



6500 Packet-Optical Platform

Fault Management - Alarm Clearing, Part 2 of 2

Release 13.0

What's inside...

[New in this release](#)

[Alarm clearing procedures—I to Z](#)

See Part 1 for the following...

[Alarm and trouble clearing strategy](#)

[Alarm surveillance](#)

[Alarm hierarchies and alarm severities](#)

[Alarm clearing procedures—A to H](#)

323-1851-543 - Standard Issue 1

September 2018

Copyright© 2010-2018 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.

Copyright© 2010-2018 Ciena® Corporation. All Rights Reserved

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		
In North America	1-800-CIENA-24 (243-6224) 410-865-4961	
In Europe, Middle East, and Africa	800-CIENA-24-7 (800-2436-2247) +44-207-012-5508 00 0800 77 454 (Slovenia)	
In Asia-Pacific	800-CIENA-24-7 (800-2436-2247) +81-3-6367-3989 +91-124-4340-600 120 11104 (Vietnam) 000 8004401369 (India)	
In Caribbean and Latin America	800-CIENA-24-7 (800-2436-2247) 1230-020-0845 (Chile) 009 800-2436-2247 (Colombia) 0800-77-454 (Mexico and Peru) 00 008000442510 (Panama)	
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 or (2) as a standalone application, and Software includes upgrades acquired by you from Ciena or a Ciena authorized reseller. 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 and only for its intended use as evidenced by the applicable product documentation. Unless the context does not permit, Software also includes associated documentation.

2. Open Source and Third Party Licenses. Software excludes any open source or third-party programs supplied by Ciena under a separate license, and you agree to be bound by the terms of any such license. If a separate license is not provided, any open source and third party programs are considered “Software” and their use governed by the terms of this License.

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.

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 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 period 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.

Contents

New in this release	xiii
Alarm clearing procedures—I to Z	5-1
Abbreviations used in this chapter	5-1
Associated procedures	5-4
List of alarms	5-5
List of procedures	
5-1 Incomplete Channel Topology	5-21
5-2 Incomplete Software Lineup	5-22
5-3 Input Loss Of Signal	5-24
5-4 Integrated Test Set Configured	5-28
5-5 Integrated Test Set Data Save In Progress	5-29
5-6 Intercard Suspected	5-30
5-7 Intercard Suspected - Pluggable	5-35
5-8 Intercard Suspected - Pluggable I/O Carrier 1/2	5-36
5-9 Internal Database Synch in Progress	5-38
5-10 Internal Mgmt Comms Suspected	5-40
5-11 Intrusion Attempt	5-42
5-12 Invalid Site Topology	5-44
5-13 I/O Module Mismatch	5-46
5-14 I/O Module Missing	5-47
5-15 I/O Module Unknown	5-48
5-16 I/O Panel Mismatch	5-50
5-17 I/O Panel Missing	5-52
5-18 I/O Panel Unknown	5-54
5-19 Isolated Station	5-56
5-20 LACP Failed	5-57
5-21 LAN alarms	5-58
5-22 Laser Failed	5-61
5-23 Laser Frequency Out Of Range	5-63
5-24 Licensing Trusted Store Mismatch	5-64
5-25 License Violation	5-65
5-26 Line A Input OTDR High Loss Detected	5-67
5-27 Line A Input OTDR High Reflection Detected	5-69
5-28 Line Adjacency Manual Provisioning Required	5-71
5-29 Line Flapping	5-72
5-30 Link Aggregation Group Fail	5-75

5-31	Link Aggregation Group Partial Fail	5-77
5-32	Link Data Retrieval In Progress	5-78
5-33	Link Data Save In Progress	5-79
5-34	Link Down	5-80
5-35	Link Pulse Missing	5-84
5-36	Local Optical Controller Disabled	5-85
5-37	Log Collection In Progress	5-86
5-38	Log Save In Progress	5-87
5-39	Loopback Active	5-88
5-40	Loopback Active - Facility	5-89
5-41	Loopback Active - Terminal	5-91
5-42	Loopback Traffic Detected	5-93
5-43	Loss of Alignment Marker	5-94
5-44	Loss of Alignment - VCAT	5-96
5-45	Loss of Channel	5-98
5-46	Loss of Clock	5-101
5-47	Loss Of Data Synch	5-105
5-48	Loss of Extra Traffic	5-109
5-49	Loss of Frame and Multiframe	5-110
5-50	Loss of Frame Delineation	5-115
5-51	Loss Of Frame, Loss Of Multiframe, or Signal Fail alarms	5-119
5-52	Loss of Lane Alignment	5-130
5-53	Loss of Lock	5-132
5-54	Loss Of Multiframe (WAN)	5-143
5-55	Loss of Multiframe - VCAT	5-144
5-56	Loss of OPU Multiframe Identifier	5-145
5-57	Loss of Pointer	5-150
5-58	Loss of Sequence - VCAT	5-153
5-59	Loss of Service Delineation	5-155
5-60	Loss Of Signal (Ethernet)	5-157
5-61	Loss Of Signal (OC/STM, ETH10G, ETH40G, ETH100G, FC, OTM1, OTM2, OTM3, OTM4, PTP, FLEX)	5-161
5-62	Loss Of Signal (OPTMON, VOA)	5-171
5-63	Loss Of Synchronization Messaging Channel	5-176
5-64	Low Optical Return Loss at Input	5-178
5-65	Low Optical Return Loss at Output	5-181
5-66	Low Order Bandwidth Near Limit	5-185
5-67	Low Received Span Loss	5-186
5-68	Low Voltage (DSM)	5-188
5-69	MAC Database Near Capacity	5-189
5-70	MAC Flapping Detected	5-190
5-71	MAC Status Defect	5-191
5-72	Manual Area Address Dropped from area	5-192
5-73	Mapping Mismatch	5-194
5-74	Max Stations Exceeded	5-197
5-75	Member Release Misaligned	5-198
5-76	Member Shelf Mismatch	5-199
5-77	Member Shelf Unknown	5-201
5-78	Member Shelf Unreachable	5-203
5-79	Minimum Gain	5-206

5-80	Modem Class Mismatch	5-208
5-81	MSI Mismatch (ODUTTP, ODUCTP, OTM0, OTM1, OTM2, OTM3, ODU0, ODU1, ODUFLEX, OTMFLEX)	5-209
5-82	Multiplexed Rate Mismatch	5-212
5-83	NE Mode Unknown	5-214
5-84	Network Trace Identifier Mismatch (FLEX)	5-215
5-85	Node ID Mismatch	5-217
5-86	Number of Level 1 NEs Exceeded	5-219
5-87	OAM Not Available	5-220
5-88	OCH Link Data Retrieval In Progress	5-223
5-89	OCH Link Data Save In Progress	5-224
5-90	ODU LCK	5-225
5-91	ODU Loss of Frame and Multiframe	5-226
5-92	ODU OCI	5-227
5-93	ODU Skew Out Of Range	5-228
5-94	ODU Signal Degrade	5-230
5-95	ODU Signal Fail	5-234
5-96	ODU/OTU Trace Identifier Mismatch	5-238
5-97	Optical Line Fail	5-242
5-98	Optimization Scanning in Progress	5-250
5-99	OPU Payload Type Mismatch	5-251
5-100	OSC Loss Of Signal	5-254
5-101	OSC RFI	5-259
5-102	OSC Signal Degrade	5-260
5-103	OSPF Adjacency Loss alarms	5-265
5-104	OSPF Max Capacity Reached	5-269
5-105	OSRP CCI Session Down	5-270
5-106	OSRP CCI Session Out of Sync	5-271
5-107	OSRP Configuration in Progress	5-272
5-108	OSRP Line Operationally Blocked	5-273
5-109	OSRP Node Operationally Blocked	5-275
5-110	OSRP Port Capability Mismatch	5-277
5-111	OTDR Trace In Progress	5-278
5-112	OTL Skew Out Of Range	5-279
5-113	OTS Provisioning Error	5-281
5-114	OTU Signal Degrade	5-287
5-115	OTU Signal Fail (OTM, OTM2, OTUTTP)	5-291
5-116	Output Loss Of Signal	5-294
5-117	Packet Configuration Integrity Fail	5-297
5-118	Packet Rate Limit Exceeded	5-300
5-119	Packet Rate Limit Exceeded - CPU2	5-301
5-120	Payload Extended Label Mismatch	5-302
5-121	Payload Label Mismatch	5-304
5-122	PHY Map Mismatch	5-306
5-123	Pluggable I/O Carrier 1/2 Fail	5-307
5-124	Pluggable I/O Carrier 1/2 Missing	5-308
5-125	Pluggable I/O Carrier 1/2 Unknown	5-309
5-126	Pluggable I/O Panel Mismatch	5-310
5-127	Pluggable I/O Panel Missing	5-311
5-128	Pluggable I/O Panel Unknown	5-313

5-129	Port Bandwidth Near Limit	5-315
5-130	Power Failure	5-317
5-131	Power Failure - A or Power Failure - B	5-319
5-132	Power Failure - A (DSM) or Power Failure - B (DSM)	5-323
5-133	Power Failure - Fuse Blown	5-325
5-134	Power Failure - Low Voltage	5-328
5-135	Pre-FEC Signal degrade	5-330
5-136	Pre-FEC Signal Fail	5-333
5-137	Primary License Server Unavailable	5-335
5-138	Primary RADIUS Accounting Server Unavailable	5-336
5-139	Primary RADIUS Server Unavailable	5-338
5-140	Primary Shelf Unreachable	5-340
5-141	Protection Default K-bytes	5-343
5-142	Protection Exerciser Failed	5-345
5-143	Protection Exerciser Failed Protection	5-348
5-144	Protection Exerciser Failed Working	5-352
5-145	Protection Invalid K-bytes	5-358
5-146	Protection Locked	5-361
5-147	Protection Mode Mismatch	5-362
5-148	Protection Scheme Mismatch	5-364
5-149	Protection Sub-module Mismatch	5-365
5-150	Protection Sub-module Missing	5-367
5-151	Protection Sub-module Unknown	5-369
5-152	Protection Switch Active alarms	5-370
5-153	Protection Switch Complete	5-376
5-154	Protection Switch Complete - Revertive	5-379
5-155	Provisioning Database Freeze Enable	5-381
5-156	Provisioning Incompatible	5-382
5-157	Provisioning Incompatible - Pluggable	5-385
5-158	Provisioning Mismatch	5-387
5-159	Reach Violation	5-388
5-160	RAMAN Failed To Turn On	5-389
5-161	Redundant Database Synch Failed	5-391
5-162	Redundant Database Synch Failed - CP	5-393
5-163	Redundant Database Synch in Progress	5-395
5-164	Redundant Release Synch Failed	5-396
5-165	Redundant Release Synch in Progress	5-397
5-166	Release Server Mismatch	5-398
5-167	Release Server URL Fail	5-399
5-168	Remote Alarm Indication	5-400
5-169	Remote CCM Error	5-402
5-170	Remote Client Circuit Pack Failed - Pluggable	5-404
5-171	Remote Client Circuit Pack Missing - Pluggable	5-405
5-172	Remote Client Circuit Pack Unknown - Pluggable	5-406
5-173	Remote Client High Received Optical Power	5-407
5-174	Remote Client Link Down	5-409
5-175	Remote Client Low Received Optical Power	5-412
5-176	Remote Defect Indication	5-414
5-177	Remote Invalid Configuration	5-417
5-178	Remote Inventory Not Supported	5-419

5-179	Remote Line High Received Optical Power	5-421
5-180	Remote Line Low Received Optical Power	5-423
5-181	Remote Loopback Active	5-425
5-182	Remote Loopback Fail	5-426
5-183	Remote Node Unreachable	5-428
5-184	Remote Port OOS	5-432
5-185	Remote Port Unreachable	5-433
5-186	Remote Power Fail Indication	5-435
5-187	Remote Power Supply 1/2 Missing	5-436
5-188	Remote Receiver Fail	5-437
5-189	Resources Above Threshold	5-439
5-190	Resources At Limit	5-440
5-191	Ring Failure	5-441
5-192	Ringlet Failure	5-443
5-193	Ring Protection Exerciser Failed	5-445
5-194	Ring Protection Switch Complete	5-448
5-195	Ring Protection Switch Fail	5-449
5-196	Rollover in Progress	5-451
5-197	Root Directory Has Reached Maximum File Entry Limit	5-452
5-198	Rx Channel Power Out of Range	5-453
5-199	Rx Ethernet Idle	5-456
5-200	Rx Partial Loss of Capacity - LCAS	5-457
5-201	Rx Power Out of Range	5-458
5-202	Rx Total Loss of Capacity - LCAS	5-461
5-203	Secondary alarms	5-463
5-204	Secondary License Server Unavailable	5-475
5-205	Secondary RADIUS Accounting Server Unavailable	5-476
5-206	Secondary RADIUS Server Unavailable	5-478
5-207	Secondary Service Failed	5-479
5-208	Secondary SETS Locking to Primary	5-481
5-209	Server Certificate About to Expire (6500)	5-483
5-210	Server Certificate Expired (6500)	5-484
5-211	Service Defect Indication	5-485
5-212	Service Mismatch	5-489
5-213	Shelf Bandwidth Near Limit	5-490
5-214	Shelf Data Missing	5-491
5-215	Shelf Power Near Limit	5-492
5-216	Shutoff Threshold Crossed	5-494
5-217	Site Provisioning Required (DSM)	5-497
5-218	Skew Out Of Range	5-498
5-219	SLDD Adjacency Loss	5-500
5-220	Slot Empty	5-501
5-221	Slot Sequence Provisioning Incomplete	5-502
5-222	SNC Datapath Fault	5-503
5-223	SNCG Not On Home Path	5-505
5-224	SNCG Unavailable	5-507
5-225	SNC Not On Home Path	5-509
5-226	SNC Reservation Unavailable	5-511
5-227	SNC Takeover Failed	5-512
5-228	SNC Unavailable	5-515

- 5-229 Software Auto-Upgrade in Progress 5-517
- 5-230 Software Configuration Unknown 5-518
- 5-231 Software Delivery Incomplete 5-519
- 5-232 Software Delivery in Progress 5-520
- 5-233 Software Mismatch 5-521
- 5-234 Software Subsystem Failed 5-522
- 5-235 Software Subsystem Restart 5-524
- 5-236 Software Upgrade Failed 5-525
- 5-237 Software Upgrade in Progress 5-526
- 5-238 Span protection Switch Complete 5-527
- 5-239 Span protection Switch Fail 5-528
- 5-240 Span Protection Exerciser Fail 5-529
- 5-241 Switch Shelf ID Mismatch Detected 5-531
- 5-242 Synchronization Protection alarms 5-532
- 5-243 TACACS Server 1/2 Unavailable 5-534
- 5-244 Tamper Detected 5-535
- 5-245 Target Unachievable 5-537
- 5-246 TCM Loss of Tandem Connection 5-539
- 5-247 Telemetry Loss of Signal 5-540
- 5-248 Test Access in Progress alarms 5-542
- 5-249 Threshold AIS ESO-A/ESO-B 5-544
- 5-250 Time Out 5-549
- 5-251 Timing Distribution Loss of Reference - n Ref 5-551
- 5-252 Timing Generation Entry to Freerun 5-553
- 5-253 Timing Generation Entry to Holdover 5-557
- 5-254 Timing Generation Failure To Lock 5-560
- 5-255 Timing Generation Loss of Reference - n Ref 5-562
- 5-256 TOD Server Not Provisioned 5-565
- 5-257 TODR Reversion Inhibited 5-567
- 5-258 TOD Threshold Exceeded 5-568
- 5-259 Topology Build Failed 5-569
- 5-260 Topology Failure 5-570
- 5-261 Topology Instability 5-571
- 5-262 Trace Identifier Mismatch (OCn/STMn) 5-572
- 5-263 Trace Identifier Mismatch (STS/HO VC and VT/LO VC) 5-575
- 5-264 Traffic Squelched 5-578
- 5-265 Transport Data Recovery Failed 5-580
- 5-266 TR Control Disabled 5-582
- 5-267 TR Control Echo Trace Mismatch 5-583
- 5-268 TR Control Initialization in Progress 5-585
- 5-269 TR Control IS Optimization in Progress 5-587
- 5-270 Tributary Slots Not Available 5-588
- 5-271 Tx AIS (DS1) 5-589
- 5-272 Tx AIS (DS3/E3) 5-591
- 5-273 Tx Frequency Out of Range 5-593
- 5-274 Tx Loss of Frame (DS1) 5-594
- 5-275 Tx Loss of Frame (DS3/E3) 5-596
- 5-276 Tx Loss Of Signal 5-599
- 5-277 Tx Manual Provisioning Required 5-601
- 5-278 Tx Partial Loss of Capacity - LCAS 5-602

-
- 5-279 Tx Power In Reduced State 5-604
 - 5-280 Tx Power Out of Range 5-606
 - 5-281 Tx Remote Alarm Indication 5-609
 - 5-282 Tx Remote Defect Indication 5-611
 - 5-283 Tx Total Loss of Capacity - LCAS 5-613
 - 5-284 TX Tuning in Progress 5-615
 - 5-285 Unable to Synchronize TOD 5-616
 - 5-286 Unassigned Channel Detected 5-618
 - 5-287 Unequipped 5-620
 - 5-288 Unpaired SSH Key 5-623
 - 5-289 Unsupported Channel Provisioned 5-624
 - 5-290 Validation Certificate About to Expire 5-625
 - 5-291 Validation Certificate Expired 5-626
 - 5-292 VOA Output LOS 5-627
 - 5-293 VT-STS bandwidth near limit 5-628
 - 5-294 Warm Restart Required 5-630
 - 5-295 Wavelength Measurement Error 5-631
 - 5-296 Wavelength Measurement Warning 5-632
 - 5-297 WAYSIDE 1/2 Port Failure 5-633

New in this release

This Technical Publication supports 6500 Packet-Optical Platform (6500) Release 13.0 software and subsequent maintenance releases for Release 13.0.

ATTENTION

This document is presented in two parts: Part 1 and Part 2. Each part has its own table of contents. The table of contents in Part 1 contains topics found in Part 1 only. The table of contents in Part 2 contains topics found in Part 2 only.

You are reading Part 2 of *Fault Management - Alarm Clearing* 323-1851-543. The following section details what's new in *Fault Management - Alarm Clearing, Part 2 of 2*, 323-1851-543, Standard Issue 1 for Release 13.0.

Issue 1

The following new/enhanced features are covered in this document.

- New Hardware
 - X-Conn 800G PTS 1xQSFP28/2xSFP+
 - PTS PDH I/F 2xDIM
 - PTS MRO I/F 2xSFP+/14xSFP

New/Changed alarm procedures

The following table lists the new and changed alarm procedures for Release 13.0 in this document.

