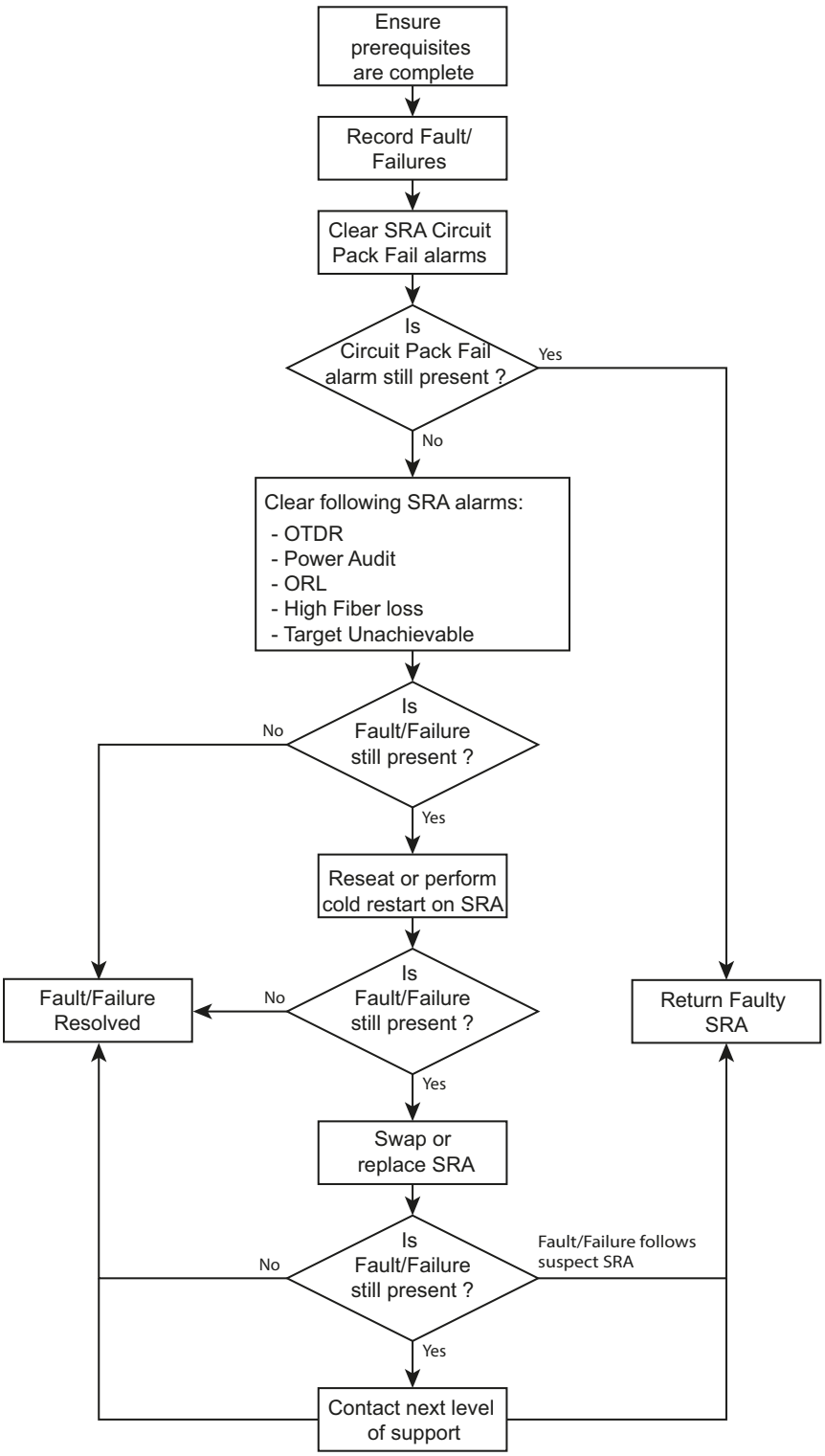
Copyright© 2019-2025 Ciena® Corporation

The flow chart provides a high-level view of the SRA troubleshooting process intended to provide guidance to network installers in the detection and correction of Single Line Raman Amplifier (SRA) related issues before deeming an SRA circuit pack needs to be returned.

For more information on the SRA troubleshooting, refer to alarm clearing procedures in the “Alarms” section in this document.

Copyright© 2019-2025 Ciena® Corporation

Figure 82 SRA troubleshooting



Copyright© 2019-2025 Ciena® Corporation

Overview

Use this procedure to replace one of the following modules:

- SRA C-Band Module (NTK830AA and NTK870AA)
- SRA C&L-Band Module (NTK830AC and NTK880AC)

CAUTION
Service affecting procedure
SRA module replacement is service affecting. Ensure you have exhausted all other troubleshooting options before performing this procedure and if possible, re-route the traffic to minimize the traffic loss.

Note: OTDR trace runs on the circuit pack replacement of the SRA circuit pack on the line only. If there is a DLA or RLA circuit pack replacement and there is a SRA on the line, the OTDR will not run.

Steps

1 Check the date and time of the last backup and check whether a data backup is required. Refer to *Licensing, Security, and Administration*, 323-2051-300 for details on how to view the current backup state and how to save provisioning data.

2 Verify the current alarm conditions on the network element. Depending on the configuration of the node where this procedure is to be performed, the following alarms can appear throughout the network during this procedure:

- Automatic Power Reduction Active
- Automatic Shutoff
- Circuit Pack Missing
- Shutoff Threshold Crossed
- Optical Line Fail

3 Verify that the replacement Product Engineering Code (PEC) is the same as the current PEC.

4 Switch traffic away from this optical link by performing a protection switch at the service layer to prevent traffic loss. Refer to *Equipment/Facility Provisioning and Protection*, 323-2051-310.

5 Provision the admin state of the module to “Disabled”.

If you want to perform the procedure using	**Then** go to the
CLI commands	“CLI INTERFACE STEPS”
Node Essentials	“NODE ESSENTIALS STEPS”

Copyright© 2019-2025 Ciena® Corporation

CLI INTERFACE STEPS

6 The following step is performed using CLI commands.

```
set slots <slot #> config circuit-pack admin-state
<Disabled>
```

7 Go to step 13.

NODE ESSENTIALS STEPS

8 Select **Facilities** from the Node Essentials navigation menu.

The Facilities menu opens.

9 From the **Equipment** grid, select the module to be replaced.

10 Click the **Pencil** icon (Edit Equipment).

11 Set the Admin state of the equipment to Disabled

12 Click **Confirm**.

13 Verify the current alarm conditions on the network element. Depending on the configuration of the node where this procedure is to be performed, the following alarms can appear throughout the network during this procedure:

- Automatic Power Reduction Active
- Automatic Shutoff
- Circuit Pack Missing
- Shutoff Threshold Crossed
- Loss Of Signal
- Connection Validation Data Missing

14 Ensure that the blue LED on the module faceplate is off.

15

CAUTION
Risk of laser radiation exposure
Do not look directly into the optical beam. Invisible light can severely damage your eyes.