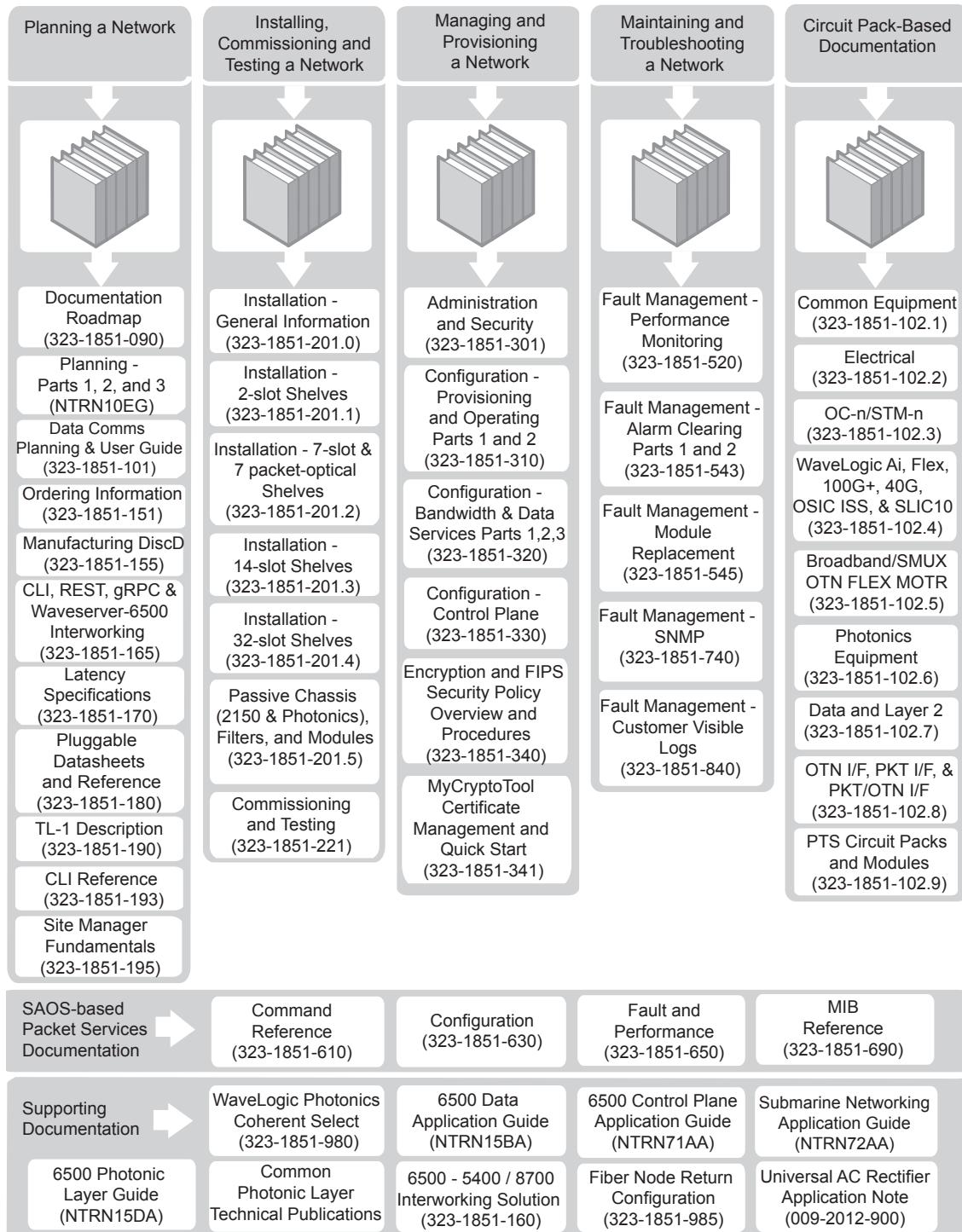
Alarm name	New/Changed
Link Down	Changed
Loopback Active - Terminal	Changed
Loss Of Data Synch	Changed
Loss Of Frame, Loss Of Multiframe, or Signal Fail alarms	Changed
Loss of Pointer	Changed

Alarm name	New/Changed
Payload Label Mismatch	Changed
Pre-FEC Signal degrade	Changed
Pre-FEC Signal Fail	Changed
Remote Alarm Indication	New
Resources Above Threshold	New
Resources At Limit	New
Secondary alarms	Changed
Service Defect Indication	Changed
Software Subsystem Restart	New
Trace Identifier Mismatch (STS/HO VC and VT/LO VC)	Changed
Unequipped	Changed

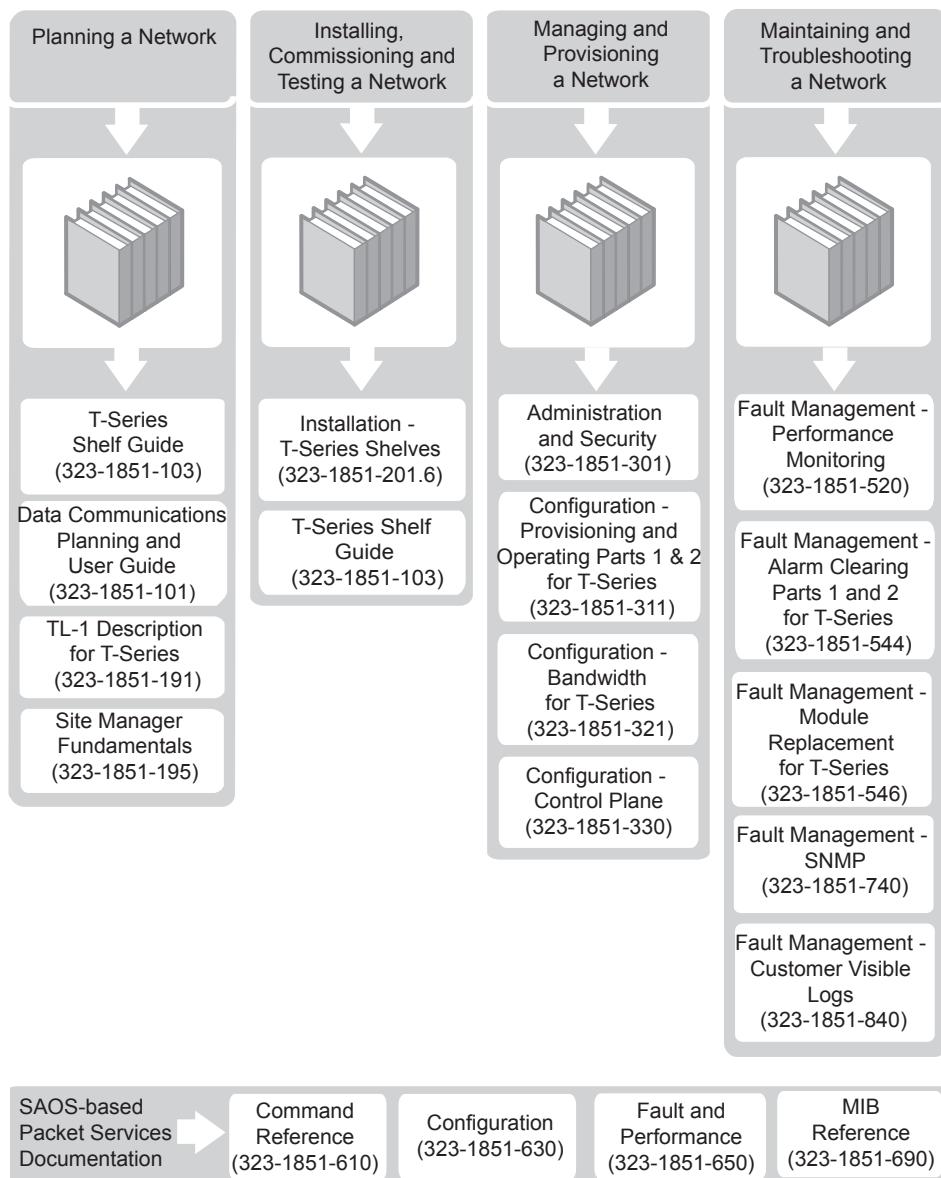
6500 technical publications

The following two roadmaps identify the technical publications that support the 6500 D-Series and S-Series and the technical publications that support the 6500 T-Series platform for Release 13.0.

6500 D-Series and S-Series roadmap



6500 T-Series roadmap



Alarm clearing procedures—I to Z

ATTENTION

The alarm clearing procedures are presented in two chapters, “Alarm clearing procedures—A to H” and “Alarm clearing procedures—I to Z”. The complete “List of alarms” is included in both chapters.

The 6500 Packet-Optical Platform (6500) shelf offers the following services in this release:

- Multi-service provisioning platform (MSPP) services
- Broadband services
- Photonic services
- Converged MSPP and Broadband services
- Converged Broadband and Photonic services
- PKT/OTN transport and switched services

For more information on the services (and the circuit packs related to each service) offered in this release, refer to the Introduction chapter in Part 1 of *6500 Planning*, NTRN10EG.

This chapter provides procedures for clearing single and generic alarms. Generic procedures are used for clearing more than one alarm type.

A complete list of alarms is provided. Refer to the “[List of alarms](#)” on page 5-5 to determine whether you must perform a specific or a generic alarm clearing procedure to clear the alarm.

Abbreviations used in this chapter

AIS	Alarm Indication Signal
ALS	Automatic Laser Shutdown
AMP	Amplifier
APR	Automatic Power Reduction

5-2 Alarm clearing procedures—I to Z

APS	Automatic Protection Switching
BDI	Backward Defect Indication
CDC	Colorless Directionless Contentionless
CFM	connectivity fault management
CHMON	Channel Monitoring
CMF	Client Management Frame
CP	Circuit Pack
CPE	Customer Premise Equipment
CTM	Control timing module
DCN	Data Communications Network
DIM	distributed I/O modules
DOC	Domain Optical Controller
DUS	Do not Use for Synchronization
DWDM	Dense Wavelength Division Multiplexing
EDP	Engineering Documentation Package
ES	Errored Second
ESD	Electrostatic Discharge
ESI	External Synchronization Input
ESO	External Synchronization Output
FEC	Forward Error Correction
FIM	Fiber Interconnect Module
FPGA	Field Programmable Gate Array
GCC	General Communication Channel
GFP-F	Generic Framing Procedure - Framed
HO	High Order
IS	In-Service
iVLLI	Inverse Virtual Link Loss Indicator
LAN	Local Area Network

LED	Light-Emitting Diode
LO	Low Order
LOFEF	Laser Off Far-End Fail
LOF	Loss of Frame
LOS	Loss of Signal
LSP	Label switched path
MPLS	Multiprotocol Label Switching
NNS	Network Name Server
NSA	Non-Service-Affecting
OBB	Optical Broadcast & Bridge
OBMD 1x8	Optical Broadband Mux/Demux
OBM	Optical Bandwidth Manager
OC	Optical Carrier
OCI	Optical Channel Interface
ODU	Optical Channel Data Unit
OOS	Out-of-Service
OPU	Optical Channel Payload Unit
OPM	Optical Power Monitor
OSC	Optical Service Channel
OSI	Open Systems Interconnection
OSNR	Optical Signal to Noise ratio
OST	Optical System Topology
OTDR	Optical Time Domain Reflectometer
OTN	Optical Transport Network
OTU	Optical Channel Transport Unit
PEC	Product Engineering Code
PSI	Payload Structure Identifier
PTS	Packet Transport System

RLA	ROADM with Line Amplifier
ROADM	Re-configurable Optical Add-Drop Multiplexer
SA	Service-Affecting
SD	Signal Degrade
SETS	Synchronization Equipment Timing Source
SLA	Single Line Amplifier
SLAT	System Lineup and Test
SNCP	Subnetwork Connection Protection
SONET	Synchronous Optical Network
SP	Shelf Processor
SPLI	Service Photonic Layer Interoperability
SSH	Secure Shell Protocol
SSM	Synchronization Status Message
SSU	Synchronization Supply Unit
STM	Synchronous Transport Module
SWT	Shelf Wavelength Topology
TOD	Time of Day
TTI	Trail Trace Identifier
UNI	Unidirectional
UPI	User Payload Identifier
UPC	User Privilege Code
VLLI	Virtual Link Loss Indicator
WAN	Wide Area Network
WSS w/OPM	Wavelength Selective Switch with Optical Power Monitor

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 in to the network element. Refer to the “Interface login and logout” procedures in *Administration and Security*, 323-1851-301.

List of alarms

The complete list of alarms is included here. However, the alarm clearing procedures are presented in two parts (A to H and I to Z). The alarm clearing procedures beginning with I to Z are included in this chapter. Additionally, non-hyperlinked references to procedures beginning with A to H (included in Part 1 of this document) are provided here.

A

- 1+1 APS, see Part 1 of this document
- Adjacency Discovery Unreliable, see Part 1 of this document
- Adjacency Far End Not Discovered, see Part 1 of this document
- Adjacency Mismatch, see Part 1 of this document
- Adjacency Provisioning Error, see Part 1 of this document
- AIS (ESI), see Part 1 of this document
- [“AIS \(OTUTTP, STTP, PATH, PDH\)”, see “Secondary alarms” on page 5-463](#)
- Alarm Provisioning Near Limit, see Part 1 of this document
- All License Servers Unavailable, see Part 1 of this document
- All Provisioned RADIUS Accounting Servers Unavailable, see Part 1 of this document
- All Provisioned RADIUS Servers Unavailable, see Part 1 of this document
- All Provisioned TACACS Servers Unavailable, see Part 1 of this document
- ALS Disabled, see Part 1 of this document
- ALS Triggered - Laser is shutdown, see Part 1 of this document
- Automatic Power Reduction Active, see Part 1 of this document
- Automatic Shutoff, see Part 1 of this document
- Automatic Shutoff Compromised, see Part 1 of this document
- Automatic Shutoff Disabled, see Part 1 of this document
- Auto Protection Switch Acknowledge Time Out, see Part 1 of this document
- Autoprovisioning Mismatch, see Part 1 of this document
- Autoprovisioning Mismatch - Pluggable, see Part 1 of this document
- AutoRoute Configuration Mismatch, see Part 1 of this document

B

Backplane ID Module 1/2 Failed, see Part 1 of this document
Bandwidth Oversubscribed, see Part 1 of this document
Battery Low, see Part 1 of this document
BW Lockout Configured, see Part 1 of this document

C

Cable Degrade, see Part 1 of this document
Cable Failure, see Part 1 of this document
Cable Not Connected, see Part 1 of this document
Cable Trace Compromised, see Part 1 of this document
Calibration Required, see Part 1 of this document
CCM Error, see Part 1 of this document
Certificate About to Expire, see Part 1 of this document
Certificate Expired, see Part 1 of this document
Channel Contention, see Part 1 of this document
Channel Controller: Failure Detected, see Part 1 of this document
Channel Controller: Unexpected Loss Detected, see Part 1 of this document
Channel Degrade, see Part 1 of this document
Channel Opacity Error, see Part 1 of this document
Circuit Pack Configuration Save Failed, see Part 1 of this document
Circuit Pack Failed, see Part 1 of this document
Circuit Pack Failed - Pluggable, see Part 1 of this document
Circuit Pack Failed-Sync, see Part 1 of this document
Circuit Pack Latch Open, see Part 1 of this document
Circuit Pack Mate Mismatch, see Part 1 of this document
Circuit Pack Mismatch, see Part 1 of this document
Circuit Pack Mismatch - Pluggable, see Part 1 of this document
Circuit Pack Missing, see Part 1 of this document
Circuit Pack Missing - Pluggable, see Part 1 of this document
Circuit Pack 3rd Party - Pluggable, see Part 1 of this document
Circuit Pack Operational Capability Exceeded, see Part 1 of this document
Circuit Pack Powered Down, see Part 1 of this document
Circuit Pack Unknown, see Part 1 of this document

Circuit Pack Unknown - Pluggable, see Part 1 of this document
Circuit Pack Upgrade Failed, see Part 1 of this document
Client Service Mismatch, see Part 1 of this document
CMF UPI Mismatch, see Part 1 of this document
[“COLAN-A OSPF Adjacency Loss”](#), see “[OSPF Adjacency Loss alarms](#)” on page 5-265
[“COLAN-A Port Failure”](#), see “[LAN alarms](#)” on page 5-58
[“COLAN-X OSPF Adjacency Loss”](#), see “[OSPF Adjacency Loss alarms](#)” on page 5-265
[“COLAN-X Port Failure”](#), see “[LAN alarms](#)” on page 5-58
Cold Restart Required, see Part 1 of this document
Connectivity Mismatch, see Part 1 of this document
Config Mismatch - LCAS, see Part 1 of this document
Configuration Mismatch, see Part 1 of this document
Configuration Mismatch - Adv BW Limit, see Part 1 of this document
Configuration Mismatch - BW Lockout, see Part 1 of this document
Configuration Mismatch - BW Threshold, see Part 1 of this document
Configuration Mismatch - Common ID, see Part 1 of this document
Configuration Mismatch - Concatenation, see Part 1 of this document
Configuration Mismatch - Link ID, see Part 1 of this document
Configuration Mismatch - Node, see Part 1 of this document
Configuration Mismatch - OVPN ID, see Part 1 of this document
Configuration Mismatch - Primary State, see Part 1 of this document
Control Mode Conversion Failed, see Part 1 of this document
Control Mode Conversion in Progress, see Part 1 of this document
Control Mode Provisioning mismatch, see Part 1 of this document
Control Plane Operations Blocked, see Part 1 of this document
Control Plane System mismatch, see Part 1 of this document
Co-Routed SNC Degraded, see Part 1 of this document
Co-Routed SNC Unavailable, see Part 1 of this document
Corrupt Inventory Data, see Part 1 of this document
CPE Discovery Protocol Fail, see Part 1 of this document
CP Loss of Host Timing Ref., see Part 1 of this document
Craft Load Missing, see Part 1 of this document

Craft Load Unpacking Aborted - Low Disk Space, see Part 1 of this document

Cross-connection Mismatch, see Part 1 of this document

Cross connect Error, see Part 1 of this document

Crossed Fibers Suspected, see Part 1 of this document

D

Dark Fiber Loss Measurement Disabled, see Part 1 of this document

Database Auto Save in Progress, see Part 1 of this document

Database Integrity Fail, see Part 1 of this document

Database Not Recovered For Slot, see Part 1 of this document

Database Recovery Incomplete, see Part 1 of this document

Database Restore in Progress, see Part 1 of this document

Database Save Failed, see Part 1 of this document

Database Restore Failed, see Part 1 of this document

Database Commit Failed, see Part 1 of this document

Database Save in Progress, see Part 1 of this document

DCC Link Fail alarms, see Part 1 of this document

Debug Port in Use, see Part 1 of this document

Delay Measurement Enabled on Slave Node, see Part 1 of this document

Delay Measurement Failed, see Part 1 of this document

Delay Measurement Mismatch Capability, see Part 1 of this document

Deskew Fail, see Part 1 of this document

Deskew Out Of Range, see Part 1 of this document

Disk 75 percent Full, see Part 1 of this document

Disk 90 percent Full, see Part 1 of this document

Disk Full, see Part 1 of this document

DOC Action: Channel Add In Progress, see Part 1 of this document

DOC Action: Channel Delete In Progress, see Part 1 of this document

DOC Action Failed: Add, see Part 1 of this document

DOC Action Failed: Delete, see Part 1 of this document

DOC Action Failed: Monitor, see Part 1 of this document

DOC Action Failed: Optimize, see Part 1 of this document

DOC Action: Fault Detected, see Part 1 of this document

DOC Consecutive Re-Opt Threshold Crossed, see Part 1 of this document

DOC Domain Not Optimized, see Part 1 of this document

DOC Invalid Photonic Domain, see Part 1 of this document

DOC Power Audit Failed, see Part 1 of this document

Domain Optical Controller Disabled, see Part 1 of this document

Dormant Account Detected, see Part 1 of this document

Duplicate Adjacency Discovered, see Part 1 of this document

Duplicate IP Address, see Part 1 of this document

Duplicate IPv6 Address, see Part 1 of this document

Duplicate Primary Shelf, see Part 1 of this document

Duplicate Shelf Detected, see Part 1 of this document

Duplicate Site ID, see Part 1 of this document

E

Equipment Configuration Mismatch, see Part 1 of this document

Equipment OOS with Subtending Facilities IS, see Part 1 of this document

Equipment Reconfiguration In Progress, see Part 1 of this document

Error alarms (ETTP), see Part 1 of this document

Error alarms (STTP), see Part 1 of this document

ESI alarms, see Part 1 of this document

Event Log full, see Part 1 of this document

Excessive Error Rate (ESI), see Part 1 of this document

Excessive Input Power, see Part 1 of this document

F

Facility Provisioning Failure, see Part 1 of this document

Facility Reconfiguration In Progress, see Part 1 of this document

Facility Reconfiguration Required, see Part 1 of this document

Fan Failed, see Part 1 of this document

Fan Missing, see Part 1 of this document

Fan Incompatible, see Part 1 of this document

Far End Client Signal Fail, see Part 1 of this document

Far End Protection Line Fail, see Part 1 of this document

Fiber Loss Detection Disabled, see Part 1 of this document

Fiber Type Manual Provisioning Required, see Part 1 of this document

Filter Replacement Timer Expired, see Part 1 of this document
Flash Banks Mismatch, see Part 1 of this document
Flash FPGA baseline unsupported, see Part 1 of this document
[“Forced Switch Active”](#), see “[Protection Switch Active alarms](#)” on page 5-370
Frequency Out of Range (ETTP, STTP), see Part 1 of this document
Frequency Provisioning Mismatch, see Part 1 of this document