CAUTION
Risk of damage to modules
Never disconnect an optical fiber that is connected to an active or powered up optical amplifier. To disconnect or reconnect an optical fiber, make sure the optical amplifier is “Disabled”.

CAUTION
Risk of damage to modules
Wear an antistatic wrist strap to protect the equipment from static damage. Connect the wrist strap to the ESD jack on the shelf or module.

Copyright© 2019-2025 Ciena® Corporation

Ensure that labels are applied to both ends of all cables and optical fiber patchcords.

16 Provision the Raman facility to a “Disabled” state.

17 Choose your next step:

If you want to perform the procedure using	**Then** go to the
CLI commands	“CLI INTERFACE STEPS”
Node Essentials	“NODE ESSENTIALS STEPS”

CLI INTERFACE STEPS

18 To change the admin state of the facilities to “Disabled”, enter the following command:

```
set slots <slot #> config ramans LINE-IN admin-state
<Disabled>
```

Note: This command requires confirmation as it might impact traffic. Type Y to confirm.

19 Go to step 28.

NODE ESSENTIALS STEPS

20 Select **Facilities** from the Node Essentials navigation menu.

The Facilities menu opens.

21 From the **Equipment** grid, select the module with the RAMAN facility.

The bottom part of screen becomes populated.

22 Select RAMAN facility from Facility navigator.

The RAMAN Facilities grid opens.

23 Use Row selector to select the module with the RAMAN facility from Equipment grid.

The Facilities navigator opens.

24 Select the RAMAN facility by Row selector from the RAMAN Facilities grid.

25 Click the **Pencil** icon.

The related Edit dialog opens.

26 Edit the RAMAN facility as required.

Admin state: Disabled

27 Click **Confirm**.

28 Disconnect all optical connectors from the module to be replaced.

29 Put protective caps on the ends of the patchcords to protect them from contamination and damage.

30 Push outwards on both pull tabs simultaneously and pull the module out of the slot.

31 Gently pull the module until it is fully removed from the shelf.

Copyright© 2019-2025 Ciena® Corporation

Installing the module

32 Install the replacement module into the corresponding slot. For complete equipping rules and module slot numbering, refer to “Module descriptions, equipping rules, specifications” in *6500 RLS Planning Guide*, NTRN10WA.

33 Wait for the module to start.

34 You can retrieve the inventory data for the module you inserted.

If you want to perform the procedure using	**Then** go to the
CLI commands	“CLI INTERFACE STEPS”
Node Essentials	“NODE ESSENTIALS STEPS”

CLI INTERFACE STEPS

35 The following step is performed using CLI commands.

```
show slots <SlotNum> inventory circuit-pack [pec]
[hardware-release] [common-language-equipment-
identifier][serial-number] [manufacturing date] [power]
[diagnostic] [current-temperature] [average-
temperature]
```

36 Go to step 38.

NODE ESSENTIALS STEPS

37 Click on the **Chassis** menu and select the module you want to retrieve the inventory for.

The inventory information appears on the right side of the screen.

38 Clean all fiber connectors disconnected from the ports in step 28 and reconnect them to the appropriate ports on the module. For instructions on inspecting and cleaning optical fiber, refer to *Optical Connector Inspection and Cleaning*, 323-1859-500.

39 Wait for the OTDR go-nogo to complete. Ensure the go-nogo trace indicates “go”.

40 Retrieve the OTDR trace status.

If you want to perform the procedure using	**Then** go to the
CLI commands	“CLI INTERFACE STEPS”
Node Essentials	“NODE ESSENTIALS STEPS”

CLI INTERFACE STEPS

41 To display the OTDR events raising the issue. Enter the following command:

```
show-otdr-response name slot-<slot #>-port-<port #>
trace-tag current trace-type <office, short, or long>
```

42 Go to step 46.

NODE ESSENTIALS STEPS

43 Select **Tools** from the Node Essentials navigation menu.

Copyright© 2019-2025 Ciena® Corporation

The OTDR grid opens.

44 Use row selector to select the **OTDR** that you ran the OTDR Go/No-Go trace to display the OTDR events in the SOR traces grid.

45 Choose the desired SOR Trace and click on the “View trace” icon on the top corner of the SOR traces grid. Click on the key events or parameters in the OTDR trace window to see the resulting information.

46 Clean the fibers again if no-go is obtained.

47 Provision the Raman facility back to a “Enabled” state.

If you want to perform the procedure using	**Then** go to the
CLI commands	“CLI INTERFACE STEPS”
Node Essentials	“NODE ESSENTIALS STEPS”

CLI INTERFACE STEPS

48 To change the admin state of the facilities to “Enabled”, enter the following command:

```
set slots <slot #> config ramans LINE-IN admin-state
<Enabled>
```

49 Go to step 58.

NODE ESSENTIALS STEPS

50 Select **Facilities** from the Node Essentials navigation menu.

The Facilities menu opens.

51 From the **Facilities** grid, select the replaced module with the RAMAN facility.

The bottom part of screen becomes populated.

52 Select RAMAN facility from Facility navigator.

The RAMAN Facilities grid opens.

53 Use Row selector to select the module with the RAMAN facility from Equipment grid.

The Facilities navigator opens.

54 Select the RAMAN facility by Row selector from the RAMAN Facilities grid.

55 Click the **Pencil** icon.

The related Edit dialog opens.

56 Edit the RAMAN facility as required.

Admin state: Enabled

57 Click **Confirm**.

58 Provision the admin state of the module to “Enabled”.

If you want to perform the procedure using	**Then** go to the
CLI commands	“CLI INTERFACE STEPS”
Node Essentials	“NODE ESSENTIALS STEPS”

Copyright© 2019-2025 Ciena® Corporation

CLI INTERFACE STEPS

59 The following step is performed using CLI commands.

```
set slots <slot #> config circuit-pack admin-state
<Enabled>
```

60 Go to step 66.

NODE ESSENTIALS STEPS

61 Select **Facilities** from the Node Essentials navigation menu.

The Facilities menu opens.

62 From the **Equipment** grid, select the module to be replaced.

63 Click the **Pencil** icon (Edit Equipment).

64 Set the Admin state of the equipment to Enabled

65 Click **Confirm**.

66 Retrieve all the active alarms and alarm details:

If you want to perform the procedure using	**Then** go to the
CLI commands	"CLI INTERFACE STEPS"
Node Essentials	"Retrieving the data for the active alarm object" on page 32 in this document, Then go to step 68.

CLI INTERFACE STEPS

67 The following step is performed using CLI commands.

```
show active-alarm <id> [name] [resource] [raise-time]
[raise-time] [cause] [condition-type] [direction]
[location] [severity] [service-impact] [additional-info]
[user-notes...]
```

The current alarms and alarm details will appear.

68 If the "Upgrade In Progress" alarm is active, wait until the alarm clears before continuing.

Note: It can take up to 15 minutes for this alarm to clear.

69 Check for and clear any unexpected remaining active alarms. If the alarms are not clear, Contact your next level of support or your Ciena support group.

70 Undo any traffic switches invoked in step 4.

71 Update the user label with the current shelf and slot number.

72 Ensure there are no active alarms against the newly installed module(s).

Copyright© 2019-2025 Ciena® Corporation

Figure 83 SRA C-Band module (NTK870AA)

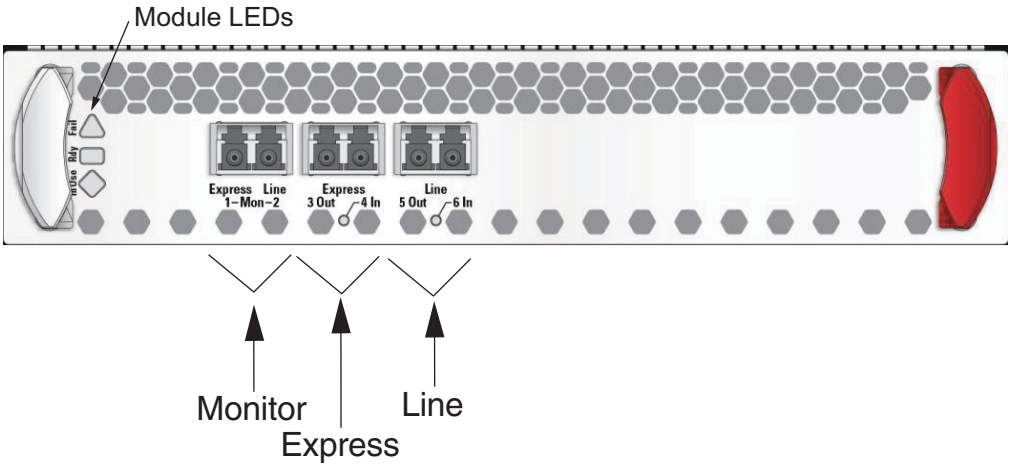


Figure 84 SRA C-Band module (NTK830AA)

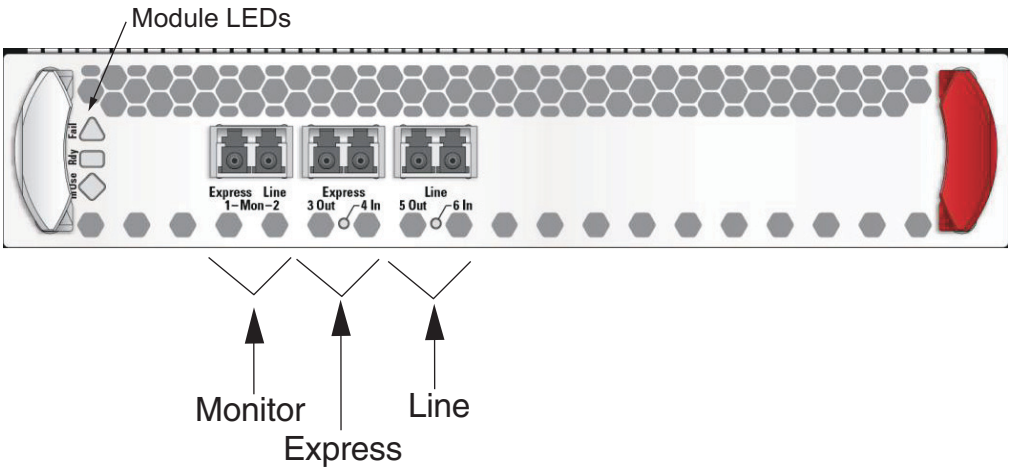
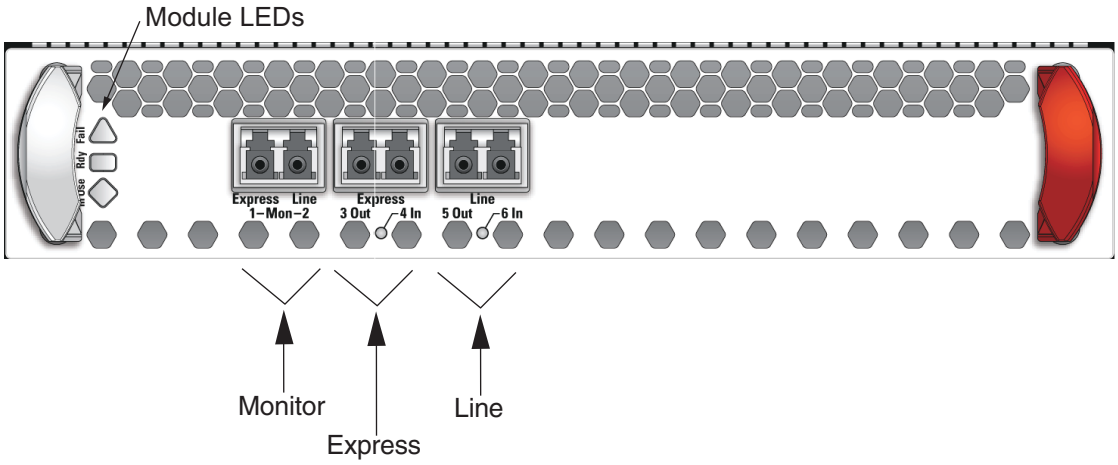
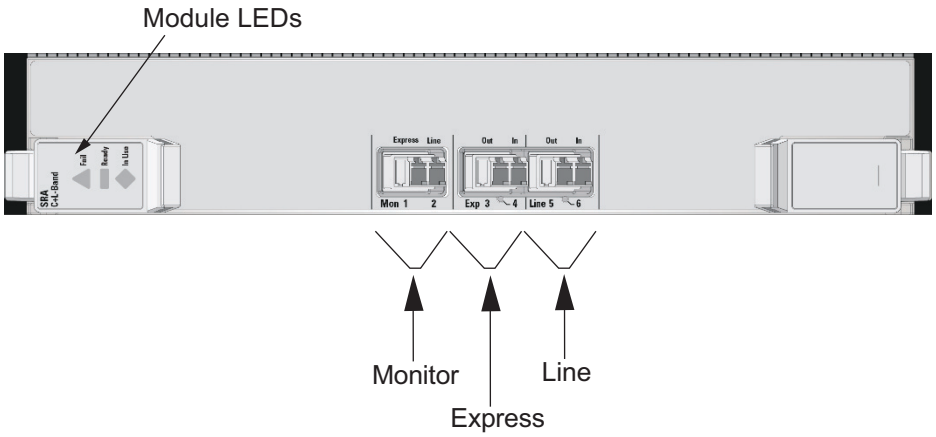


Figure 85 SRA C&L-Band module (NTK830AC variant)



Copyright© 2019-2025 Ciena® Corporation

Figure 86 SRA C&L-Band module (NTK880AC)



Copyright© 2019-2025 Ciena® Corporation

Procedure 161 Replacing a DLE or DLA module

Requirements

- observe all safety requirements described in *6500 RLS Shelf Installation Guide,* 323-2051-201
- have the correct replacement module (the replacement Product Engineering Code [PEC] is the same as the current PEC)
- have protective caps for the patchcords

CAUTION
Risk of equipment damage
Electrostatic discharge (ESD) can damage electrostatic sensitive devices. You must use antistatic protection while unpacking and installing all Field-Replaceable Units (FRU) and cables.