G

Gauge Threshold Crossing Alert Summary, see Part 1 of this document
GCC0/GCC1/GCC2 Link Fail, see Part 1 of this document
GCC0/GCC1/GCC2 OSPF Adjacency Loss, see “[OSPF Adjacency Loss alarms](#)” on page 5-265
GID Mismatch (6500), see Part 1 of this document

H

Hardware Subsystem Failed, see Part 1 of this document
High Fiber Loss, see Part 1 of this document
High Optical Power, see Part 1 of this document
High received Span Loss, see Part 1 of this document
High Temperature, see Part 1 of this document
High Temperature Warning, see Part 1 of this document
Home Path Not defined, see Part 1 of this document

I

“ILAN-IN OSPF Adjacency Loss”, see “[OSPF Adjacency Loss alarms](#)” on page 5-265
“ILAN-IN Port Failure”, see “[LAN alarms](#)” on page 5-58
“ILAN-OUT OSPF Adjacency Loss”, see “[OSPF Adjacency Loss alarms](#)” on page 5-265
“ILAN-OUT Port Failure”, see “[LAN alarms](#)” on page 5-58
“Incomplete Channel Topology” on page 5-21
“Incomplete Software Lineup” on page 5-22
“Input Loss Of Signal” on page 5-24
“Integrated Test Set Configured” on page 5-28
“Integrated Test Set Data Save In Progress” on page 5-29
“Intercard Suspected” on page 5-30
“Intercard Suspected - Pluggable” on page 5-35

“Internal Database Synch in Progress” on page 5-38
“Internal Mgmt Comms Suspected” on page 5-40
“Intrusion Attempt” on page 5-42
“Invalid Site Topology” on page 5-44

L

“LACP Failed” on page 5-57
“LAN alarms” on page 5-58
“LAN Link Failure”, see “LAN alarms” on page 5-58
“Laser Frequency Out Of Range” on page 5-63
“Licensing Trusted Store Mismatch” on page 5-64
“License Violation” on page 5-65
“Line A Input OTDR High Loss Detected” on page 5-67
“Line A Input OTDR High Reflection Detected” on page 5-69
“Line Adjacency Manual Provisioning Required” on page 5-71
Line DCC Link Failure, see DCC Link Fail alarms in Part 1 of this document
“Line Flapping” on page 5-72
“LINE/MS DCC OSPF Adjacency Loss”, see “OSPF Adjacency Loss alarms” on page 5-265
“Link Aggregation Group Fail” on page 5-75
“Link Aggregation Group Partial Fail” on page 5-77
“Link Data Retrieval In Progress” on page 5-78
“Link Data Save In Progress” on page 5-79
“Link Down” on page 5-80
“Link Pulse Missing” on page 5-84
“Local Optical Controller Disabled” on page 5-85
“Lockout Active”, see “Protection Switch Active alarms” on page 5-370
“Log Collection In Progress” on page 5-86
“Log Save In Progress” on page 5-87
“Loopback Active” on page 5-88
“Loopback Active - Facility” on page 5-89
“Loopback Active - Terminal” on page 5-91
“Loopback Traffic Detected” on page 5-93
“Loss of Alignment Marker” on page 5-94

- “Loss of Alignment - VCAT” on page 5-96
- “Loss of Channel” on page 5-98
- “Loss of Clock” on page 5-101
- “Loss Of Data Synch” on page 5-105
- “Loss of Extra Traffic” on page 5-109
- “Loss of Frame and Multiframe” on page 5-110
- “Loss Of Frame (OTM1, OTM2, OTM3, OTM4, OTMC2, OTUTTP, ETTP, STTP, FLEX, PDH)”, see “Loss Of Frame, Loss Of Multiframe, or Signal Fail alarms” on page 5-119
- “Loss of Frame Delineation” on page 5-115
- “Loss Of Frame, Loss Of Multiframe, or Signal Fail alarms” on page 5-119
- “Loss of Lane Alignment” on page 5-130
- “Loss of Lock” on page 5-132
- “Loss Of Multiframe (WAN)” on page 5-143
- “Loss of Multiframe - VCAT” on page 5-144
- Loss Of Multiframe, see “Loss Of Frame, Loss Of Multiframe, or Signal Fail alarms” on page 5-119
- “Loss of OPU Multiframe Identifier” on page 5-145
- “Loss of Pointer” on page 5-150
- “Loss of Sequence - VCAT” on page 5-153
- “Loss of Service Delineation” on page 5-155
- Loss Of Signal (ESI), see ESI alarms in Part 1 of this document
- “Loss Of Signal (Ethernet)” on page 5-157
- “Loss Of Signal (OC/STM, ETH10G, ETH40G, ETH100G, FC, OTM1, OTM2, OTM3, OTM4, PTP, FLEX)” on page 5-161
- “Loss Of Signal (OPTMON, VOA)” on page 5-171
- “Loss Of Synchronization Messaging Channel” on page 5-176
- “Low Optical Return Loss at Output” on page 5-181
- “Low Order Bandwidth Near Limit” on page 5-185
- “Low Received Span Loss” on page 5-186
- “Low Voltage (DSM)” on page 5-188

M

- “MAC Status Defect” on page 5-191
- “Manual Area Address Dropped from area” on page 5-192

“Manual Switch Active”, see “Protection Switch Active alarms” on page 5-370
“Member Release Misaligned” on page 5-198
“Member Shelf Mismatch” on page 5-199
“Member Shelf Unknown” on page 5-201
“Member Shelf Unreachable” on page 5-203
“Minimum Gain” on page 5-206
“Modem Class Mismatch” on page 5-208
MS DCC Link Failure, see DCC Link Fail alarms in Part 1 of this document
“MSI Mismatch (ODUTTP, ODUCTP, OTM0, OTM1, OTM2, OTM3, ODU0, ODU1, ODUFLEX, OTMFLEX)” on page 5-209
“Multiplexed Rate Mismatch” on page 5-212

N

“Number of Level 1 NEs Exceeded” on page 5-219

O

“OAM Not Available” on page 5-220
“OCH Link Data Retrieval In Progress” on page 5-223
“OCH Link Data Save In Progress” on page 5-224
“ODU LCK” on page 5-225
“ODU Loss of Frame and Multiframe” on page 5-226
“ODU OCI” on page 5-227
“ODU Skew Out Of Range” on page 5-228
“ODU AIS (OTMFLEX, OTM0, OTM1, OTM2, OTM3, OTM4 for Broadband services, ODUTTP, ODUCTP, ODU0, ODU1, ODUFLEX, TCMCTP, TCMTTP)”, see “Secondary alarms” on page 5-463
“OTU BDI (OTUTTP, OTM1, OTM2, OTM3, or OTM4 for Broadband services)”, see “Secondary alarms” on page 5-463
“ODU Signal Degrade” on page 5-230
“ODU Signal Fail” on page 5-234
“ODU/OTU Trace Identifier Mismatch” on page 5-238
“Optical Line Fail” on page 5-242
“Optimization Scanning in Progress” on page 5-250
“OPU AIS (OTM0, OTM1, OTM2, OTM3, or OTM4 for Broadband services, ODUCTP, ETTP, STTP, ODUTTP)”, see “Secondary alarms” on page 5-463
“OPU Payload Type Mismatch” on page 5-251

- “OSC Loss Of Signal” on page 5-254
- “OSC RFI” on page 5-259
- “OSC Signal Degrade” on page 5-260
- “OSPF Adjacency Loss alarms” on page 5-265
- “OSPFv3 Adjacency Loss”, see “OSPF Adjacency Loss alarms” on page 5-265
- “OSPF Max Capacity Reached” on page 5-269
- “OSRP CCI Session Down” on page 5-270
- “OSRP CCI Session Out of Sync” on page 5-271
- “OSRP Configuration in Progress” on page 5-272
- “OSRP Line Operationally Blocked” on page 5-273
- “OSRP Node Operationally Blocked” on page 5-275
- “OSRP Port Capability Mismatch” on page 5-277
- “OTDR Trace In Progress” on page 5-278
- “OTL Skew Out Of Range” on page 5-279
- “OTS Provisioning Error” on page 5-281
- “OTU Signal Degrade” on page 5-287
- “OTU Signal Fail (OTM, OTM2, OTUTTP)” on page 5-291
- OTU Trace Identifier Mismatch, see “ODU/OTU Trace Identifier Mismatch” on page 5-238
- “Output Loss Of Signal” on page 5-294

P

- “Packet Configuration Integrity Fail” on page 5-297
- “Packet Rate Limit Exceeded” on page 5-300
- “PHY Map Mismatch” on page 5-306
- “Pluggable I/O Carrier 1/2 Fail” on page 5-307
- “Pluggable I/O Carrier 1/2 Missing” on page 5-308
- “Pluggable I/O Carrier 1/2 Unknown” on page 5-309
- “Pluggable I/O Panel Mismatch” on page 5-310
- “Pluggable I/O Panel Missing” on page 5-311
- “Pluggable I/O Panel Unknown” on page 5-313
- “Port Bandwidth Near Limit” on page 5-315
- “Power Failure” on page 5-317
- “Power Failure - A or Power Failure - B” on page 5-319

- “Power Failure - Fuse Blown” on page 5-325
- “Power Failure - Low Voltage” on page 5-328
- “Pre-FEC Signal degrade” on page 5-330
- “Pre-FEC Signal Fail” on page 5-333
- “Primary License Server Unavailable” on page 5-335
- “Primary RADIUS Accounting Server Unavailable” on page 5-336
- “Primary RADIUS Server Unavailable” on page 5-338
- “Primary Shelf Unreachable” on page 5-340
- Protection Channel Match Fail, see 1+1 APS alarms in Part 1 of this document
 - “Protection Exerciser Failed” on page 5-345
 - “Protection Mode Mismatch” on page 5-362
 - “Protection Scheme Mismatch” on page 5-364
- Protection Switch Byte Fail, see 1+1 APS alarms in Part 1 of this document
 - “Protection Switch Complete” on page 5-376
 - “Protection Switch Complete - Revertive” on page 5-379
 - “Provisioning Database Freeze Enable” on page 5-381
 - “Provisioning Incompatible” on page 5-382
 - “Provisioning Incompatible - Pluggable” on page 5-385

R

- “Reach Violation” on page 5-388
- “RAMAN Failed To Turn On” on page 5-389
- “Redundant Database Synch Failed” on page 5-391
- “Redundant Database Synch Failed - CP” on page 5-393
- “Redundant Database Synch in Progress” on page 5-395
- “Redundant Release Synch Failed” on page 5-396
- “Redundant Release Synch in Progress” on page 5-397
- “Release Server Mismatch” on page 5-398
- “Release Server URL Fail” on page 5-399
- “Remote Alarm Indication” on page 5-400
- “Remote CCM Error” on page 5-402
- “Remote Client Circuit Pack Failed - Pluggable” on page 5-404
- “Remote Client Circuit Pack Missing - Pluggable” on page 5-405

- “Remote Client Circuit Pack Unknown - Pluggable” on page 5-406
- “Remote Client High Received Optical Power” on page 5-407
- “Remote Client Link Down” on page 5-409
- “Remote Client Low Received Optical Power” on page 5-412
- “Remote Defect Indication” on page 5-414
- “Remote Fault (ETTP)”, see “Secondary alarms” on page 5-463
- “Remote Invalid Configuration” on page 5-417
- “Remote Inventory Not Supported” on page 5-419
- “Remote Line High Received Optical Power” on page 5-421
- “Remote Line Low Received Optical Power” on page 5-423
- “Remote Loopback Active” on page 5-425
- “Remote Loopback Fail” on page 5-426
- “Remote Node Unreachable” on page 5-428
- “Remote Port OOS” on page 5-432
- “Remote Port Unreachable” on page 5-433
- “Remote Power Fail Indication” on page 5-435
- “Remote Power Supply 1/2 Missing” on page 5-436
- “Remote Receiver Fail” on page 5-437
- “Resources Above Threshold” on page 5-439
- “Resources At Limit” on page 5-440
- “RFI (PATH)”, see “Secondary alarms” on page 5-463
- “RFI (STTP)”, see “Secondary alarms” on page 5-463
- “Ring Protection Exerciser Failed” on page 5-445
- “Ring Protection Switch Complete” on page 5-448
- “Ring Protection Switch Fail” on page 5-449
- “Rollover in Progress” on page 5-451
- “Root Directory Has Reached Maximum File Entry Limit” on page 5-452
- RS DCC Link Failure, see DCC Link Fail alarms in Part 1 of this document
- “Rx Channel Power Out of Range” on page 5-453
- “Rx Power Out of Range” on page 5-458

S

- “Secondary alarms” on page 5-463
- “Secondary License Server Unavailable” on page 5-475

- “Secondary RADIUS Accounting Server Unavailable” on page 5-476
- “Secondary RADIUS Server Unavailable” on page 5-478
- “Secondary Service Failed” on page 5-479
- “Secondary SETS Locking to Primary” on page 5-481
- Section DCC Link Failure, see DCC Link Fail alarms in Part 1 of this document
 - “SECTION/RS DCC OSPF Adjacency Loss”, see “OSPF Adjacency Loss alarms” on page 5-265
 - “Service Defect Indication” on page 5-485
 - “Service Mismatch” on page 5-489
 - “Shelf Bandwidth Near Limit” on page 5-490
 - “Shelf Data Missing” on page 5-491
 - “Shelf Power Near Limit” on page 5-492
 - “Shutoff Threshold Crossed” on page 5-494
- Signal Degrade (WAN), see Error alarms (WAN) in Part 1 of this document
 - “Signal Fail (OC48/192/768/STM16/64/256 Broadband, STTP)”, see “Loss Of Frame, Loss Of Multiframe, or Signal Fail alarms” on page 5-119
 - “Skew Out Of Range” on page 5-498
 - “SLDD Adjacency Loss” on page 5-500
 - “Slot Empty” on page 5-501
 - “Slot Sequence Provisioning Incomplete” on page 5-502
 - “SNC Datapath Fault” on page 5-503
 - “SNCG Not On Home Path” on page 5-505
 - “SNCG Unavailable” on page 5-507
 - “SNC Not On Home Path” on page 5-509
 - “SNC Reservation Unavailable” on page 5-511
 - “SNC Takeover Failed” on page 5-512
 - “SNC Unavailable” on page 5-515
 - “Software Auto-Upgrade in Progress” on page 5-517
 - “Software Configuration Unknown” on page 5-518
 - “Software Delivery Incomplete” on page 5-519
 - “Software Delivery in Progress” on page 5-520
 - “Software Mismatch” on page 5-521
 - “Software Subsystem Failed” on page 5-522

“Software Subsystem Restart” on page 5-524
“Software Upgrade Failed” on page 5-525
“Software Upgrade in Progress” on page 5-526
“Span Protection Exerciser Fail” on page 5-529
“Switch Shelf ID Mismatch Detected” on page 5-531
“Synchronization Protection alarms” on page 5-532

T

“TACACS Server 1/2 Unavailable” on page 5-534
“Tamper Detected” on page 5-535
“Target Unachievable” on page 5-537
“TCM Loss of Tandem Connection” on page 5-539
“Telemetry Loss of Signal” on page 5-540
“Test Access in Progress alarms” on page 5-542
“Threshold AIS ESO-A/ESO-B” on page 5-544
“Timing Distribution Loss of Reference - n Ref” on page 5-551
“Time Out” on page 5-549
“Timing Distribution Forced Switch - n Ref”, see “Synchronization Protection alarms” on page 5-532
“Timing Distribution Lockout - n Ref”, see “Synchronization Protection alarms” on page 5-532
“Timing Distribution Loss of Reference - n Ref” on page 5-551
“Timing Distribution Manual Switch - n Ref”, see “Synchronization Protection alarms” on page 5-532
“Timing Generation Entry to Freerun” on page 5-553
“Timing Generation Entry to Holdover” on page 5-557
“Timing Generation Failure To Lock” on page 5-560
“Timing Generation Forced Switch - n Ref”, see “Synchronization Protection alarms” on page 5-532
“Timing Generation Lockout - n Ref”, see “Synchronization Protection alarms” on page 5-532
“Timing Generation Loss of Reference - n Ref” on page 5-562
“Timing Generation Manual Switch - n Ref”, see “Synchronization Protection alarms” on page 5-532
“TOD Server Not Provisioned” on page 5-565
“TODR Reversion Inhibited” on page 5-567

- “TOD Threshold Exceeded” on page 5-568
- “Topology Build Failed” on page 5-569
- “Topology Failure” on page 5-570
- “Topology Instability” on page 5-571
- “Trace Identifier Mismatch (OCn/STMn)” on page 5-572
- “Trace Identifier Mismatch (STS/HO VC and VT/LO VC)” on page 5-575
- “Traffic Squelched” on page 5-578
- “Transport Data Recovery Failed” on page 5-580
- “TR Control Disabled” on page 5-582
- “TR Control Echo Trace Mismatch” on page 5-583
- “TR Control Initialization in Progress” on page 5-585
- “TR Control IS Optimization in Progress” on page 5-587
- “Tributary Slots Not Available” on page 5-588
- “Tx AIS (DS1)” on page 5-589
- “Tx AIS (DS3/E3)” on page 5-591
- “Tx Frequency Out of Range” on page 5-593
- “Tx Loss of Frame (DS1)” on page 5-594
- “Tx Loss of Frame (DS3/E3)” on page 5-596
- “Tx Loss Of Signal” on page 5-599
- “Tx Manual Provisioning Required” on page 5-601
- “Tx Partial Loss of Capacity - LCAS” on page 5-602
- “Tx Power In Reduced State” on page 5-604
- “Tx Power Out of Range” on page 5-606
- “Tx Remote Alarm Indication” on page 5-609
- “Tx Remote Defect Indication” on page 5-611
- “Tx Total Loss of Capacity - LCAS” on page 5-613
- “TX Tuning in Progress” on page 5-615

U

- “Unable to Synchronize TOD” on page 5-616
- “Unassigned Channel Detected” on page 5-618
- “Unequipped” on page 5-620
- “Unpaired SSH Key” on page 5-623
- “Unsupported Channel Provisioned” on page 5-624

V

- [“Validation Certificate About to Expire” on page 5-625](#)
- [“Validation Certificate Expired” on page 5-626](#)
- [“VOA Output LOS” on page 5-627](#)
- [“VT-STS bandwidth near limit” on page 5-628](#)

W

- [“Warm Restart Required” on page 5-630](#)
- [“Wavelength Measurement Error” on page 5-631](#)
- [“Wavelength Measurement Warning” on page 5-632](#)
- [“WAYSIDE 1/2 Port Failure” on page 5-633](#)

Procedure 5-1

Incomplete Channel Topology

Alarm ID: 1679

Probable cause

This alarm is raised as a warning to highlight stale or leftover Shelf Wavelength Topology (SWT) provisioning (for example, orphaned Tx/Rx adjacency or unused cross-connection), which is not part of a complete NCT channel.

Such leftover provisioning can result in unintended channels being built as a result of subsequent provisioning actions. For example, an orphaned Rx adjacency causing a channel to drop unexpectedly and creating an “accidental” Drop and Continue channel.

This warning is raised against an OTS one hour after detecting one or more wavelengths in that OTS with ROUTING set to ADD, DROP, or PASSTHROUGH, and COMPLETE set to FALSE.

Impact

Warning

Prerequisites

To perform this procedure, you require an account with at least a level 3 UPC.

Step	Action
1	Retrieve the SWT provisioning using Site Manager Shelf Wavelength Topology application.
2	Find the wavelength(s) with COMPLETE flag set to FALSE and confirm these are wavelengths you were not expecting to be provisioned in the network.
3	Delete the unused SWT provisioning by putting the corresponding Tx/Rx adjacency out-of-service (for ADD/DROP routing) or by deleting the unused cross-connection (for PASSTHROUGH routing).
4	If a desired channel is unexpectedly marked incomplete, traverse the expected path of that channel upstream and downstream from that node to find the node where the channel provisioning is missing (that is, ROUTING=UNKNOWN) and add the missing provisioning at that node.
5	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-2

Incomplete Software Lineup

Alarm ID: 92

Probable cause

This alarm is raised when a load file is missing. This can occur when a new circuit pack is inserted into the shelf, or when a shelf processor inserted into the shelf does not contain the software release that is active on the shelf.

This alarm can also be raised when a SP is replaced and the new SP is running a different software release than the active release on the network element.

This alarm can also be raised on a SP if the service bundle on the replacement SP does not match before the replacement.

If this alarm is raised during an upgrade activity contact your next level of support or your Ciena support group.

Impact

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

Prerequisites

To perform this procedure, you require an account with at least a level 3 UPC.

Step	Action
1	Verify the current load release on the shelf processor. Refer to the “Checking the current software release” procedure in <i>Commissioning and Testing</i> , 323-1851-221.
2	Retrieve all alarms on the system. Record the current state of the system.
3	Perform a software load transfer. Refer to the “Transferring a software load to a network element” procedure in <i>Administration and Security</i> , 323-1851-301. Note: A load transfer can take three hours. Contact your next level of support or your Ciena support group for assistance if necessary.
4	Perform a warm restart of the shelf processor. See “Restarting a circuit pack or shelf processor” procedure in Part 1 of this document.
5	Retrieve all alarms to ensure that the system is restored to its original state. If any alarm not recorded in step 2 is displayed, refer to the appropriate alarm clearing procedure.

Procedure 5-2 (continued)
Incomplete Software Lineup

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

—end—

Procedure 5-3

Input Loss Of Signal

Alarm ID: 557

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.

For CDC configurations, this alarm is raised on the AMP facility of CCMD8x16, RLA 5x1 or CCMD12 circuit packs.

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.

This alarm is masked by the “Shutoff Threshold Crossed” alarm. This alarm masks the “Output Loss Of Signal” alarm on the same amplifier facility.

Impact

Major, service-affecting (M, SA) alarm

Prerequisites

To perform this procedure, you must:

- use an account with at least a level 3 UPC
- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0
- have a network and site diagram

Procedure 5-3 (continued)

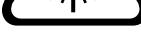
Input Loss Of Signal

- have a fiber cleaning kit
- have the LOS threshold level for this amplifier

Step	Action	
1	Check for and clear any active Optical Line Fail alarm.	
2	If the original alarm has	Then
	cleared	the procedure is complete
	not cleared	go to step 3
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	If the alarm is raised against	Then go to
	a CCMD12 or CCMD8x16 circuit pack	step 8
	otherwise	step 11
8	Ensure there are no ports switching to the Demux Degree AMP where the Connection Validation Test will be performed.	
9	Set the AMP to Amplified Spontaneous Emission (ASE) mode to generate light.	
10	If the original alarm has	Then
	cleared	the procedure is complete
	not cleared	go to step 11
11	Verify the AMP facility parameters are correctly provisioned. If required, correct any discrepancies. Refer to the “Editing facility parameters” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.	

Procedure 5-3 (continued)

Input Loss Of Signal

Step	Action
12	If the original alarm has cleared not cleared
	Then the procedure is complete go to step 13
13	Place the alarmed AMP facility out of service (OOS). Refer to the “Changing the primary state of a facility” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
14	<p>DANGER Risk of laser radiation exposure Do not look directly into the optical beam. Invisible light can severely damage your eyes.</p> 
	<p>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 out of service (OOS), then disconnect or reconnect the fiber.</p> 
	<p>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.</p> 
	Clean and then reconnect the output fibers and connectors at the amplifier. Refer to the “Cleaning Connectors” chapter in <i>Installation - General Information</i> , 323-1851-201.0.
15	Place the amplifier back in-service (IS). Refer to the “Changing the primary state of a facility” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
16	If the original alarm has cleared not cleared
	Then the procedure is complete go to step 17

Procedure 5-3 (continued)

Input Loss Of Signal

Step	Action				
17	<p>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, Circuit Pack Missing, and Loss Of Signal.</p> <p>If there are no upstream alarms, then verify the optical patchcord connected to the port reporting the alarm:</p> <ul style="list-style-type: none"> • ensure it is connected at both ends and that there is no problem with the optical patchcord • clean the connectors. Refer to the “Cleaning Connectors” procedure in <i>Installation - General Information</i>, 323-1851-201.0. 				
18	<p>If the original alarm has Then</p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 40%;">cleared</td> <td style="width: 60%;">the procedure is complete</td> </tr> <tr> <td>not cleared</td> <td>go to step 19</td> </tr> </table>	cleared	the procedure is complete	not cleared	go to step 19
cleared	the procedure is complete				
not cleared	go to step 19				
19	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 the “Editing facility parameters” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.				
20	Wait at least one minute for the alarm to clear. Change the Input LOS Threshold value back to the original value.				
21	<p>If the original alarm has Then</p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 40%;">cleared</td> <td style="width: 60%;">the procedure is complete</td> </tr> <tr> <td>not cleared</td> <td>go to step 22</td> </tr> </table>	cleared	the procedure is complete	not cleared	go to step 22
cleared	the procedure is complete				
not cleared	go to step 22				
22	Restart the circuit pack supporting the alarmed AMP facility. Refer to “Restarting a circuit pack or shelf processor” procedure in Part 1 of this document.				
23	<p>If the original alarm has Then</p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 40%;">cleared</td> <td style="width: 60%;">the procedure is complete</td> </tr> <tr> <td>not cleared</td> <td>go to step 24</td> </tr> </table>	cleared	the procedure is complete	not cleared	go to step 24
cleared	the procedure is complete				
not cleared	go to step 24				
24	Replace the circuit pack supporting the alarmed AMP facility. Refer to the procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.				
25	If the alarm does not clear, contact your next level of support or your Ciena support group.				

—end—

Procedure 5-4

Integrated Test Set Configured

Alarm ID: 1519, 1520, 1521, 1522, 1628, 1629, 1630, 1631, 2070, 2093

Probable cause

This alarm is raised when the Integrated Test Set feature has been provisioned on the ETH10G, ETH40G, ETH100G, OC192/STM64, OC768/STM256, OTM2, OTM3, or OTM4 facility of 40G+ CFP OCI, 100G OCI, 100G WL3e OTR, or 10x10G MUX circuit packs.

Impact

Warning, non-service-affecting (w, NSA) alarm

Prerequisites

To perform this procedure, you require an account with at least a level 3 UPC.

Step	Action
1	Select Integrated Test Set from the Configuration drop-down menu. If there is more than one possible facility on the shelf, select the appropriate facility from the facility list. Refer to the “Performing a test with the integrated test set” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310, for more information.
2	Disable the GEN & MON patterns. <i>Gen and Mon patterns are set to No Pattern.</i>
3	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-5

Integrated Test Set Data Save In Progress

Alarm ID: 1531, 1532, 1533, 1534, 1664, 1665, 1666, 1667, 2072, 2095

Probable cause

This alarm is raised when there is a save in progress on a port with the Integrated Test Set provisioned.

Impact

Warning

Prerequisites

To perform this procedure, you require an account with at least a level 3 UPC.

Step	Action
1	No action is required. The alarm clears when the data save process is completed.
2	If the alarm does not clear or is unexpected, contact your next level of support or Ciena support group.

—end—

Procedure 5-6 Intercard Suspected

Alarm ID: 73

Probable cause

This alarm is raised when a data path or communications path fault is detected within the product, but the fault is unable to be isolated to a specific circuit pack or to the backplane. Because the fault cannot be isolated to a specific component, the alarm will be raised against more than one circuit pack. Examples are:

- A circuit pack that has a loss of traffic or degraded signal integrity on a backplane link which interfaces to another circuit pack in the shelf. The alarm would be raised against both circuit packs.
- A communications bus (clock, parity, or interprocessor communication) failure between a shelf processor and a circuit pack. The alarm would be raised against the shelf processor and the other circuit pack.

ATTENTION

This alarm can be seen against the XC and 20G L2SS circuit packs after a WAN configuration change, which triggers an automatic cold restart of the 20G L2SS circuit pack. This alarm clears after the cold restart is completed.

ATTENTION

When performing the commit, during restoring provisioning data procedure, on a network element containing GE, L2SS, and 20G L2SS cards, an Intercard Suspected alarm can be raised against the XC, OC-n/STM-n, GE, L2SS, and 20G L2SS circuit packs. These alarms clear automatically within a few minutes after the network element recovers from the commit.

ATTENTION

This alarm can be seen on adjacent eMOTR circuit packs following a cold restart of both eMOTR circuit packs. These alarms may clear automatically within 10 minutes, in which case no further action is required. Otherwise follow the clearing procedures.

Procedure 5-6 (continued)

Intercard Suspected**Impact**

Critical, service-affecting (C, SA) alarm if raised on the SP, XC, MSPP, Transponder, eMOTR, or POTS circuit pack and the circuit pack is currently active

Minor, non-service-affecting (m, NSA) alarm if the circuit pack is not currently active, or if it is a photonic circuit pack

The status of the circuit pack can be unknown because of the loss of communications. Additional failures can be service-affecting.

Prerequisites

To perform this procedure, you must

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545
- have an antistatic wrist strap to dissipate electrostatic charges

Step Action

- 1** Identify the circuit pack(s) raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document.
- 2** If there are any “Circuit Pack Failed” alarms present, address those alarms first.
- 3** Determine the time since the “Intercard Suspected” alarm was raised. It is recommended that circuit packs 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 circuit pack which has a red LED turned on, and that circuit pack has not been replaced within the past 48 hours, then replace the circuit pack. Refer to the appropriate circuit pack replacement procedure in *Fault Management - Module Replacement*, 323-1851- 545.
- 5** If the alarm is raised on any of the following combinations of circuit packs, 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.
 - If the alarm is raised on the SP, XC, or MSPP circuit pack, then replace the circuit pack. Refer to the appropriate circuit pack replacement procedure in *Fault Management - Module Replacement*, 323-1851- 545.
 - If the alarm is raised on the Transponder or eMOTR circuit pack, then restart the circuit pack. Refer to the appropriate circuit pack restart procedure in *Fault Management - Module Replacement*, 323-1851- 545.
 - If the alarm is raised on the POTS circuit pack, then restart the circuit pack. Refer to the appropriate circuit pack restart procedure in *Fault Management - Module Replacement*, 323-1851- 545.

Procedure 5-6 (continued)

Intercard Suspected

Step	Action
6	If the alarmed circuit packs are: Then perform the following: See Note 1 and Note 2
	one XC and one or more circuit packs which use the XC 1- Cold Restart XC circuit pack raising the alarm 2- Replace XC circuit pack raising the alarm
	two XCs and only one tributary circuit pack which uses the XC 1- Cold Restart the tributary circuit pack raising the alarm 2- Replace the tributary circuit pack raising the alarm
	Two XCs and more than one tributary circuit pack which uses the XC 1- Cold restart the active XC 2- Replace the active XC 3- Cold restart the other XC 4- Replace the other XC 5- Cold restart alarmed tributary circuit pack with the lowest slot number 6- Replace alarmed tributary circuit pack with the lowest slot number 7- Continue with the remaining tributary circuit packs, in order of increasing slot numbers
	two XCs only 1-Cold restart the active XC 2- Replace the active XC 3- Cold restart the other XC 4- Replace the other XC
	one or more SPs and only one other circuit pack 1- Cold restart the other circuit pack raising the alarm 2- Replace other circuit pack raising the alarm
	one or more SPs and one or more other circuit packs 1- Cold restart the active SP 2- Replace the active SP 3- Cold restart the other SP 4- Replace the other SP

If the alarmed circuit packs are:	Then perform the following: See Note 1 and Note 2
a single (1+8)xOTN Flex MOTR in an even slot with traffic to another (1+8)xOTN Flex MOTR circuit pack in the adjacent, lower numbered slot	1- Cold restart the (1+8)xOTN Flex MOTR in the even slot 2- Replace the (1+8)xOTN Flex MOTR in the even slot 3- Cold restart the (1+8)xOTN Flex MOTR in the odd slot 4-Replace the (1+8)xOTN Flex MOTR in the odd slot
two Flex2 WL3/WL3e OCLD Submarine circuit packs with an equipment Profile=BPSK2x50G which have PECs that do not match	1- Replace either of the circuit packs with the other PEC, so that both PECs match
two matching transponder circuit packs which carry traffic between them, such as OCLD/OCLD pairs, OCI/OCI pairs or OCI/MUX pairs	1- Cold restart the transponder circuit pack in the higher numbered slot 2- Replace the transponder circuit pack in the higher numbered slot 3- Cold restart the transponder circuit pack in the lower numbered slot 4- Replace the transponder circuit pack in the lower numbered slot
A combination of an OCI/MUX and an OCLD circuit pack which carry traffic between them	1- Cold restart the OCI/MUX circuit pack 2- Replace both circuit packs

If the alarmed circuit packs are: Then perform the following:
See Note 1 and Note 2

two or more tributary circuit packs which use the XCs

1- Cold Restart the alarmed circuit pack in the lowest slot number

2- Replace the alarmed circuit pack in the lowest slot number

3- Continue with remaining circuit packs in order of increasing slot numbers

two adjacent eMOTR circuit packs which carry traffic between them

1- Cold restart the eMOTR circuit pack that was restarted the latest.

2- Cold restart the adjacent eMOTR circuit pack. See Note 3.

Note 1: To perform a cold restart on the identified circuit pack, refer to the “Restarting a circuit pack or shelf processor” procedure in Part 1 of this document.

Note 2: Replace a circuit pack only if it is not been replaced within the past 48 hours. To replace a circuit pack, refer to the appropriate circuit pack replacement procedure in *Fault Management - Module Replacement*, 323-1851- 545.

Note 3: To determine which eMOTR circuit pack was the latest to cold restart, verify the “Historical Fault Browser” in Site Manager to find the latest “Cold Restart Completed” event for one of the eMOTR circuit packs.

- 7 If the alarm persists after 10 minutes, or if the circuit packs had already been replaced within the past 48 hours, contact your next level of support or your Ciena support group.

—end—

Procedure 5-7

Intercard Suspected - Pluggable

Alarm ID: 344

Probable cause

This alarm is raised when an SFP/SFP+/XFP/CFP/DPO/QSFP/QSFP+/QSFP28 reports suspected communications bus failures. The fault may be on the circuit pack or on the pluggable module but the software is unable to determine exactly where the fault exists.

Impact

Critical, service-affecting (C, SA) alarm for an active pluggable
Minor, non-service-affecting (m, NSA) alarm for an inactive pluggable

Prerequisites

To perform this procedure, you must:

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545
- have an antistatic wrist strap to dissipate electrostatic charges
- obtain a supported pluggable module for the corresponding circuit pack (refer to the “Supported SFP/SFP+/XFP/CFP/DPO/QSFP/QSFP+/QSFP28 modules for interface circuit packs” table in chapter 7 of *6500 Planning*, NTRN10EG)

Step	Action
1	Identify the pluggable module raising the alarm and the circuit pack on which it exists. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document.
2	Perform a cold restart on the circuit pack identified in step 1. Refer to the “Restarting a circuit pack or shelf processor” procedure in Part 1 of this document.
3	If the alarm persists after 10 minutes then replace the pluggable module you identified in step 1 with a supported pluggable module. Refer to the appropriate pluggable module replacement procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.
4	If the alarm persists after 10 minutes, contact your next level of support or your Ciena support group.

—end—

Procedure 5-8

Intercard Suspected - Pluggable I/O Carrier 1/2

Alarm IDs: 1060, 1061

Probable cause

This alarm is raised against a pluggable I/O carrier when there is suspected communications bus failures with an associated circuit pack (such as 20G L2SS). This occurs when the I/O carrier cannot power up after power is enabled by the circuit pack. The pluggable I/O carrier is suspected by software based on a majority conviction algorithm.

Impact

Critical, service-affecting (C, SA) alarm for an active I/O carrier

Minor, non-service-affecting (m, NSA) alarm for an inactive I/O carrier

Prerequisites

To perform this procedure, you must:

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545
- have an antistatic wrist strap to dissipate electrostatic charges
- obtain a supported pluggable I/O carrier for the corresponding circuit pack (refer to Part 1 of *Planning*, NTRN10EG)

Step	Action
1	Identify the circuit pack raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document. The Unit field in the Active Alarms application specifies the circuit pack, shelf ID, circuit pack slot, and pluggable port using the following format: <circuit pack>-<shelf-id>-slot#-pluggable port#
2	Ensure that I/O support is enabled.
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	Replace the I/O carrier you identified in step 1 with a supported I/O carrier. Refer to the “Replacing an optical interface circuit pack” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.
5	Retrieve all alarms to determine if the original alarm has cleared.

1 Identify the circuit pack raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document. The **Unit** field in the **Active Alarms** application specifies the circuit pack, shelf ID, circuit pack slot, and pluggable port using the following format:

<circuit pack>-<shelf-id>-slot#-pluggable port#

2 Ensure that I/O support is enabled.

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 Replace the I/O carrier you identified in step 1 with a supported I/O carrier. Refer to the “Replacing an optical interface circuit pack” procedure in *Fault Management - Module Replacement*, 323-1851-545.

5 Retrieve all alarms to determine if the original alarm has cleared.

Procedure 5-8 (continued)

Intercard Suspected - Pluggable I/O Carrier 1/2

Step	Action
6	If the alarm does not clear, replace the circuit pack you identified in step 1 . Refer to the “Replacing an optical interface circuit pack” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.
7	If the alarm is still active, contact your next level of support or your Ciena support group.