Overview

Use this procedure to replace the following Dual Line Equalizer (DLE) or Dual Line Amplifier (DLA) modules.

- DLE C-Band 2xSFP (NTK850DA and NTK880DA)
- DLE C&L-Band 2xSFP (NTK850DC and NTK890DC)
- DLA C-Band 2xSFP Module (NTK850BA and NTK880BA)
- DLA C&L-Band 2xSFP Module (NTK850BC and NTK890BC)

CAUTION
Service affecting procedure
Amplifier replacement is service affecting. Ensure that you have exhausted all other troubleshooting options before performing this procedure and if possible, re-route the traffic to minimize the traffic loss.

Steps

1 Check the date and time of the last backup and check whether a data backup is required. Refer to *Licensing, Security, and Administration*, 323-2051-300 for details on how to view the current backup state and how to save provisioning data.

Copyright© 2019-2025 Ciena® Corporation

2 Verify the current alarm conditions on the network element. Depending on the configuration of the node where this procedure is to be performed, the following alarms can appear throughout the network during this procedure:

- Automatic Power Reduction Active
- Automatic Shutoff
- Circuit Pack Missing
- Shutoff Threshold Crossed
- High Fiber Loss
- Optical Line Fail

3 Verify that the replacement Product Engineering Code (PEC) is the same as the current PEC.

4 Switch traffic away from this optical link by performing a protection switch at the service layer to prevent traffic loss. Refer to *Equipment/Facility Provisioning and Protection*, 323-2051-310.

5 Provision the admin state of the module to “Disabled”.

If you want to perform the procedure using	**Then** go to the
CLI commands	“CLI INTERFACE STEPS”
Node Essentials	“NODE ESSENTIALS STEPS”

CLI INTERFACE STEPS

6 The following step is performed using CLI commands.

```
set slots <slot #> config circuit-pack admin-state
<Disabled>
```

7 Go to step 13.

NODE ESSENTIALS STEPS

8 Select **Facilities** from the Node Essentials navigation menu.

The Facilities menu opens.

9 From the **Equipment** grid, select the module to be replaced.

10 Click the **Pencil** icon (Edit Equipment).

11 Set the Admin state of the equipment to Disabled.

12 Click **Confirm**.

13 Ensure that the blue LED on the module faceplate is off.

14

CAUTION
Risk of laser radiation exposure
Do not look directly into the optical beam. Invisible light can severely damage your eyes.

Copyright© 2019-2025 Ciena® Corporation

CAUTION
Risk of damage to modules
Never disconnect an optical fiber that is connected to an active or powered up optical amplifier. To disconnect or reconnect an optical fiber, make sure the optical amplifier is “Disabled”.

CAUTION
Risk of damage to modules
Wear an antistatic wrist strap to protect the equipment from static damage. Connect the wrist strap to the ESD jack on the shelf or module.

Ensure that labels are applied to both ends of all cables and optical fiber patchcords.

15 Disconnect all optical connectors from the module to be replaced.

16 Put protective caps on the ends of the patchcords to protect them from contamination and damage.

17 Push outwards on both pull tabs simultaneously and pull the module out of the slot.

18 Gently pull the module until it is fully removed from the module.

Installing the module

19 Install the replacement module into the corresponding slot and press the latches to close. For complete equipping rules and module slot numbering, refer to “Module descriptions, equipping rules, specifications” in *6500 RLS Planning Guide*, NTRN10WA.

20 Wait a few minutes for the module to initialize before you check its inventory.

21 You can retrieve the inventory data for the module you inserted.

If you want to perform the procedure using	**Then** go to the
CLI commands	“CLI INTERFACE STEPS”
Node Essentials	“NODE ESSENTIALS STEPS”

CLI INTERFACE STEPS

22 The following step is performed using CLI commands.

```
show slots <SlotNum> inventory circuit-pack [pec]
[hardware-release] [common-language-equipment-
identifier][serial-number] [manufacturing date] [power]
[diagnostic] [current-temperature] [average-
temperature]
```

23 Go to step 25.

NODE ESSENTIALS STEPS

24 Click on the **Chassis** menu and select the module you want to retrieve the inventory for.

Copyright© 2019-2025 Ciena® Corporation

The inventory information appears on the right side of the screen.

25 Clean all fiber connectors disconnected from the ports in step 15 and reconnect them to the appropriate ports on the module. For instructions on inspecting and cleaning optical fiber, refer to *Optical Connector Inspection and Cleaning*, 323-1859-500.

26 Wait for the module to start.

27 Retrieve all the active alarms and alarm details:

If you want to perform the procedure using	**Then** go to the
CLI commands	"CLI INTERFACE STEPS"
Node Essentials	See the Node Essential steps in "Retrieving the data for the active alarm object" on page 32 in this document. Then go to step 29.

CLI INTERFACE STEPS

28 The following step is performed using CLI commands.

```
show active-alarm <id> [name] [resource] [raise-time]
[raise-time] [cause] [condition-type] [direction]
[location] [severity] [service-impact] [additional-info]
[user-notes...]
```

The current alarms and alarm details will appear.

29 If the "Upgrade In Progress" alarm is active, wait until the alarm clears before continuing.

Note: It can take up to 15 minutes for this alarm to clear.

30 If the "Autoprovisioning Mismatch" alarm is active, a problem with provisioning the module has been detected.

31 Undo any traffic switches invoked in step 4.

32 Provision the admin state of the module to "Enabled".

If you want to perform the procedure using	**Then** go to the
CLI commands	"CLI INTERFACE STEPS"
Node Essentials	"NODE ESSENTIALS STEPS"

CLI INTERFACE STEPS

33 The following step is performed using CLI commands.

```
set slots <slot #> config circuit-pack admin-state
<Enabled>
```

34 Go to step 40.

NODE ESSENTIALS STEPS

35 Select **Facilities** from the Node Essentials navigation menu.

The Facilities menu opens.

Copyright© 2019-2025 Ciena® Corporation

36 From the **Equipment** grid, select the module to be replaced.

37 Click the **Pencil** icon (Edit Equipment).

38 Set the Admin state of the equipment to Enabled

39 Click **Confirm**.

40 Update the user label with the current shelf and slot.

41 Ensure there are no active alarms against the newly installed module(s).

Figure 87 DLE C-Band 2xSFP module (NTK850DA)

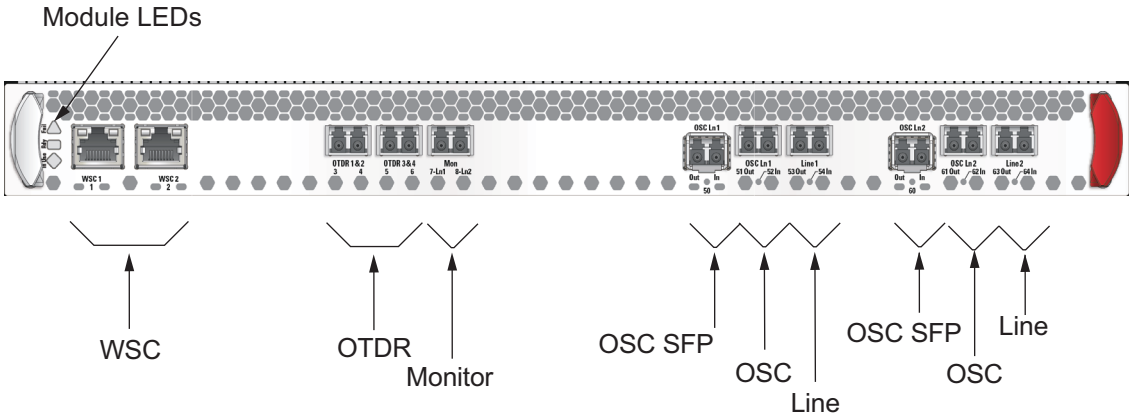
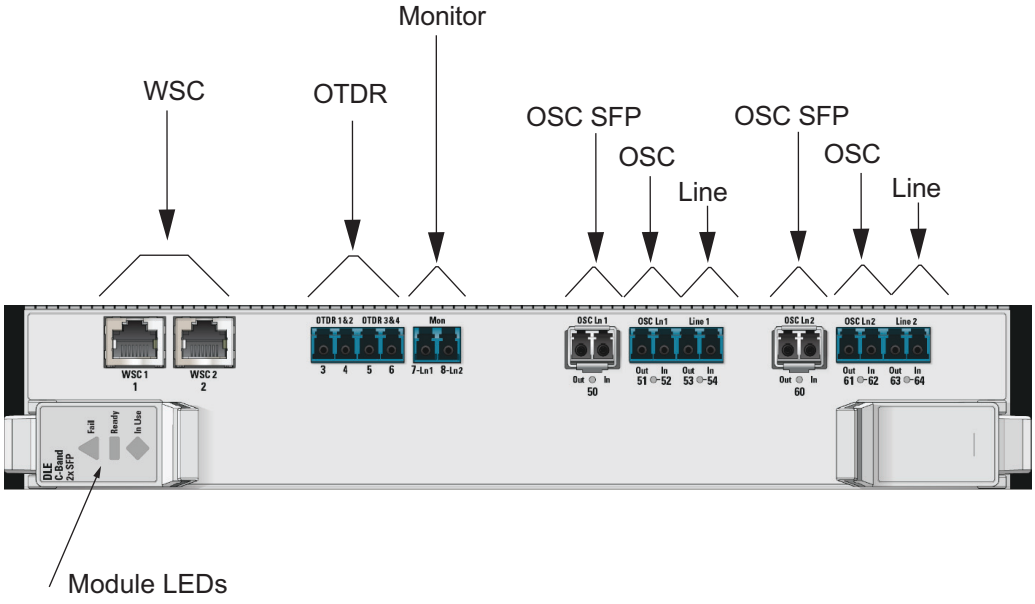


Figure 88 DLE C-Band 2xSFP module (NTK880DA)



Copyright© 2019-2025 Ciena® Corporation

Figure 89 DLE C&L-Band 2xSFP module (NTK850DC)

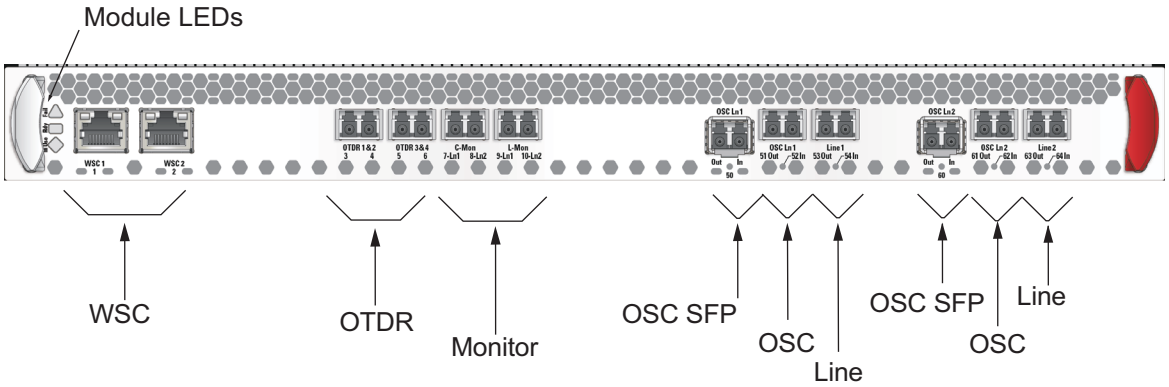
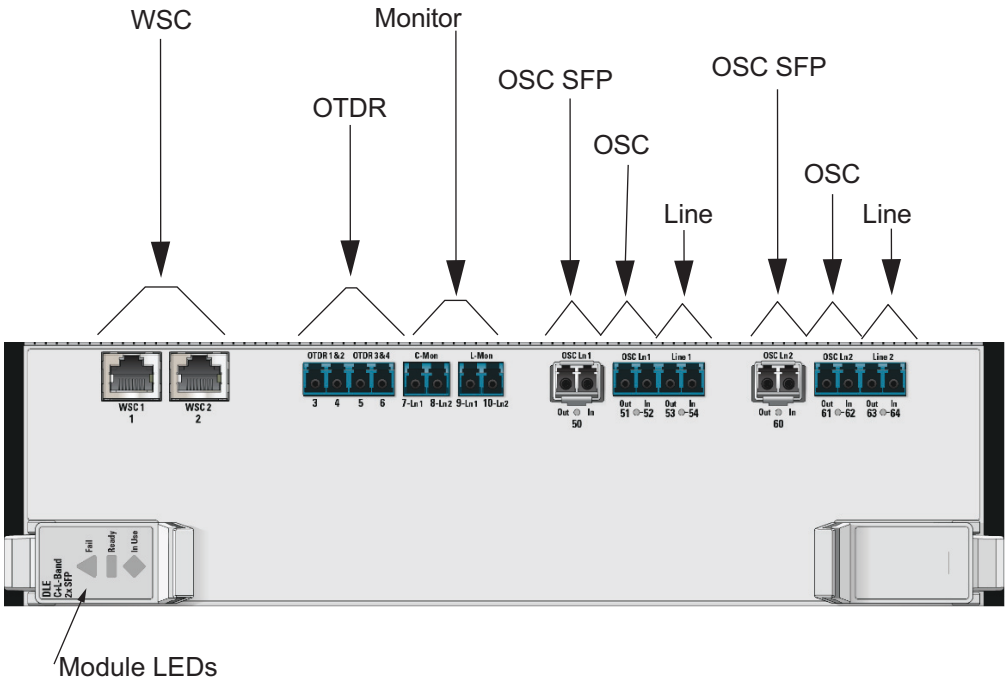