—end—

Procedure 5-9

Internal Database Synch in Progress

Alarm ID: 1598

Probable cause

This alarm is raised to indicate that the SP and OTN XC (X-Conn 600G PKT/OTN [NTK615AA] and X-Conn 1600G PKT/OTN [NTK616AA] circuit packs) databases are re-synchronizing in order to maintain a consistent database. Some OTN commands might not work properly when this alarm is active.

This alarm is only applicable for OTN shelves with an OTN XC provisioned. The alarm is only raised under these scenarios:

- after an SP restart (cold and warm)
- after an SP switchover for dual SP scenarios
- after an OTN XC restart (cold and warm)
- after an XC switchover for dual XC scenarios
- after any loss of communication between the SP and OTN XC
- after a Database restore
- during an NE upgrade
- after commissioning the OSRP OTN Control Plane on the node (due to the XC SWACT that is required)

Note: The alarm is cleared automatically after the re-sync is complete. When the alarm is cleared, in Site Manager a dialog may appear which requires user acknowledgment.

Impact

Warning, non-service-affecting (w, NSA) alarm

Prerequisites

To perform this procedure, you must

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0
- have an antistatic wrist strap to dissipate electrostatic charges

Procedure 5-9 (continued)

Internal Database Synch in Progress

Step	Action
1	If the alarm does not clear automatically, wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf and insert the OTN XC circuit pack. After the XC has booted up, the re-sync will occur and the alarm will clear.
2	If the alarm does not clear, restart the SP. Refer to the “Restarting a circuit pack or shelf processor” in Part 1 of this document.
3	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-10 **Internal Mgmt Comms Suspected**

Alarm ID: 438

Probable cause

This alarm is raised when the communication channel failure between two circuit packs is suspected. The alarm is raised against both circuit packs suspected of being the cause of the failure.

Impact

Minor, non-service-affecting (m, NSA) alarm, if a circuit pack is provisioned for 1+1/MSP linear or 1:N

Major, service-affecting (M, SA) alarm, if a circuit pack is unprotected or provisioned for UPSR/SNCP or 2-Fiber/4-Fiber BLSR/MS-SPRing/HERS protection

Prerequisites

To perform this procedure, you must

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0
 - have an antistatic wrist strap to dissipate electrostatic charges

Procedure 5-10 (continued)
Internal Mgmt Comms Suspected

Step	Action	Then
7	Reseat the other circuit pack raising the alarm. Refer to the “Reseating a circuit pack” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.	
8	If the original alarm has	Then
	cleared	the procedure is complete
	not cleared	go to step 9
9	If the circuit pack reseated in step 5 was	Then go to
	not replaced in the past 48 hours	step 10
	replaced in the past 48 hours	step 12
10	Replace the circuit pack reseated in step 5. Refer to the “Replacing an optical interface circuit pack” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.	
11	If the original alarm has	Then
	cleared	the procedure is complete
	not cleared	go to step 12
12	If the circuit pack reseated in step 7 was	Then go to
	not replaced in the past 48 hours	step 13
	replaced in the past 48 hours	step 15
13	Replace the circuit pack reseated in step 7. Refer to the “Replacing an optical interface circuit pack” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.	
14	If the original alarm has	Then
	cleared	the procedure is complete
	not cleared	go to step 15
15	If the alarm does not clear, contact your next level of support or your Ciena support group.	

—end—

Procedure 5-11 Intrusion Attempt

Alarm ID: 267

Probable cause

This alarm is raised when the shelf processor detects an intruder attempting to gain shelf access using either an IPv4 or IPv6 connection, and the maximum number of login attempts exceeds the provisioned number allowed.

The alarm is raised when an intrusion is detected and the channel/port locks. The alarm clears automatically after the lockout period expires. However, an administrator 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.

ATTENTION

Clearing this alarm clears all other alarms of the SECU class (except those raised against the Primary and secondary RADIUS servers).

Impact

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

Prerequisites

To perform this procedure, you must:

- be able to connect to the SP
- use an account with at least a level 4 UPC

Step	Action
1	Allow the alarm to clear itself when the lockout time expires or go to step 2 .
2	Select the alarmed network element in the navigation tree.
3	Select Clear Security Alarm from the Faults menu. Clearing the Intrusion Attempt alarm has no effect on the alarmed port. It only removes the alarm from the alarm list. The port will continue to be locked out until valid login information is delivered. The channel is locked out and no one can log in from the originating address for the duration of the lockout. The alarm clears from the network element when the channel unlocks after the provisioned elapsed time.

Procedure 5-11 (continued)

Intrusion Attempt

Step	Action
4	Click Yes in the confirmation dialog box.
5	Follow your company policy for handling intrusion attempts. —end—

Procedure 5-12

Invalid Site Topology

Alarm ID: 872

Probable cause

This alarm is raised against the Optical Transmission Section (OTS) entity when there are more than two OTSs with the same site identifier and optical system identifier (OSID).

Note: This alarm may be raised if there is a duplicate site provisioned within an OSID.

This alarm will also be raised whenever the number of OTSs within a site (with the same Site ID) exceeds the maximum limit. The limit is different depending to the shelf and circuit pack type in the system. For the maximum number of OTSs in each site, refer to the OTS engineering rules section in the *Data Application Guide*, NTRN15BA. The alarm will be raised against each OTS in the site.

ATTENTION

Do not use the same Tx/Rx ID in the same site, even if they are used on different shelves.

Impact

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

Prerequisites

To perform this procedure, you require an account with at least a level 4 UPC.

Step	Action
1	Identify the network elements raising the alarm.
2	Determine from network plans or other documents which network element has the correct site identifier and OSID.
3	Log into the network element with the duplicate site identifier and OSID.

Procedure 5-12 (continued)

Invalid Site Topology

Step	Action
4	<p>CAUTION</p>  <p>Risk of loss of functionality Ensure every network element has a unique site identifier. If you are changing the site identifier of a network element, ensure it is unique.</p>
	<p>Enter the correct Site identifier and Optical system identifier values. Refer to the “Editing the nodal shelf parameters” procedure in <i>Administration and Security</i>, 323-1851-301.</p>
5	Wait for the network element to complete the automatic restart.
6	Ensure that no other Invalid Site Topology alarms exist. If there are other Invalid Site Topology alarms, repeat this procedure.
7	If the alarm does not clear, verify the number of OTSs in the site. Refer to the “Retrieving OTS Management, OTS Equipment, and Facility details” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
8	Reduce the number of OTSs in the site to less than or equal to the limit.
9	If the alarm does not clear, verify that the Tx/Rx IDs are unique among all the shelves within the site.
10	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-13

I/O Module Mismatch

Alarm ID: 798

Probable cause

This alarm is raised only in a 14-slot metro front electrical shelf, where the I/O module is present but is not the type required by the E1 circuit pack.

Impact

Major, service-affecting (M, SA) alarm

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

Prerequisites

To perform this procedure, you must:

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545
- have an antistatic wrist strap to dissipate electrostatic charges
- obtain a supported I/O module for the 63xE1 circuit pack (refer to the “I/O and protection hardware” section in Part 1 of *Planning*, NTRN10EG)

Step	Action
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	Replace the I/O module with the type that is required by the E1 circuit pack. Refer to the “Replacing the E1 I/O module in a metro front electrical shelf” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545, for instructions.

—end—

Procedure 5-14 I/O Module Missing

Alarm ID: 799

Probable cause

This alarm is raised only in a 14-slot metro front electrical shelf, where the I/O module is not present.

Impact

Major, service-affecting (M, SA) alarm

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

Prerequisites

To perform this procedure, you must:

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545
- have an antistatic wrist strap to dissipate electrostatic charges
- obtain a supported I/O module for the 63xE1 circuit pack (refer to the “I/O and protection hardware” section in Part 1 of *Planning*, NTRN10EG)

Step	Action
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	Install the required I/O module in the shelf. Ensure that you use the type that is required by the E1 circuit pack. Refer to <i>equipment replacement procedures in Fault Management - Module Replacement</i> , 323-1851-545, for instructions.

—end—

Procedure 5-15 I/O Module Unknown

Alarm ID: 800

Probable cause

This alarm is raised only in a 14-slot metro front electrical shelf, where an I/O module is present but its type cannot be determined.

Impact

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

Prerequisites

To perform this procedure, you must:

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545
- have an antistatic wrist strap to dissipate electrostatic charges
- obtain a supported I/O module for the 63xE1 circuit pack (refer to the “I/O and protection hardware” section in Part 1 of *Planning*, NTRN10EG)

Step	Action
1	Identify the I/O module raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document.
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	Compare the I/O module raising the alarm with the supported I/O modules for each slot on the circuit pack. Refer to the “Shelf equipping rules” in <i>Planning - Ordering Information</i> , 323-1851-151. If the I/O module raising the alarm is in Then
	an unsupported slot go to step 4
	a supported slot the module may be damaged. Go to step 5.
4	Replace the I/O module raising the alarm with a I/O module supported in that slot. Refer to the “Replacing the E1 I/O module in a metro front electrical shelf” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-543. Go to step 6.

Procedure 5-15 (continued)

I/O Module Unknown

Step	Action
5	Replace the I/O module with an identical I/O module. Refer to the “Replacing the E1 I/O module in a metro front electrical shelf” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-543.
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	contact your next level of support or your Ciena support group
If you replaced an I/O module in step 5, the I/O module you replaced was damaged.	

—end—

Procedure 5-16 I/O Panel Mismatch

Alarm ID: 602

Probable cause

This alarm is raised when an I/O panel is present but is not the correct type for the 63xE1, 24xDS3/EC-1, 24xDS3/E3, 16xSTM-1e, or 24x10/100BT circuit pack. Consider the following:

- For E1, the left I/O panel supports the 63xE1 circuit packs in slots 1 to 4. The right I/O panel supports the 63xE1 circuit packs in slots 9 to 12.
- For DS3/EC-1 or DS3/E3, the first I/O panel supports slots 1 and 2, the second I/O panel supports slots 3 and 4, the third I/O panel supports slots 9 and 10, and the fourth I/O panel supports slots 11 and 12.
- For STM-1e, the first I/O panel supports slots 1 and 2, the second I/O panel supports slots 3 and 4, the third I/O panel supports slots 9 and 10, and the fourth I/O panel supports slots 11 and 12.
- For 10/100BT, the first I/O panel supports slots 1 and 2, the second I/O panel supports slots 3 and 4, the third I/O panel supports slots 9 and 10, and the fourth I/O panel supports slots 11 and 12.

For the 14-slot metro front electrical shelf, this alarm is raised when the I/O panel is present but is not the type required by the 24xDS3/E3, 24xDS3/EC-1, or 24x10/100BT (FE) circuit pack provisioned in slot 5 and/or 6.

Impact

Major, service-affecting (M, SA) alarm for an I/O panel associated with an in-service circuit pack with cross-connects

Minor, non-service-affecting (m, NSA) alarm for an I/O panel associated with an out-of-service circuit pack or an in-service circuit pack without cross-connects

Prerequisites

To perform this procedure, you must:

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545
- have an antistatic wrist strap to dissipate electrostatic charges
- obtain a supported I/O panel (refer to the “I/O and protection hardware” section in Part 1 of *Planning*, NTRN10EG)

Procedure 5-16 (continued)

I/O Panel Mismatch

Step	Action
1	Identify the circuit pack raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document. The Unit field in the Active Alarms application specifies the circuit pack and circuit pack slot using the following format: <circuit pack>-slot#
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	Replace the I/O panel associated with the circuit pack you identified in step 1 with a supported I/O panel. Refer to the I/O panel replacement procedures in <i>Fault Management - Module Replacement</i> , 323-1851-545.
4	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-17 I/O Panel Missing

Alarm ID: 603

Probable cause

This alarm is raised when an I/O panel required by the 63xE1, 24xDS3/EC-1, 24xDS3/E3, 16xSTM-1e, or 24x10/100BT circuit pack is not present.

Consider the following:

- For DS3/EC-1 or DS3/E3, the first I/O panel supports slots 1 and 2, the second I/O panel supports slots 3 and 4, the third I/O panel supports slots 9 and 10, and the fourth I/O panel supports slots 11 and 12.
- For STM-1e, the first I/O panel supports slots 1 and 2, the second I/O panel supports slots 3 and 4, the third I/O panel supports slots 9 and 10, and the fourth I/O panel supports slots 11 and 12.
- For 10/100BT, the first I/O panel supports slots 1 and 2, the second I/O panel supports slots 3 and 4, the third I/O panel supports slots 9 and 10, and the fourth I/O panel supports slots 11 and 12.

For the 14-slot metro front electrical shelf, this alarm is raised when the associated I/O panel is not present for:

- a 24xDS3/E3 or 24xDS3/EC-1 circuit pack provisioned in slot 5 and/or 6.
- a 24x10/100BT (FE) circuit pack (with provisioned I/O-dependent ETH facilities) provisioned in slot 5 and/or 6.

Impact

Major, service-affecting (M, SA) alarm for an I/O panel associated with an in-service circuit pack with cross-connects

Minor, non-service-affecting (m, NSA) alarm for an I/O panel associated with an out-of-service circuit pack or an in-service circuit pack without cross-connects.

Prerequisites

To perform this procedure, you must:

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545
- have an antistatic wrist strap to dissipate electrostatic charges
- obtain a supported I/O panel for the 63xE1, 24x10/100BT, or 24xDS3/EC-1 circuit pack (refer to the “I/O and protection hardware” section in Part 1 of *Planning*, NTRN10EG)

Procedure 5-17 (continued)

I/O Panel Missing

Step	Action
1	Identify the circuit pack raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document. The Unit field in the Active Alarms application specifies the circuit pack and circuit pack slot using the following format: <circuit pack>-slot#
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	Install a supported I/O panel associated with the 63xE1, 24xDS3/EC-1, 24xDS3/E3, 16xSTM-1e or 24x10/100BT circuit pack you identified in step 1 . Refer to the “Installing electrical I/O hardware and I/O panels in the <i>Installation</i> technical publication specific to the respective 6500 shelf type.
4	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-18 I/O Panel Unknown

Alarm ID: 604

Probable cause

This alarm is raised when an unrecognized I/O panel is installed in a shelf provisioned with 63xE1, 24xDS3/EC-1, 24xDS3/E3, 16xSTM-1e, or 24x10/100BT circuit packs. Consider the following:

- For DS3/EC-1 or DS3/E3, the first I/O panel supports slots 1 and 2, the second I/O panel supports slots 3 and 4, the third I/O panel supports slots 9 and 10, and the fourth I/O panel supports slots 11 and 12.
- For STM-1e, the first I/O panel supports slots 1 and 2, the second I/O panel supports slots 3 and 4, the third I/O panel supports slots 9 and 10, and the fourth I/O panel supports slots 11 and 12.
- For 10/100BT, the first I/O panel supports slots 1 and 2, the second I/O panel supports slots 3 and 4, the third I/O panel supports slots 9 and 10, and the fourth I/O panel supports slots 11 and 12.

For the 14-slot metro front electrical shelf, this alarm is raised when an unrecognized I/O panel is installed in a shelf with a 24xDS3/E3, 24xDS3/EC-1, or 24x10/100BT (FE) circuit pack provisioned in slot 5 and/or 6.

Impact

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

The alarm is m, NSA as the panel can be operating correctly, but its inventory cannot be read. Payload alarms will signal the degree of the fault.

Prerequisites

To perform this procedure, you must:

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545
- have an antistatic wrist strap to dissipate electrostatic charges
- obtain a supported I/O panel for the 63xE1, DS3/EC-1, DS3/E3, 16xSTM-1e or 24x10/100BT circuit pack (refer to the “I/O and protection hardware” section in Part 1 of *Planning*, NTRN10EG)

Procedure 5-18 (continued)

I/O Panel Unknown

Step	Action
1	Identify the circuit pack raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document. The Unit field in the Active Alarms application specifies the circuit pack and circuit pack slot using the following format: <circuit pack>-slot#
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	Replace the I/O panel for the 63xE1, 24xDS3/EC-1, 24xDS3/E3, 16xSTM-1e or 24x10/100BT circuit pack you identified in step 1 with a supported I/O panel. Refer to the I/O panel replacement procedures in <i>Fault Management - Module Replacement</i> , 323-1851-545.
4	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-19 Isolated Station

Alarm ID: 815

Probable cause

This alarm is raised when the station can no longer send data traffic to any of the other stations on the RPR.

Impact

Critical, service-affecting (C, SA) alarm

Prerequisites

To perform this procedure, you must observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545.

Step	Action
1	Verify the OC-n/STM-n fiber connections related to RPR ring. Repair, clean, and reconnect the fibers as required. Refer to the cleaning connectors procedures in <i>Installation - General Information</i> , 323-1851-201.0.
2	If the original alarm has Then
	cleared the procedure is complete
	not cleared go to step 3
3	Use the appropriate alarm clearing procedure to clear any alarms on the RPR ring including Loss Of Signal and AIS (STS Rx) alarms. If the alarms are against OC-n/STM-n circuit packs, clear these alarms first.
4	If the WAN Link Down alarm is raised against the RPR circuit pack, clear the alarm using the appropriate alarm clearing procedure.
5	If the alarm does not clear, ensure the WAN links on the adjacent circuit packs are not OOS.
6	If the alarm does not clear, ensure that forced switches on the WAN links of the adjacent RPR circuit packs are not active.
7	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-20 LACP Failed

Alarm IDs: 1067, 1068, 1371

Probable cause

This alarm is raised against an ETH or ETH10G facility when LACP is enabled on the facility, but the facility cannot establish the LACP peering because there is no LACPDU received on the link.

The alarm can also be raised on the LAG member when edge services polling time is set to fast and there are 500 or more VCEs on a LACP port.

Impact

Critical, service-affecting (C, SA) alarm

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

Prerequisites

To perform this procedure, you must use an account with at least a level 3 UPC.

Step	Action
1	Check the configuration of the remote equipment whether LACP is enabled on the port.
2	Check if the link is connected to the correct port.
3	If there are 500 or more VCEs on a LACP port, provision the poll time on the near-end and the far-end to 30 seconds.
4	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-21 LAN alarms

Use this procedure to clear alarms associated with the LAN ports.

A transient LAN port failure alarm can be raised momentarily when a LAN port is created.

COLAN-A Port Failure

Alarm ID: 533

Probable cause

This alarm is raised when the COLAN A port (SP-A COLAN) on the access panel does not receive any Ethernet packets. This occurs if there is a bad Ethernet connection, or the COLAN-A port fails.

COLAN-X Port Failure

Alarm ID: 535

Probable cause

This alarm is raised when the COLAN-X port (COLAN) on the access panel does not receive any Ethernet packets. This occurs if there is a bad Ethernet connection, or the COLAN-X port fails.

Impact

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

ILAN-IN Port Failure

Alarm ID: 531

Probable cause

This alarm is raised when the ILAN-IN port (LAN IN) on the access panel does not receive any Ethernet packets. This occurs if there is a bad Ethernet connection or the ILAN-IN port fails.

The alarm is also raised when the adjacent shelf is a 6500 shelf and the MIC is failed or removed.

Impact

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

Procedure 5-21 (continued)

LAN alarms

ILAN-OUT Port Failure

Alarm ID: 532

Probable cause

This alarm is raised when the ILAN-OUT port (LAN OUT) on the access panel does not receive any Ethernet packets. This occurs if there is a Ethernet bad connection or the ILAN-OUT port fails.

The alarm is also raised when the adjacent shelf is a 6500 shelf and the MIC is failed or removed.