Figure 90 DLE C&L-Band 2xSFP module (NTK890DC)



Copyright© 2019-2025 Ciena® Corporation

Figure 91 DLA C-Band module (NTK850BA)

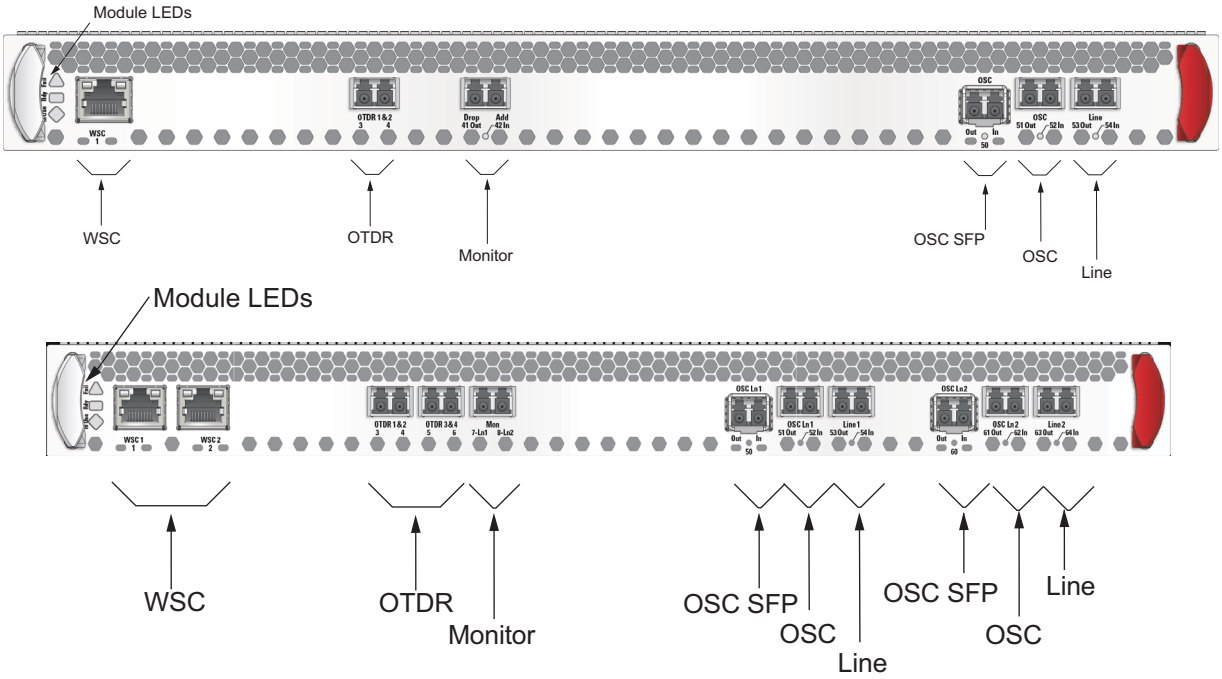
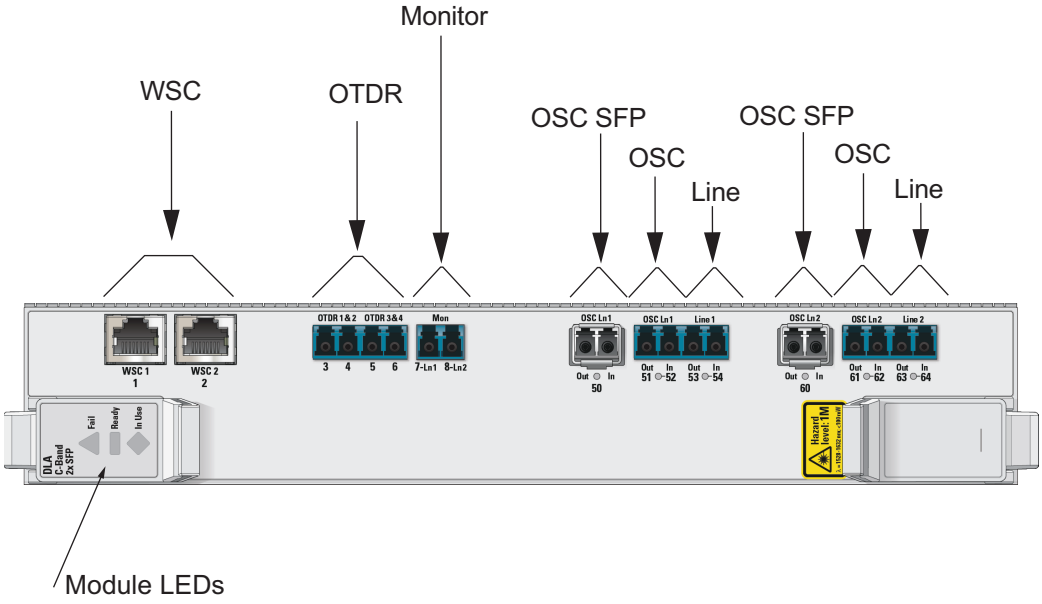


Figure 92 DLA C-Band module (NTK880BA)



Copyright© 2019-2025 Ciena® Corporation

Figure 93 DLA C&L-Band module (NTK850BC)