Impact

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

ETH LAN Port Failure

Alarm ID: 536

Probable cause

This alarm is raised when the LAN port (Local Craft 10/100 BT) on the shelf processor in slot 15 or 16 of the 6500-7 packet-optical shelf or 14 slot shelf, or slot 41 or 42 of the 32-slot shelf does not receive any Ethernet packets. This occurs if there is a Ethernet bad connection, the LAN port fails, or there is no craft terminal physically connected.

Impact

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

LAN Link Failure

Alarm ID: 1874

Probable cause

This alarm is raised when the link status of a COLAN or ILAN port is down in a network indicating that either COLAN or ILAN port lost its link/connectivity to the network and the port is not available for any further communication.

This alarm is raised on the 6500 shelves participating in a network. It tracks the link status of all the provisioned LAN ports in the network. The alarm will be automatically cleared when the link comes up for the corresponding LAN port.

Impact

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

Prerequisites

To perform this procedure, you must use an account with at least a level 3 UPC.

Procedure 5-21 (continued)

LAN alarms

Step	Action						
1	<p>Check the DCN information to determine if the appropriate LAN port must be enabled.</p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 40%; vertical-align: top; padding-right: 10px;">If the LAN must be</td><td style="width: 60%;">Then go to</td></tr> <tr> <td>disabled</td><td style="color: blue;">step 2</td></tr> <tr> <td>enabled</td><td style="color: blue;">step 3</td></tr> </table>	If the LAN must be	Then go to	disabled	step 2	enabled	step 3
If the LAN must be	Then go to						
disabled	step 2						
enabled	step 3						
2	<p>Disable the appropriate LAN port. Refer to the “Deleting an entry in the communications settings” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i>, 323-1851-310.</p> <p>Note: The ETH LAN port cannot be disabled. For the ETH LAN port Failure alarm, disable the alarm using an alarm profile. Refer to the “Editing an alarm profile” procedure in Part 1 of this document.</p> <p>Go to step 7.</p>						
3	<p>Check that the LAN configuration at both ends of the link are the same. Refer to the “Retrieving communications settings” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i>, 323-1851-310.</p> <p>If the configuration is different, edit the configuration as required. Refer to the “Editing the communications settings” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i>, 323-1851-310.</p>						
4	<p>At the local network element, retrieve all alarms to determine if the original alarm has cleared.</p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 40%; vertical-align: top; padding-right: 10px;">If the original alarm has</td><td style="width: 60%;">Then</td></tr> <tr> <td>cleared</td><td>the procedure is complete</td></tr> <tr> <td>not cleared</td><td style="color: blue;">go to step 5</td></tr> </table>	If the original alarm has	Then	cleared	the procedure is complete	not cleared	go to step 5
If the original alarm has	Then						
cleared	the procedure is complete						
not cleared	go to step 5						
5	Ensure that the appropriate cable is correctly connected to the required LAN port on the access panel or shelf processor.						
6	If the alarm is raised against the ILAN-IN or ILAN OUT ports and the adjacent shelf for that port is a 6500 shelf, check the status of the MIC on the adjacent shelf. Ensure that the MIC is not failed or removed.						
7	If the alarm does not clear, contact your next level of support or your Ciena support group.						

—end—

Procedure 5-22

Laser Failed

Alarm ID: 1513

Probable cause

This alarm is raised when one or more lasers in the Idler facility has failed. If one of the lasers in the Idler pair fails, both lasers in the pair will be shut off. If all IDLER facilities have Laser Failed alarms against them, the Laser Failed alarms will be replaced by a Circuit Pack Failed alarm.

Impact

Major, service-affecting (M, SA) alarm

Prerequisites

Before you perform this procedure, you must

- observe all the safety requirements described in *Installation*, 323-1851-201.0, or *Module Replacement Procedures*, 323-1851-545
- have an antistatic wrist strap to dissipate electrostatic charges

Step	Action	
1	If a spare Idler facility is available on the SLIC10 or SLIC10 Flex C-Band circuit pack, deprovision the failed Idler by putting it OOS and set the wavelengths to 0.0 nm. Refer to the “Changing the primary state of a facility” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.	
2	Provision the spare Idler to have the failed Idler’s original values.	
3	If the original alarm has	Then
	cleared	the procedure is complete
	not cleared	go to step 4
4	If a spare Idler facility is not available on the SLIC10 or SLIC10 Flex C-Band circuit pack, re-evaluate the failed Idler by setting its wavelength to 0.0 nm and then back to its original wavelength. If the problem has cleared, this will trigger re-evaluation and clear the laser failed alarm.	
5	If the original alarm has	Then
	cleared	the procedure is complete
	not cleared	go to step 6

5-62 Alarm clearing procedures—I to Z

Procedure 5-22 (continued)

Laser Failed

Step	Action
6	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf and replace the circuit pack reporting the alarm. Refer to the “Replacing an optical interface circuit pack” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.
7	If the alarm does not clear, contact your next level of support or Ciena support group.

—end—

Procedure 5-23

Laser Frequency Out Of Range

Alarm IDs: 2017, 2049

Probable cause

This alarm is raised when the difference between the nominal provisioned frequency and the actual frequency achieved via the TR controller exceeds the provisioned threshold.

Impact

Major, service-affecting (M, SA) alarm if not protected

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

Step	Action
1	If possible, clear all other alarms from the network.
2	Check the frequency specification at the line port at either end of the fiber span.
3	If the alarm is not clear, verify that the equipment at the far end of the optical line meets the frequency specification. If the equipment does not meet the specification, change the far end equipment to be within specifications.
4	If the alarm did not clear, re-provision the thresholds of the line port. Refer to Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
5	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-24 Licensing Trusted Store Mismatch

Alarm ID: 2013

Probable cause

This alarm is raised when the 6500 software detects that the encrypted license database (Trusted Store) has been modified or does not contain expected shelf identifier.

Impact

Major, non-service-affecting (M, nsa) alarm

Step	Action
1	Operate a License Audit manually or a warm restart the SP/CTM. Refer to the “Restarting a circuit pack or shelf processor” procedure in Part 1 of this document. Note: This alarm will also be cleared automatically after an automatic daily License Audit (default time is 3am).
2	If the alarm does not clear, contact your next level of support or Ciena support group.

—end—

Procedure 5-25

License Violation

Alarm ID: 1999, 2037

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 6500 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.

Impact

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

Critical, non-service-affecting (C, NSA) alarm, when the shelf is in arrears for 10 or more of any feature license. License Violation alarm is defined per release

Procedure 5-25 (continued)

License Violation

Step	Action
	<p>Note: This alarm automatically clears when the licensing software retrieves the missing licenses from the license server/manager.</p>
1	Add the licenses to the license server/manager. The new licenses can be purchased and loaded onto the licensing server.
2	Once the licenses are present on the license server/manager, operate License Audit manually (in Site Manager or TL1). The alarm will also clear after the daily License Audit that occurs nightly (default 3am).
3	If the alarm does not clear, contact your next level of support or Ciena support group.

—end—

Procedure 5-26

Line A Input OTDR High Loss Detected

Alarm ID: 2047

Probable cause

This alarm is raised when the event loss calculated by the OTDR trace is higher than the provisioned threshold either for a single event loss or for the total loss within 20 km.

For SRA circuit packs, this will prevent turning on the Raman pumps.

Since 6500 Release 12.1, all OTDR related parameters and alarms are migrated from the port 5 Telemetry facility to the new OTDRCFG facility on port 8.

Impact

Major, service-affecting (M, SA) alarm

Step	Action
1	Check the additional info field for the alarm for the information about the trace causing the alarm: <ul style="list-style-type: none"> • High Loss - Short Trace • High Loss - Office Trace • Flat Trace - Long Trace
2	Based on which trace is the cause for the alarm, verify the respective trace in the OTDR screen.
3	From the OTDR screen, select the short trace and select the View trace(s) button. The View Trace button can be selected only if a Facility is selected from the Facility Configuration and a Trace is selected from the SOR Trace.
4	In the OTDR Graph View, examine the resulting graph to determine the location of the fault(s).
5	From the graph, find the highest event loss within the first 20km by selecting the View event button.
6	If the highest loss is outside of the fiber plant, re-spliced the fiber at that location.
7	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 the "Cleaning connectors" chapter in <i>Installation - General Information</i> , 323-1851-201.0.
8	If cleaning connectors fails to resolve the issue, replace faulty fiber patch cords.

5-68 Alarm clearing procedures—I to Z

Procedure 5-26 (continued)

Line A Input OTDR High Loss Detected

Step	Action
9	Once the fiber is reconnected, the OTDR Traces run automatically. If the new trace passes, the alarm will clear.
10	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-27

Line A Input OTDR High Reflection Detected

Alarm ID: 2048

Probable cause

This alarm is raised when the event reflection calculated by the OTDR trace is higher than the provisioned threshold either for a single event reflection or for the total reflection within 20 km.

For SRA circuit packs, this will prevent turning on the Raman pumps.

Since 6500 Release 12.1, all OTDR related parameters and alarms are migrated from the port 5 Telemetry facility to the new OTDRCFG facility on port 8.

Impact

Major, service-affecting (M, SA) alarm

Step	Action
1	Check the additional info field for the alarm for the information about the trace causing the alarm: <ol style="list-style-type: none"> High Reflection - Short Trace High Reflection - Office Trace Flat Trace - Long Trace
2	Based on which trace is the cause for the alarm, the respective trace should be checked in the OTDR screen.
3	In the OTDR Graph View, examine the resulting graph to determine the location of the fault(s).
4	From the graph, find the largest event Reflection within the first 20km by selecting the View event button.
5	Check proper connections at patch panels or replace pads if any.
6	If the largest Reflection is outside of the fiber plant, re-spliced the fiber at that location.
7	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 the “Cleaning connectors” chapter in <i>Installation - General Information</i> , 323-1851-201.0.

Procedure 5-27 (continued)

Line A Input OTDR High Reflection Detected

Step	Action
8	If cleaning connectors fails to resolve the issue, replace faulty fiber patch cords.
9	Once the fiber is reconnected, the OTDR Traces run automatically. If the new trace passes, the alarm will clear.
10	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-28

Line Adjacency Manual Provisioning Required

Alarm IDs: 1945

Probable cause

This warning is raised against the ADJ-LINE facility when the equipment is provisioned as the LIM slot in an OTS and the Target Span Loss has a default value of 0 dB.

When the Target Span Loss is 0 the “High Received Span Loss” (HRSL) alarm is disabled. When the HRSL alarm is disabled, DOC’s ability to compensate for changing span losses is compromised and there is a risk of power overshoots if the span loss increases and then drops again.

Applies to all LIM equipment variants (for example, SLA, MLA, MLA2v) and to all other equipment which can be provisioned as the LIM slot (SAM, ESAM, SRA, and RLA).

Impact

Warning

Step	Action
1	Provision the Target Span Loss to the expected value as per network link budgets. Refer to the “Editing facility parameters” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
2	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-29

Line Flapping

Alarm ID: 1774

Probable cause

If the Line Flapping alarm is enabled, the alarm is raised against the TCMTTP facility (not any other provisioned TCMTTP on the same line) for the OSRP line of a 100G PKT/OTN XCIF, 10x10G PKT/OTN I/F, 10x10G OTN I/F, or 40G OTN XCIF circuit pack when the line is oscillating beyond the provisioned Line Flapping Alarm Threshold within the provisioned Line Flapping Alarm Raise Time. The alarm is present on the system for the affected TCMTTP for the period defined in the provisioned Line Flapping Alarm Clear Time. These Line Flapping alarm settings are applicable to all lines on the NE. For more information on the Line Flapping Alarm Clear Time, Line Flapping Alarm Raise Time, and Line Flapping Alarm Threshold parameters, refer to the “Node information” chapter in *Administration and Security*, 323-1851-301.

For example, if the Line Flapping Alarm Threshold is provisioned to three, the Line Flapping Alarm Raise Time is provisioned to 300 seconds, and the Line Flapping Alarm Clear Time is provisioned to 600 seconds, then three events (such as LOS) must occur within 300 seconds for the alarm to raise. The alarm will be active for 600 seconds. If the line continues to oscillate during this period and the alarm is masked by a higher priority events (see triggers below), then the alarm is raised again and the Line Flapping Alarm Clear Time timer is restarted.

The alarm can also be raised based on the following supported TCM triggers:

- LOS, LOF, or LOM condition
- TCM ODU AIS, OCI, LCK, LTC, or LOF condition
- Disabling the Line Flapping alarm or disabling/re-enabling the Line Flapping alarm clears all Line Flapping alarms on the NE
- the provisioned Line Flapping Alarm Clear Time is reached
- the provisioned Line Flapping Alarm Raise Time is reached
- the provisioned Line Flapping Alarm Threshold is reached

Impact

Major, service-affecting (M, SA) alarm

Procedure 5-29 (continued)

Line Flapping

Prerequisites

To perform this procedure, you must have the optical fiber connection information (that is, how the circuit packs on each network element connect to other network elements).

Step	Action
1	Retrieve all alarms at the transmit end of the line. Clear any higher order alarms using the appropriate procedure.
2	If the original alarm has Then
	cleared the procedure is complete
	not cleared go to step 3
3	Verify that the provisioned line rate on the upstream circuit pack matches the line rate on the local circuit pack. Correct any mismatches.
4	If the original alarm has Then
	cleared the procedure is complete
	not cleared go to step 5
5	Verify that the FEC setting on the upstream circuit pack matches the FEC setting on the local circuit pack. Correct any mismatches. Refer to the “Retrieving equipment and facility details” or “Editing facility parameters” procedures in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
6	If the original alarm has Then
	cleared the procedure is complete
	not cleared go to step 7
7	If a photonic line system is used to transport the signal of the circuit pack raising the alarm, retrieve all alarms on the photonic line system. Clear any alarms on the photonic line system associated with the alarmed channel using the appropriate procedures.
8	If the alarm does not clear, restart the circuit pack reporting the alarm. Refer to the “Restarting a circuit pack or shelf processor” procedure in Part 1 of this document.
9	If the alarm does not clear, disable the Line Flapping Alarm globally and re-enable the Line Flapping Alarm parameter to reset the alarm. Refer to “Editing the nodal system parameters” procedure in <i>Administration and Security</i> , 323-1851-301.

5-74 Alarm clearing procedures—I to Z

Procedure 5-29 (continued)

Line Flapping

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

—end—

Procedure 5-30

Link Aggregation Group Fail

Alarm ID: 691

Probable cause

This alarm is raised against a Link Aggregation Group (LAG) when the LAG admin state is in-service (IS), but there is no member port able to carry traffic (there are no member ports in a LAG or all the member ports are failed). This can be caused when one of the following conditions occurs:

- all member ports are out of service (OOS)
- there is a Link Down alarm on all member ports
- there is Loss Of Signal (LOS) on all member ports

This alarm applies to the L2SS, 20G L2SS, L2MOTR, PDH gateway, and RPR circuit packs.

Impact

Critical, service-affecting (C, SA) alarm, if L2 endpoints are provisioned
Minor, non-service-affecting (m, NSA) alarm, if no L2 endpoints are provisioned

Prerequisites

To perform this procedure, you must observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545.

Step	Action
1	Verify the status of LAG member ports.
2	If the LAG
	does not have member ports
	has member port(s)
3	Set the LAG admin state to OOS. Refer to the “Changing the primary state of a facility” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310. Go to step 7 .
4	Set the member port(s) state(s) to IS. Refer to the “Changing the primary state of a facility” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
5	Retrieve all alarms to determine if the original alarm has cleared.

5-76 Alarm clearing procedures—I to Z

Procedure 5-30 (continued)

Link Aggregation Group Fail

Step	Action
6	Clear the alarms on member ports using the appropriate alarm clearing procedures. At least one member port must be able to carry traffic (not under failure condition).
7	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-31

Link Aggregation Group Partial Fail

Alarm ID: 939

Probable cause

This alarm is raised against a Link Aggregation Group (LAG) when the LAG admin state is in-service (IS), but there is one or more (but not all) member ports unable to carry traffic. This can be caused when one of the following conditions occurs:

- a member port is out of service (OOS)
- there is a Link Down alarm on a member port
- there is Loss Of Signal (LOS) on a member port

This alarm applies to the RPR circuit pack.

Impact

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

Prerequisites

To perform this procedure, you must observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545.

Step	Action
1	Verify the status of LAG member ports.
2	Set the member port(s) state(s) to IS. Refer to the “Changing the primary state of a facility” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
3	Retrieve all alarms to determine if the original alarm has cleared.
4	Clear the alarms on member ports using the appropriate alarm clearing procedures. All of the member ports must be able to carry traffic (not under failure condition).
5	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-32

Link Data Retrieval In Progress

Alarm IDs: 1884

Probable cause

This alarm is raised when a user invokes the link data collection process for the PTP facility in the Site Manager.

Impact

Warning

Step	Action
------	--------

- | | |
|---|--|
| 1 | No action is required. The alarm clears when the data collection process is completed. |
| 2 | If the alarm does not clear or is unexpected, contact your next level of support or Ciena support group. |

—end—

Procedure 5-33

Link Data Save In Progress

Alarm IDs: 1886

Probable cause

This alarm is raised when a user invokes a link data save process.

Impact

Warning

Step	Action
-------------	---------------

- 1 No action is required. The alarm clears when the link data save process is completed.
- 2 If the alarm does not clear or is unexpected, contact your next level of support or Ciena support group.

—end—

Procedure 5-34

Link Down

Alarm IDs: 333, 334, 367, 821, 865, 1975

Probable cause

This alarm is raised against

- an ETH or WAN facility of a 4xGE, 20G L2SS, L2SS, PDH gateway, L2 MOTR, 8xOTN Flex MOTR, (1+8)xOTN Flex MOTR, or RPR circuit pack
- an ETH10G or WAN facility of a FLEX MOTR circuit pack
- an ETH10G or WAN facility of a 1x10GE EPL circuit pack
- an ETH100 or WAN facility of a 24x10/100BT circuit pack
- a WAN facility of a 10G OTR, 10G OTSC, 2x10G OTR, 4x10G OTR, (1+2) 100G PKT/OTN I/F, 10X10G PKT/OTN I/F, 10x10G MUX OCI, 100G (2xQSFP+/2xSFP+) MUX, 200G (2x100G/5x40G) MUX, 5x100G/12x40G QSFP PKT/OTN IF, 40x10G SFP+ PKT/OTN IF, X-Conn 800G PTS, or 40G MUX OCI circuit pack
- an ETH, ETH100, FC100/FC200/FC400, or WAN facility of a SuperMux circuit pack

This alarm is raised against an Ethernet facility of a 4xGE, 1x10GE EPL, 24x10/100BT, 20G L2SS, L2SS, PDH gateway, L2 MOTR, FLEX MOTR, RPR, or SuperMux circuit pack when one of the following occurs:

- a fiber is disconnected
- conditioning exists at the far-end
- the auto-negotiation between the 4xGE, 24x10/100BT, 20G L2SS, L2SS, PDH gateway, L2 MOTR, FLEX MOTR, or RPR circuit pack and the subtending client equipment does not complete successfully
- the auto-negotiation setting on the 4xGE, 24x10/100BT, 20G L2SS, L2SS, PDH gateway, L2 MOTR, FLEX MOTR, 8xOTN Flex MOTR, or RPR circuit pack does not match the auto-negotiation setting on the subtending client equipment
- the administrative state of a facility on the 4xGE, 24x10/100BT, 20G L2SS, L2SS, PDH gateway, L2 MOTR, FLEX MOTR, 8xOTN Flex MOTR, RPR, or SuperMux circuit pack is up, but the operating state of the facility is down (the subtending equipment may be defective).

Procedure 5-34 (continued)

Link Down

This alarm is raised against a WAN facility of a 4xGE, 1x10GE EPL, 24x10/100BT, 20G L2SS, L2SS, PDH gateway, L2 MOTR, FLEX MOTR, 8xOTN Flex MOTR, (1+8)xOTN Flex MOTR, RPR, 10G OTR, 10G OTSC, 2x10G OTR, 4x10G OTR, 10x10G MUX OCI, 40G MUX OCI, or SuperMux circuit pack when the administrative state of a facility is up, but the operating state of the facility is down. When the Link Down alarm is raised against the WAN facility, the link cannot carry traffic. The Link Down alarm raised against a WAN facility masks the Link Down alarm against an Ethernet or Fiber Channel facility.

When one of the following alarms is raised, the Link Down alarm is raised against the WAN facility:

- Client Service Mismatch
- Loss of Alignment - VCAT
- Loss of Frame Delineation
- Loss of Multiframe - VCAT
- Loss of Sequence - VCAT

When LCAS is enabled, the WAN Link Down alarm is raised when all VCG members fail. When LCAS is disabled, the WAN Link Down alarm is raised when any one VCG member fails.

This alarm is raised against an FC100/FC200/FC400 facility of a SuperMux circuit pack when one of the following occurs:

- a fiber is disconnected
- conditioning at the far-end (for example, the laser at the far-end circuit pack is shut down)
- the Fiber Channel link state is not active (the subtending equipment might be defective)

ATTENTION

For electrical SFPs (NTTP61BA), if this alarm is raised and the traffic cannot be brought up, change the TXCON state to Disabled.

Impact

Critical, service-affecting (C, SA) alarm
Minor, non-service-affecting (m, NSA) alarm

Prerequisites

To perform this procedure, you must

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0
- 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

Step	Action	
1	If the alarm was raised against	Then go to
	an Ethernet or Fiber Channel facility	step 2
	a WAN facility	step 6

Alarm raised against an Ethernet or Fiber Channel facility

- 2 Clear any alarms raised against the Ethernet or Fiber Channel facility of the circuit pack raising the alarm.
- 3 Ensure that the subtending client equipment is correctly provisioned, functioning, and transmitting a valid signal.
- 4 Ensure that the fiber between the subtending equipment and the Ethernet or Fiber Channel port is properly connected and is not damaged.
- 5 Ensure that the auto-negotiation setting provisioned on the subtending equipment matches the auto-negotiation setting provisioned on the 4xGE, 24x10/100BT, 20G L2SS, L2SS, PDH gateway, L2 MOTR, FLEX MOTR, 8xOTN Flex MOTR, (1+8)xOTN Flex MOTR, or RPR circuit pack. To determine the auto-negotiation setting, refer to the “Retrieving equipment and facility details” procedure in Part 1 of *Configuration - Provisioning and Operating*, 323-1851-310.

Go to [step 14](#).

Alarm raised against the WAN facility

6	If the alarm was raised against	Then go to
	a MSPP or SuperMux circuit pack	step 7
	another type of circuit pack	step 9

Procedure 5-34 (continued)

Link Down

—end—

Procedure 5-35 Link Pulse Missing

Alarm ID: 829

Probable cause

This alarm is raised against the LAN facility of the 24x10/100BT circuit pack when the associated port on the I/O panel does not receive a link pulse.

Impact

Critical, service-affecting (C, SA) alarm

Requirement

To perform this procedure, you must observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545.

Step	Action
1	Ensure that the RJ45 connector is inserted into the 48x10/100BT I/O panel port.
2	Ensure that auto-negotiation settings on the facility and the client are compatible. Refer to the “Retrieving equipment and facility details” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
3	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-36

Local Optical Controller Disabled

Alarm ID: 1950

Probable cause

This alarm is raised against the shelf when the Coherent Select Controller (CSCTRL) system parameter is disabled and there is at least one Coherent Select OTS provisioned on the shelf.

Impact

Warning

Step	Action
1	Enable the CSCTRL system parameter. Refer to “Enabling Coherent Select control” procedure in <i>WaveLogic Photonics Coherent Select</i> , 323-1851-980.
2	If the alarm does not clear, contact your next level of support or Ciena support group.

—end—

Procedure 5-37

Log Collection In Progress

Alarm ID: 1048

Probable cause

This alarm is raised when a user invokes the log collection process from the TL1 interface or from the Faults > Card Logs menu in Site Manager.

This alarm is also raised when you select “Capture logs before restart” in the confirmation window of the Faults > Restart menu of the Site Manager.

Impact

Warning

Step	Action
1	No action is required. The alarm clears when the log collection process is completed.
2	If the alarm does not clear or is unexpected, contact your next level of support or Ciena support group.

—end—

Procedure 5-38

Log Save In Progress

Alarm ID: 1569

Probable cause

This alarm is raised when a log save is in process.

For an active SP, the restart takes eight to 15 minutes. For other circuit packs, the restart takes four to 10 minutes to complete.

If after the expected time the retrieve log is not completed, Site Manager automatically issues the restart command. Refer to the “Restarting a circuit pack or shelf processor” procedure in Part 1 of this document for more information.

Impact

Warning

Step	Action
------	--------

- 1 No action is required. The alarm clears when the log save process is completed.
- 2 If the alarm does not clear or is unexpected, contact your next level of support or Ciena support group.

—end—

Procedure 5-39

Loopback Active

Alarm IDs: 26, 45, 97, 235, 329, 330, 331, 585, 652, 864, 898, 1130, 1696

Probable cause

This alarm is raised when a loopback is active on an DS1, DS1DS3, DS3, E1, E1DS3, E1E3, E3, OC-3/STM-1/STM-1J/STM-1e, OC-12/STM-4/STM-4J, OC-48/STM-16, OC-192/STM-64, or FC100/FC200/FC400 facility. The loopback active alarm is an important advisory message, as the unavailability of a circuit can affect maintenance performed at the same time. If more than one user logs into a network element and one user operates a loopback, the other users receive this message.

Execute loopbacks only during system testing. The facility is in out of service, maintenance (OOS-MA) mode while in loopback mode.

Impact

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

Prerequisites

To perform this procedure, you must

- use an account with at least a level 3 UPC
- have the connection information (that is, how the optical/electrical modules on each network element connect to other network elements)

Step	Action
1	If the alarm is raised during facility testing, no action is required. The alarm will clear once the testing is complete and the loopback is released.
2	If the alarm is unexpected, identify the circuit pack raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document. This procedure assumes that testing is complete and the circuit is ready to be released from loopback mode.
3	Release the loopback. Refer to the “Operating/releasing a loopback” procedure in Part 1 of Configuration - Provisioning and Operating, 323-1851-310.

—end—

Procedure 5-40

Loopback Active - Facility

Alarm IDs: 370, 372, 605, 634, 637, 826, 833, 845, 848, 852, 908, 909, 910, 911, 912, 913, 914, 948, 990, 997, 1165, 1251, 1303, 1350, 1448, 1457, 1466, 1784, 2068, 2091

Probable cause

This alarm is raised when a facility loopback is active.

Note that a mapped ETTP does not support facility or terminal loopbacks. A terminated ETTP supports facility loopback only. A monitor ETTP supports both facility and terminal loopbacks.

This alarm is also raised when a channelized facility (path-level or connection) loopback is applied to a VT1.5/VC-11, VT2/VC-12, STS-1/VC-3, STS-3c/VC-4, STS-12c/VC-4-4c, STS-24c/VC-4-8c or STS-48c/VC-4-16c connection.

This alarm can be raised against an OTUTTP facility of the 10x10G PKT/OTN I/F, 100G WL3/WL3e OCLD, eMOTR, and 100G OCI.

Perform loopbacks only during system testing.

Impact

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

Prerequisites

To perform this procedure, you must:

- use an account with at least a level 2 UPC
- have the fiber connection information for the line-level loopbacks (that is, how the optical modules on each network element connect to other network elements)

Procedure 5-40 (continued)

Loopback Active - Facility

Step	Action
<p>Note: If the alarm is raised during facility/connection testing, no action is required. The alarm will clear once the testing is complete and the loopback is released.</p>	
1	Identify the facility/connection in loopback mode. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document.
2	Release the loopback on the facility/connection identified in step 1 . For line-level loopbacks, refer to the “Operating/releasing a loopback” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310. For channelized loopbacks, refer to the “Operating/releasing a channelized loopback” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.

—end—

Procedure 5-41

Loopback Active - Terminal

Alarm IDs: 371, 373, 606, 635, 638, 827, 853, 915, 916, 917, 918, 919, 920, 921, 935, 1159, 1166, 1214, 1215, 1216, 1217, 1242, 1305, 1449, 1458, 1467, 1740, 1785, 2069, 2092

Probable cause

This alarm is raised when a terminal line-level loopback is active.

Note that a mapped ETTP does not support facility or terminal loopbacks. A terminated ETTP supports facility loopback only. A monitor ETTP supports both facility and terminal loopbacks.

This alarm is also raised when a channelized terminal (path-level or connection) loopback is applied to a VT1.5/VC-11, VT2/VC-12, STS-1/VC-3, STS-3c/VC-4, STS-12c/VC-4-4c, STS-24c/VC-4-8c or STS-48c/VC-4-16c connection.

This alarm can be raised against an OTUTTP facility of the 10x10G PKT/OTN I/F, 100G Perform loopbacks only during system testing.

Impact

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

Prerequisites

To perform this procedure, you must

- use an account with at least a level 2 UPC
- have the fiber connection information for the line-level loopbacks (that is, how the optical modules on each network element connect to other network elements).

Step	Action
	Note: If the alarm is raised during facility/connection testing, no action is required. The alarm will clear once the testing is complete and the loopback is released.
1	Identify the facility/connection in loopback mode. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document.

- 1 Identify the facility/connection in loopback mode. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document.

Procedure 5-41 (continued)

Loopback Active - Terminal

Step	Action
2	<p>Release the loopback on the facility/connection identified in step 1.</p> <p>For line-level loopbacks, refer to the “Operating/releasing a loopback” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i>, 323-1851-310.</p> <p>For channelized loopbacks, refer to the “Operating/releasing a channelized loopback” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i>, 323-1851-310.</p>

—end—

Procedure 5-42

Loopback Traffic Detected

Alarm ID: 1218

Probable cause

This alarm is raised when WAN traffic is returned back to the 6500 L2 service. This alarm is raised only when the WAN port is configured to detect for traffic that has returned. Loopback detection is provisionable and by default is disabled.

Impact

Critical, service-affecting (C, SA) alarm

Prerequisites

To perform this procedure, you must observe all the safety requirements described in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545.

Step	Action
1	Verify the location of the WAN facility where the loopback originated.
2	Remove the loopback condition on L1.
3	Verify that the alarm clears and egress traffic resumes after 10 seconds.
4	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-43 **Loss of Alignment Marker**

Alarm IDs: 2033

Probable cause

This alarm is raised on ETTP (ETH100G) clients that use parallel optics when the Invalid lane marker (a marker that does not match one of the encodings in Table 82-2 of IEEE 802.3ba) is detected on any lane.

Impact

Critical, service-affecting (C, SA) alarm

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

Prerequisites

To perform this procedure, you must

- have the optical fiber connection information (that is, how the circuit packs on each network element connect to other network elements)
 - have an optical power meter with the same optical connectors as the network element
 - observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0
 - have an antistatic wrist strap to dissipate electrostatic charges

Step	Action
1	Identify the circuit pack and facility raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document.
2	Use the optical fiber/cable connection information to identify the transmit and receive sites of the alarmed signal.
3	Log into the remote network element at the transmit end.
4	Retrieve all alarms at the transmit end. Clear any higher order alarms using the appropriate procedure.
5	If the original alarm has Then
cleared	the procedure is complete
not cleared	go to step 6

Procedure 5-43 (continued) **Loss of Alignment Marker**

Step	Action
6	Verify that the provisioned line rate on the upstream circuit pack matches the line rate on the local circuit pack. Correct any mismatches. Refer to the “Retrieving OTM info” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
7	If the original alarm has Then
	cleared the procedure is complete
	not cleared go to step 8
8	If a photonic line system is used to transport the signal of the circuit pack raising the alarm, retrieve all alarms on the photonic line system. Clear any alarms on the photonic line system associated with the alarmed channel using the appropriate procedures.
9	If the original alarm has Then
	cleared the procedure is complete
	not cleared perform a warm restart on the circuit pack reporting the alarm. “Restarting a circuit pack or shelf processor” procedure in Part 1 of this document.
10	If the original alarm has Then
	cleared the procedure is complete
	not cleared the receive circuit pack is faulty. Replace the circuit pack reporting the alarm. Refer to the “Replacing an optical interface circuit pack” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.
11	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-44

Loss of Alignment - VCAT

Alarm IDs: 359, 360, 687, 688, 733, 734, 735, 930, 933, 1381

Probable cause

This alarm is raised when the STS/VC/PDH members in a virtually concatenated group cannot be aligned because of excessive differential delay between the STS/VC/PDH members. This alarm is raised against the slowest STS/VC/PDH member in the virtually concatenated group that connects to the WAN facility of a 4xGE, 1x10GE, 24x10/100BT, L2SS, PDH gateway, RPR, or SuperMux circuit pack.

Maximum differential delay values can be found in the *Data Application Guide*, NTRN15BA, in the Bandwidth Management section. Latency information can be found in *Latency Specifications*, 323-1851-170. Approximately 200 km of optical fiber causes 1 ms of delay.

Impact

Critical, service-affecting (C, SA) alarm

Prerequisites

To perform this procedure, you must:

- use an account with at least a level 3 UPC
- have the fiber connection information (that is, how the optical modules on each network element connect to other network elements)

Step	Action
1	Identify the STS/VC/PDH on the optical interface circuit pack raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document. The Unit field in the Active Alarms application specifies the circuit pack, slot, port (if applicable), and STS/VC/PDH number.
2	Trace the route of all the VCG STS/VC/PDH paths, including protection and working paths. Look for paths which are significantly longer or shorter than others. Refer to the “Retrieving path connections” procedure in Part 1 of <i>Configuration - Bandwidth and Data Services</i> , 323-1851-320.

Procedure 5-44 (continued)
Loss of Alignment - VCAT

Step	Action
3	Reprovision the paths of the WAN VCG so that as many paths as possible have similar distances, and pass through a similar number of nodes. Refer to the “Adding a path connection” procedure in Part 1 of <i>Configuration - Bandwidth and Data Services</i> , 323-1851-320.
4	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-45

Loss of Channel

Alarm IDs: 1311, 1570, 1596

Probable cause

This alarm is raised when the optical power is below the Loss of channel threshold.

For 40G/100G OCLD circuit packs, the power level must be above the LOC clear threshold value for traffic to recover. For 40G/100G OCLD circuit packs, traffic can run below the LOC threshold value. However, if traffic is lost, traffic will not recover until the power level is above the LOC clear threshold. See the “Technical specifications” tables in *WaveLogic Ai, Flex, 100G+, 40G, OSIC ISS, and SLIC10 Circuit Packs*, 323-1851-102.4 for the 40G/100G OCLD expected LOS alarm clear threshold values.

Impact

Critical, service-affecting (C, SA) alarm, unprotected
Minor, non-service-affecting (m, NSA) alarm, protected

Prerequisites

To perform this procedure, you must:

- have the optical fiber connection information (that is, how the circuit packs on each network element connect to other network elements)
- have an optical power meter with the same optical connectors as the network element
- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0
- have an antistatic wrist strap to dissipate electrostatic charges

Step	Action
1	Identify the circuit pack and facility raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document.
2	If the “Rx Channel Power Out of Range” alarm is active, clear this alarm first. Refer to “ Rx Channel Power Out of Range ” on page 5-453 in this document.

Procedure 5-45 (continued)

Loss of Channel

Step	Action
3	If the original alarm has cleared the procedure is complete not cleared go to step 4
4	Check the corresponding upstream circuit pack and photonic layer for failures or alarms. Troubleshoot these alarms/failures before proceeding.
5	In the Site Manager Configuration menu, select the Equipment & Facility Provisioning application. Select the alarmed facility and retrieve the value from the Rx Channel Actual Power (dBm) column of the facility table. Refer to the “Retrieving optical power, wavelength, and dispersion ranges” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310. If the received power is out of the power monitoring range for the facility, the Rx Actual Power (dBm) column will display “OOR-HI” or “OOR-LO” instead of a numerical value.
6	Click on the Ranges button to compare the Rx Channel Actual Power (dBm) value with the Rx Channel minimum power (dBm) and Rx Channel maximum power (dBm) values displayed.
7	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
8	Use the optical power meter to measure the optical power level at the far-end upstream monitored point. Also, verify that the loss between the far-end transmitter and the Mux is an expected value.
9	If the value of the loss is unexpected troubleshoot the fiber or Photonic layer equipment expected go to step 9
10	If the original alarm has cleared the procedure is complete not cleared restart the circuit pack reporting the alarm. Refer to the “Restarting a circuit pack or shelf processor” procedure. If the original alarm has cleared the procedure is complete not cleared reseat the circuit pack reporting the alarm. Refer to the “Reseating a circuit pack” procedure in Part 1 of this document.

5-100 Alarm clearing procedures—I to Z

Procedure 5-45 (continued)

Loss of Channel

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

—end—

Procedure 5-46 Loss of Clock

Alarm IDs: 840, 843, 846, 991, 998, 1167, 1255, 1296, 1452, 2016

Probable cause

This alarm is raised when the measured frequency of the input client clock exceeds the allowed frequency deviation outlined by the corresponding standard or when the provisioned line rate at the far-end circuit pack does not match the line port rate at the near-end circuit pack.

In general, the LOC alarm is raised when the measured frequency of the input client clock exceeds the allowed frequency deviation outlined by the corresponding standard or when the provisioned line rate at the far-end circuit pack does not match the line port rate at the near-end circuit pack.

More specifically, for the following 6500 transport cards, NTK525CA, NTK525CF, NTK529BB/NTK529BX, the “Frequency OOR” alarm is raised when the measured frequency of the input client clock is greater than +/- 27.5ppm (OC192/STM64) or +/-107.5ppm (ETH10G).

The “Loss of Clock” alarm is raised when the measured frequency of the input client clock does not improve beyond the “Frequency OOR” limits or when the provisioned line rate at the far-end circuit pack does not match the line port rate at the near-end circuit pack.

The Frequency OOR alarm does not force conditioning and alarm does not apply to NTK525CA when ETH10G is provisioned with GFP mapping.

For the FLEX MOTR circuit pack this alarm is raised if;

- The subtending equipment is faulty and transmitting its signal with an out-of-spec frequency.
- The FLEX MOTR SFP is faulty and/or operating out of spec due to a hardware failure or environmental condition.
- The FLEX MOTR HW is faulty and should be replaced.

Procedure 5-46 (continued)

Loss of Clock

Any terrestrial variant of 100G OCLD circuit packs (NTK539TAE5-NTK539TDE5 and NTK539TJE5) can interwork with any other terrestrial variant of 100G OCLD circuit packs (NTK539TAE5-NTK539TDE5 and NTK539TJE5) but the performance will be reduced to the 100G OCLD circuit pack with the lesser performance specifications. The submarine variant of 100G OCLD circuit packs (NTK539TEE5) does not interwork with any terrestrial variant of 100G OCLD circuit packs (NTK539TAE5-NTK539TDE5 and NTK539TJE5). The OTM4 facility “Loss of Clock” alarm is raised against both 100G OCLD circuit packs.