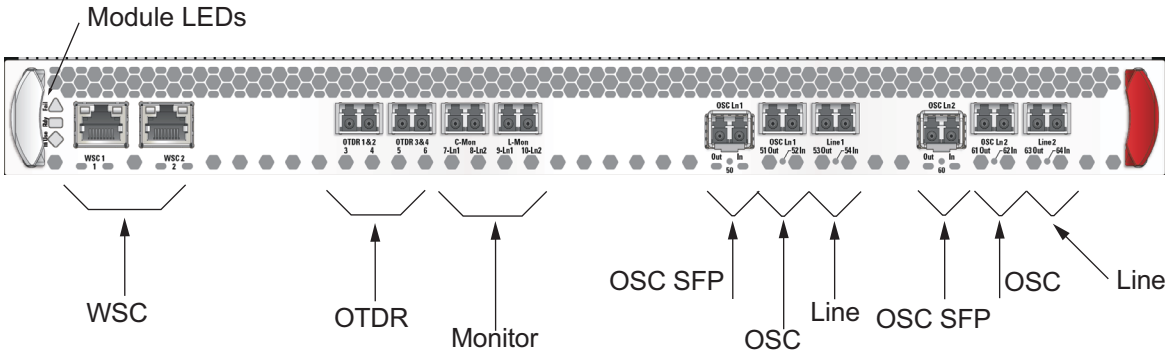
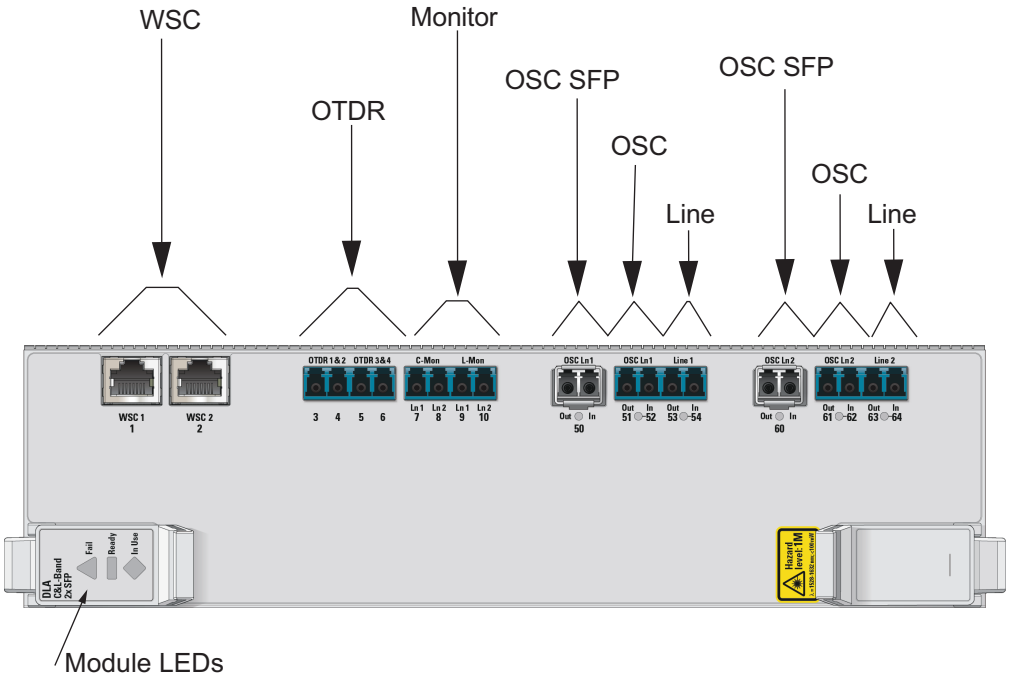


Figure 94 DLA C&L-Band module (NTK890BC)



Copyright© 2019-2025 Ciena® Corporation

Procedure 162 Replacing an OMC2 Chassis

Use this procedure to replace the 2-slot optical module chassis (OMC2) (NTK504NA) chassis

Requirements

To perform this procedure, you must:

- have a replacement OMC2. Review the “Ordering information” in *6500 RLS Planning Guide*, NTRN10WA, to make sure you select the correct PEC as the replacement part for this product platform.
- observe all safety requirements described in *6500 RLS Shelf Installation Guide,* 323-2051-201
- have the appropriate personal grounding device to dissipate electrostatic charges
- have a 3/8-in. wrench and a flathead and Phillips screwdriver

CAUTION
Risk of equipment damage
Electrostatic discharge (ESD) can damage electrostatic sensitive devices. You must use antistatic protection while unpacking and installing all Field-Replaceable Units (FRU) and cables.

Steps

Removing the OMC2

1 Identify the failed module or the module to be replaced.

2 Wear an antistatic wrist strap or foot straps to protect the shelf from static damage. If using a wrist strap, connect the wrist strap to the ESD jack on the shelf.

3 Select your next step:

If the CFIMs are	**Then**
installed in the OMC2 chassis	refer to Procedure 155, “Replacing a CFIM, UCS, or MonCS in an OMC2 chassis” procedure to remove the modules before continuing this procedure.
not installed in the OMC2	go to step 4

Copyright© 2019-2025 Ciena® Corporation

4

> **CAUTION**
> **Risk of laser radiation exposure**
> Do not look directly into the optical beam. Invisible light can severely damage your eyes.

> **CAUTION**
> **Risk of damage to modules**
> Never disconnect an optical fiber that is connected to an active or powered up optical amplifier. To disconnect or reconnect an optical fiber, make sure the optical amplifier is “Disabled”.

Locate the grounding cable location at the rear or on the side of the OMC2.

5 Use a torque wrench to detach the ground cable from the shelf.

6 Unfasten the appropriate mounting hardware that secures the OMC2 to the shelf. See Figure 95 on page 418.

7 Pull out the plunger on the right-hand side of the OMC2 chassis and pull the chassis to remove the chassis from the shelf.

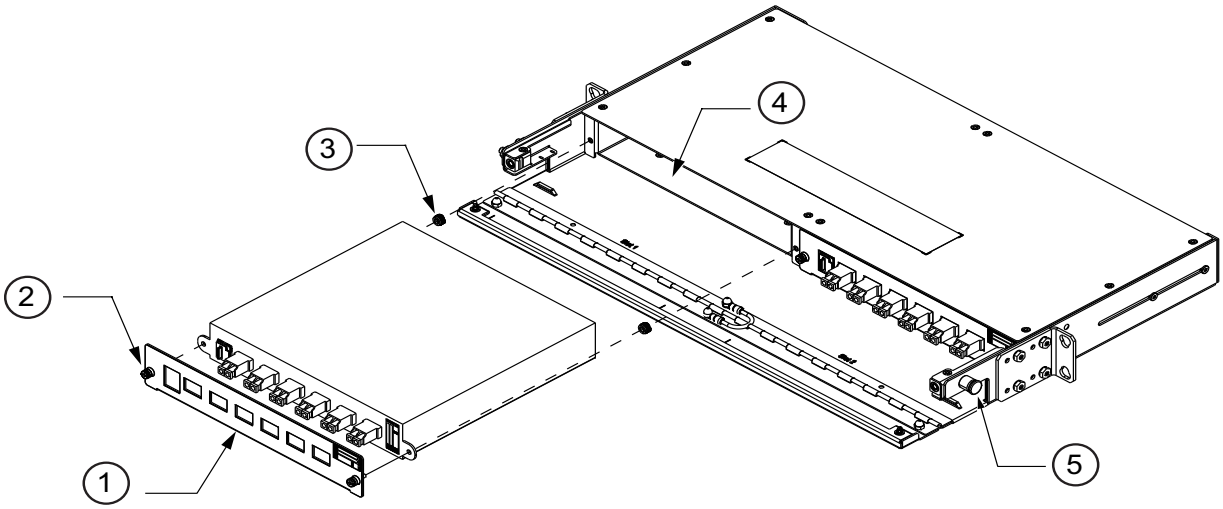
Installing the OMC2 chassis

8 Verify that the replacement PEC is the same as the current PEC.

9 Install the OMC2 into the rack. Refer to “Installing an OMC2 chassis and associated modules” in *6500 RLS Shelf Installation Guide,* 323-2051-201.

10 Ensure there are no active alarms against the newly installed module(s).

Figure 95 OMC2 module



Legend

Copyright© 2019-2025 Ciena® Corporation

1	Module faceplate	4	Chassis slot
2	Captive screw (2 places)	5	Plunger
3	Thumb nut (2 places)		

Copyright© 2019-2025 Ciena® Corporation

Procedure 163 Replacing a Trunk Protection Switch module

Use this procedure to replace a TPS Module (Trunk Protection Switch, RLS) (NTK835AA) or the TPS2 Module (Trunk Protection Switch Type 2, RLS) (NTK835BA).

Requirements

To perform this procedure, you must:

- observe all safety requirements described in *6500 RLS Shelf Installation Guide,* 323-2051-201
- have the correct replacement module (the replacement Product Engineering Code [PEC] is the same as the current PEC)
- have protective caps for the patchcords
- have a Phillips screwdriver

CAUTION
Risk of equipment damage
Electrostatic discharge (ESD) can damage electrostatic sensitive devices. You must use antistatic protection while unpacking and installing all Field-Replaceable Units (FRU) and cables.

Overview

See Figure 96 on page 422 and Figure 97 on page 422.

CAUTION
Service affecting procedure
TPS or TPS2 module replacement is service affecting. Ensure you have exhausted all other troubleshooting options before performing this procedure and if possible, reroute the traffic to minimize the traffic loss.

Steps

1 If required, backup the system database. Refer to *Licensing, Security, and Administration*, 323-2051-300 for details.

2 If not performed already, transfer all traffic currently routed through the TPS or TPS2 Module being replaced to the protection span.

All external switch requests (Manual/forced/lockout) that override default switch operation will be lost after module replacement.

3 Wear an antistatic wrist strap or foot straps to protect the shelf from static damage. If using a wrist strap, connect the wrist strap to the ESD jack on the shelf.

Copyright© 2019-2025 Ciena® Corporation

4 Ensure that the fibers are labeled properly with port and input/output designations.

5 Disconnect fiber connections from the module to be replaced.

6 Put protective dust caps on the ends of the fibers and TPS or TPS2 connectors to protect them from contamination and damage.

7 Turn the screws on each side of the TPS or TPS2 faceplate to free the module from the slot.

8 Gently pull the module using the two screws until it is fully removed from the shelf.

9 Remove the replacement module from its packaging.

10 Slide the rear of the TPS or TPS2 module into the slot.

11 Push the module until it is fully seated in the shelf.

12 Turn the screws on each side of the TPS or TPS2 faceplate to secure the module to the shelf.

13 Ensure there are no active alarms against the newly installed module(s)

14 You can retrieve the inventory data for the module you inserted.

If you want to perform the procedure using	**Then** go to the
CLI commands	“CLI INTERFACE STEPS”
Node Essentials	“NODE ESSENTIALS STEPS”

CLI INTERFACE STEPS

15 The following step is performed using CLI commands.

```
show slots <SlotNum> inventory circuit-pack [pec]
[hardware-release] [common-language-equipment-
identifier][serial-number] [manufacturing date] [power]
[diagnostic] [current-temperature] [average-
temperature]
```

16 Go to step 18.

NODE ESSENTIALS STEPS

17 Click on the **Chassis** menu and select the module you want to retrieve the inventory for.

The inventory information appears on the right side of the screen.

18 Clean and connect all fibers to the appropriate ports on the module.

Copyright© 2019-2025 Ciena® Corporation

Figure 96 TPS module

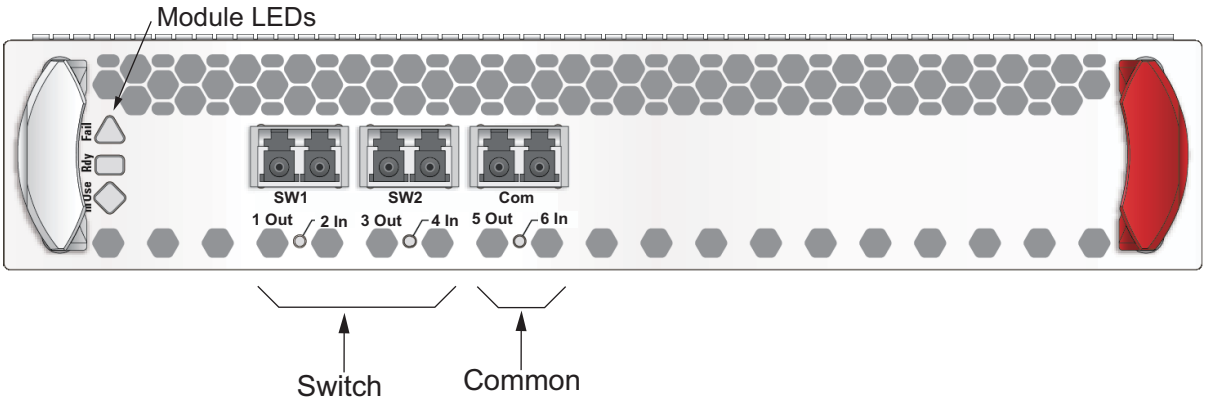
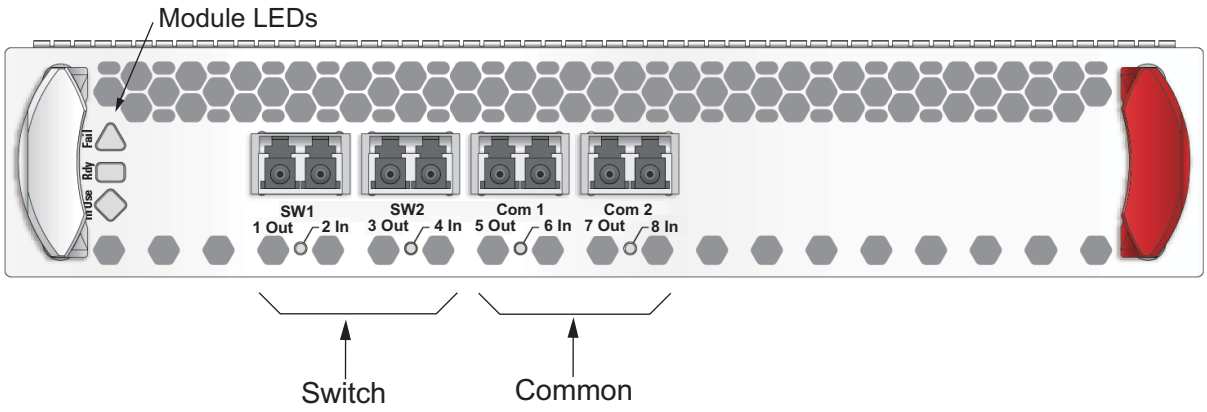


Figure 97 TPS2 module



Copyright© 2019-2025 Ciena® Corporation

6500 Reconfigurable Line System

6500 RLS Alarms and Module Replacement

Copyright© 2019-2025 Ciena® Corporation. All rights reserved.

Release 4.0
Publication: 323-2051-530
Document status: Standard
Issue 2
Document release date: May 2025

CONTACT CIENA
For additional information, office locations, and phone numbers, please visit the Ciena web site at **www.ciena.com**