Upon the differential encoding mismatch detection, “Loss of Clock” alarm is expected if SOFT differential encoding is involved at one of the two ends. This applies to all WL3/WL3e OCLDs, WL3e OTR, WL3n MOTR, and WL3n OTR circuit packs.

Impact

Critical, service-affecting (C, SA) alarm, unprotected
Minor, non-service-affecting (m, NSA) alarm, protected

Prerequisites

To perform this procedure, you must:

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0
- have an antistatic wrist strap to dissipate electrostatic charges
- have the optical fiber connection information (that is, how the circuit packs on each network element connect to other network elements)
- have an optical power meter with the same optical connectors as the network element
- have a fiber cleaning kit
- obtain a replacement VOA, if required
- obtain a replacement circuit pack, if required

Step Action

- 1 Ensure the subtending equipment is working properly and providing an error-free signal that meets the allowed frequency deviation specifications.

Procedure 5-46 (continued)

Loss of Clock

Step	Action				
2	Ensure that all the optical fibers between the subtending equipment Tx port and at the alarmed circuit pack Rx port are correctly connected.				
3	Ensure that the line rate or the client type is the same for both ends of the link.				
4	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.				
5	Use an optical power meter to measure the received power level at the Rx port of the alarmed circuit pack. Verify if the Rx power level is within the operational threshold. Record the value. For information about circuit pack technical specifications, refer to the “Technical specifications” chapter in Part 3 of 6500 <i>Planning</i> , NTRN10EG.				
6	<p>If there is Then</p> <table> <tr> <td>a VOA attached to the fiber between the alarmed circuit pack and the subtending equipment</td> <td>re-adjust, check for proper functionality, and, if necessary, replace the VOA. Note: If the circuit pack is unprotected, adjusting the VOA may impact traffic. If necessary, route traffic to an alternate path.</td> </tr> <tr> <td>no VOA attached to the fiber between the alarmed circuit pack and the subtending equipment</td> <td>Go step 7. go to step 8</td> </tr> </table>	a VOA attached to the fiber between the alarmed circuit pack and the subtending equipment	re-adjust, check for proper functionality, and, if necessary, replace the VOA. Note: If the circuit pack is unprotected, adjusting the VOA may impact traffic. If necessary, route traffic to an alternate path.	no VOA attached to the fiber between the alarmed circuit pack and the subtending equipment	Go step 7 . go to step 8
a VOA attached to the fiber between the alarmed circuit pack and the subtending equipment	re-adjust, check for proper functionality, and, if necessary, replace the VOA. Note: If the circuit pack is unprotected, adjusting the VOA may impact traffic. If necessary, route traffic to an alternate path.				
no VOA attached to the fiber between the alarmed circuit pack and the subtending equipment	Go step 7 . go to step 8				
7	<p>If the original alarm has Then</p> <table> <tr> <td>cleared</td> <td>the procedure is complete</td> </tr> <tr> <td>not cleared</td> <td>go to step 8</td> </tr> </table>	cleared	the procedure is complete	not cleared	go to step 8
cleared	the procedure is complete				
not cleared	go to step 8				
8	Use a cleaning kit to clean all the connectors between the subtending equipment Tx port and the alarmed Rx port. Refer to the cleaning connectors procedures in <i>Installation - General Information</i> , 323-1851-201.0.				
9	Record the operating power level after you clean each connector and compare it to the value recorded in step 5 . This will allow you to see if there is any improvement to the Rx power.				
10	<p>If the original alarm has Then</p> <table> <tr> <td>cleared</td> <td>the procedure is complete</td> </tr> <tr> <td>not cleared</td> <td>go to step 12</td> </tr> </table>	cleared	the procedure is complete	not cleared	go to step 12
cleared	the procedure is complete				
not cleared	go to step 12				

Procedure 5-46 (continued)

Loss of Clock

—end—

Procedure 5-47

Loss Of Data Synch

Alarm IDs: 348, 366, 825, 868, 1256, 1304, 1587

Probable cause

This alarm is raised against:

- an Ethernet facility of a 4xGE,1x10GE EPL, 24x10/100BT, 20G L2SS, L2SS, PDH gateway, L2 MOTR, 100G OCI, 4x10G OTR, 200G (2x100G/5x40G) MUX, or RPR circuit pack
- a FLEX facility of FLEX MOTR, 8xOTN Flex MOTR, 4x10G OTR, or (1+8)xOTN Flex MOTR circuit pack
- an ETTP facility of a PTS MRO IF 2xSFP+/14xSFP, X-Conn 800G PTS, 16xFLEX OTN I/F or eMOTR circuit pack
- an ETH or FC100/FC200/FC400 facility of a SuperMux circuit pack
- FC800/FC1200 clients of a 2x10G OTR (NTK530PME5 variant), 4x10G OTR, or FC800/FC1200 clients of 40G MUX OCI (NTK525CF) circuit pack
- ETH40G clients of a 40G+ CFP OCI (NTK529SJ) circuit pack
- a Gigabit Ethernet (GE) port on PKT I/F GE 48xSFP circuit pack (NTK642AA)

when one of the following conditions occurs:

- The circuit pack cannot establish bit synchronization or transmission word synchronization.
- The incorrect type of SFP/XFP optical transceiver module (SX, LX, BX, or ZX) is installed.
- The client service on the subtending equipment does not match the client service provisioned on the corresponding port of the circuit pack. For example, a Fiber Channel signal is connected to a 4xGE,1x10GE EPL, 24x10/100BT, 20G L2SS, L2SS, PDH gateway, L2 MOTR, or RPR circuit pack port; or the XFP of the 1x10GE EPL circuit pack is incorrectly connected to an OC192/STM64 optical interface.
- There is an auto-negotiation provisioning mismatch between the connected subtending equipment (a test set for example) and the corresponding port on the circuit pack.

Procedure 5-47 (continued)

Loss Of Data Synch

- For ETH100G and ETH40G clients that use parallel optics, the Virtual Lane (VL) Skew exceeds the IEEE 802.3ba VL Skew range or if duplicate alignment markers are detected.
- For the ETTP facility of eMOTR, ETTP facility figures secondary state is Layer-2 port disabled. This phenomenon can happen due to VLLI port conditioning.

When VLLI UP MEP port conditioned due to FEND UP MEP failure, NEND ETTP facility will have Loss Of Data Synch (for GE port and GE LAG)/Loss Of Frame (for 10G port or 10G LAG), indicating FEND port having an issue.

If UP MEP VLLI belonging port created on LAG client port then only Lead member (known to be least numbered LAG member port) shows the alarm and all member ports will declare L2 port disabled.

Similarly in case of Inverse VLLI operations, destination port instance (GE port or GE LAG) shuts off laser with Loss of Data Synch during normal operation of source port. This alarm clears when source port undergoes faults and destination port enabled by clearing LODS alarm and the same port will have “Service Defect Indication” alarm indicating Inverse VLLI conditioning is activated.

Impact

Critical, service-affecting (C, SA) alarm if not protected
Minor, non-service-affecting (m, NSA) alarm if protected

Prerequisites

To perform this procedure, you must:

- have the fiber connection information (that is, how the optical modules on each network element connect to other network elements)
- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0
- have an antistatic wrist strap to dissipate electrostatic charges
- if required, obtain a replacement SFP/XFP
- use an account with at least a level 3 UPC

Procedure 5-47 (continued)

Loss Of Data Synch

Step	Action
1	Determine the type of client service on the subtending equipment connected to the port of the circuit pack reporting the alarm.
2	Determine the facility (Ethernet, FLEX, or Fiber Channel) provisioned on the port of the circuit pack reporting the alarm.
3	If the subtending equipment noted in step 1 is not provisioned with an Ethernet, FLEX, or Fiber Channel Then go to step 4 service as required by the facility noted in step 2 provisioned with an Ethernet, FLEX, or Fiber Channel Then go to step 6 service as required by the facility noted in step 2
4	The 4xGE, 1x10GE EPL, 24x10/100BT, 20G L2SS, L2SS, PDH gateway, L2 MOTR, or RPR circuit packs only support Ethernet client services. If possible, provision the subtending equipment for Ethernet client services. Otherwise, contact your next level of support or your Ciena support group. The SuperMux, 40G MUX OCI (NTK525CF), 4x10G OTR, or 2x10G OTR (NTK530PME5 variants) circuit pack supports Fiber Channel client services. If possible, provision the subtending equipment for Fiber Channel client services, otherwise contact your next level of support or your Ciena support group. The 4x10G OTR, 2x10G OTR, 40G MUX, 8xOTN Flex MOTR, (1+8)xOTN Flex MOTR, Flex MOTR circuit packs support FLEX client services. If possible, provision the subtending equipment for FLEX client services, otherwise contact your next level of support or your Ciena support group.
5	If the original alarm has cleared Then the procedure is complete has not cleared Then go to step 6
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 applicable, ensure that the SFP/XFP optical transceiver module is the correct type. Use an SX SFP; or SR/SW XFP for multi-mode fiber-optic cables. Use an LX, ZX, or BX SFP; or ER/EW, LR/LW or DWDM XFP for single-mode fiber-optic cables. If required, replace the SFP/XFP optical transceiver module. Refer to the “Replacing a Pluggable module” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.

5-108 Alarm clearing procedures—I to Z

Procedure 5-47 (continued)

Loss Of Data Synch

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

—end—

Procedure 5-48

Loss of Extra Traffic

Alarm IDs: 1237, 1238

Probable cause

This alarm is raised when:

- on a span between two adjacent nodes, Extra Traffic is provisioned on one node but no Extra Traffic connection is provisioned on the other node.
- on a span between two nodes that have Extra Traffic provisioned on both sides, when there is an Active Ring switch or Active Span switch that is using the protection bandwidth. In this case, the alarm indicates that all Extra Traffic was dropped because the protection line is used to carry protected traffic.

Impact

Critical, service-affecting (C, SA) alarm

Prerequisites

To perform this procedure, you must use an account with at least a level 3 UPC.

Step	Action
1	Verify that Extra Traffic is provisioned between two adjacent nodes on a span. Refer to the “Adding a path connection” procedure in Part 1 of <i>Configuration - Bandwidth and Data Services</i> , 323-1851-320.
2	If the Extra Traffic is provisioned on one node but not on the other node, either provision the Extra Traffic on the node that has not been provisioned or remove the Extra Traffic on the side that has it provisioned. Refer to the “Adding a path connection” procedure in Part 1 of <i>Configuration - Bandwidth and Data Services</i> , 323-1851-320.
3	If the Extra Traffic is provisioned on both sides of a span and there is an active Ring switch or active Span switch that is using the protection bandwidth, then the active protection switch must be dropped (either release the manual Ring or Span switch or clear the fault condition which caused the automatic switch). Refer to “ Protection Switch Active alarms ” on page 5-370 in this document to clear the alarm.

—end—

Procedure 5-49 Loss of Frame and Multiframe

Alarm IDs: 2025

Probable cause

The alarm is raised on an OTUTTP and ETTP client facility, and PTP and OTUTTP of the line facility of the WLAI when OTUCn Loss of Frame or OTUCn Loss of Multiframe is detected on any of the lanes.

Impact

Critical, service-affecting (C, SA) alarm if not protected
Minor, non-service-affecting (m, NSA) alarm if protected

Prerequisites

To perform this procedure, you must

- have the optical fiber connection information (that is, how the circuit packs on each network element connect to other network elements)
 - have an optical power meter with the same optical connectors as the network element
 - observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0
 - have an antistatic wrist strap to dissipate electrostatic charges

Step	Action
1	Identify the circuit pack and facility raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document.
2	Use the optical fiber/cable connection information to identify the transmit and receive sites of the alarmed signal.
3	Log into the remote network element at the transmit end.
4	Retrieve all alarms at the transmit end. Clear any higher order alarms using the appropriate procedure.
5	If the original alarm has Then
cleared	the procedure is complete
not cleared	go to step 6

Procedure 5-49 (continued)
Loss of Frame and Multiframe

Step	Action				
6	Verify that the provisioned line rate on the upstream circuit pack matches the line rate on the local circuit pack. Correct any mismatches. Refer to the “Retrieving equipment and facility details” or “Editing facility parameters” procedures in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.				
7	If the original alarm has Then <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">cleared</td> <td style="width: 70%;">the procedure is complete</td> </tr> <tr> <td>not cleared</td> <td>go to step 8</td> </tr> </table>	cleared	the procedure is complete	not cleared	go to step 8
cleared	the procedure is complete				
not cleared	go to step 8				
8	Verify that the FEC setting on the upstream circuit pack matches the FEC setting on the local circuit pack. Correct any mismatches. Refer to the “Retrieving equipment and facility details” or “Editing facility parameters” procedures in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.				
9	If the original alarm has Then <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">cleared</td> <td style="width: 70%;">the procedure is complete</td> </tr> <tr> <td>not cleared</td> <td>go to step 10</td> </tr> </table>	cleared	the procedure is complete	not cleared	go to step 10
cleared	the procedure is complete				
not cleared	go to step 10				
10	If a photonic line system is used to transport the signal of the circuit pack raising the alarm, retrieve all alarms on the photonic line system. Clear any alarms on the photonic line system associated with the alarmed channel using the appropriate procedures.				
11	If the original alarm has Then <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">cleared</td> <td style="width: 70%;">the procedure is complete</td> </tr> <tr> <td>not cleared</td> <td>go to step 12</td> </tr> </table>	cleared	the procedure is complete	not cleared	go to step 12
cleared	the procedure is complete				
not cleared	go to step 12				
12	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.				
13	Determine the optical power level into the Rx interface using one of the following methods: <ul style="list-style-type: none"> • Using the Site Manager Equipment & Facility Provisioning application under the Configuration menu, retrieve the Rx Actual Power (dBm) value for the corresponding PTP facility. Refer to the “Retrieving OTM info” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i>, 323-1851-310. • Use the optical power meter to measure the optical power level into the Rx interface, and verify it is within technical specifications. Refer to the “Technical specifications” chapter in Part 3 of the <i>6500 Planning</i>, NTRN10EG. 				

Procedure 5-49 (continued)
Loss of Frame and Multiframe

Step	Action	
14	If the Rx Actual Power value or measured optical power is below the receiver sensitivity specified for the circuit pack above the receiver sensitivity specified for the circuit pack within the receiver sensitivity range specified for the circuit pack	Then go to step 15 step 17 step 23
15	Remove the Tx fiber from the far-end circuit pack, and use the optical power meter to measure the transmit power at the far-end.	
16	If the transmit power at the far-end is	
	above the launch power (minimum)	the optical fiber attenuation is too high, the optical fiber connections are dirty, or the optical fiber is damaged. Use your company procedure to determine and clear the problem. Go to step 27 .
	below the launch power (minimum)	Replace the required circuit pack at the transmit end. Refer to the procedures in <i>Fault Management - Module Replacement</i> , 323-1851-545. Go to step 27 .
	within the launch power range specified for the circuit pack	go to step 27 .
17	Clean all connections at both ends of the optical fiber link following your company standards and re-attach the optical fibers. Refer to the cleaning connectors procedures in <i>Installation - General Information</i> , 323-1851-201.0.	
18	If the original alarm has	Then
	cleared	the procedure is complete
	not cleared	go to step 19
19	Review the optical plan to verify that the correct attenuator (if required) is installed between the associated DWDM source and the receiver on the alarmed circuit pack.	

Procedure 5-49 (continued)
Loss of Frame and Multiframe

Step	Action	
	If a photonic line system is used to transport the signal, the high optical power can be caused by the photonic line system. Clear any alarms on the photonic line associated with the Loss Of Signal alarm using the appropriate procedures.	
20	If the original alarm has	Then
	cleared	the procedure is complete
	not cleared	go to step 21
21		<div style="border: 1px solid black; padding: 10px;"> <p>CAUTION Risk of traffic loss A cold restart on an unprotected circuit pack causes traffic loss. A cold restart on an active protected circuit pack causes a protection switch that impacts traffic.</p> </div>
	Once the optical path is verified to be correct, perform a cold restart on the circuit pack raising the alarm. See “Restarting a circuit pack or shelf processor” procedure in Part 1 of this document.	
22	If the original alarm has	Then
	cleared	the procedure is complete
	not cleared	go to step 23
23		<div style="border: 1px solid black; padding: 10px;"> <p>CAUTION Risk of traffic loss Connecting a facility to a test set causes traffic loss on the facility.</p> </div>
24	Use a test set to determine if a valid signal is on the facility.	
25	If the test set shows	Then
	a Loss Of Frame or incorrect framing condition	the problem is in the source.
		Go to step 26 .
	otherwise	go to step 27

Procedure 5-49 (continued)
Loss of Frame and Multiframe

Step	Action				
26	<p>If the source is connected to the alarmed circuit pack by a</p> <table> <tr> <td style="vertical-align: top;">client interface</td><td>Then Perform troubleshooting on the source system according to your company procedures.</td></tr> <tr> <td style="vertical-align: top;">line interface</td><td> <p>Retrieve all alarms at the transmit end. Clear any higher order alarms using the appropriate procedure.</p> <p>If no alarms exist on the transmit end, then perform a warm restart on the transmit circuit pack. Refer to the “Restarting a circuit pack or shelf processor” procedure in Part 1 of this document.</p> <p>If the alarm still does not clear, then the transmit circuit pack is faulty. Replace the transmit circuit pack. Refer to the equipment replacement procedures in <i>Fault Management - Module Replacement</i>, 323-1851-545.</p> </td></tr> </table>	client interface	Then Perform troubleshooting on the source system according to your company procedures.	line interface	<p>Retrieve all alarms at the transmit end. Clear any higher order alarms using the appropriate procedure.</p> <p>If no alarms exist on the transmit end, then perform a warm restart on the transmit circuit pack. Refer to the “Restarting a circuit pack or shelf processor” procedure in Part 1 of this document.</p> <p>If the alarm still does not clear, then the transmit circuit pack is faulty. Replace the transmit circuit pack. Refer to the equipment replacement procedures in <i>Fault Management - Module Replacement</i>, 323-1851-545.</p>
client interface	Then Perform troubleshooting on the source system according to your company procedures.				
line interface	<p>Retrieve all alarms at the transmit end. Clear any higher order alarms using the appropriate procedure.</p> <p>If no alarms exist on the transmit end, then perform a warm restart on the transmit circuit pack. Refer to the “Restarting a circuit pack or shelf processor” procedure in Part 1 of this document.</p> <p>If the alarm still does not clear, then the transmit circuit pack is faulty. Replace the transmit circuit pack. Refer to the equipment replacement procedures in <i>Fault Management - Module Replacement</i>, 323-1851-545.</p>				
27	<p>If the original alarm has</p> <table> <tr> <td style="vertical-align: top;">cleared</td><td>Then the procedure is complete</td></tr> <tr> <td style="vertical-align: top;">not cleared</td><td>perform a warm restart on the circuit pack reporting the alarm. “Restarting a circuit pack or shelf processor” procedure in Part 1 of this document.</td></tr> </table>	cleared	Then the procedure is complete	not cleared	perform a warm restart on the circuit pack reporting the alarm. “Restarting a circuit pack or shelf processor” procedure in Part 1 of this document.
cleared	Then the procedure is complete				
not cleared	perform a warm restart on the circuit pack reporting the alarm. “Restarting a circuit pack or shelf processor” procedure in Part 1 of this document.				
28	<p>If the original alarm has</p> <table> <tr> <td style="vertical-align: top;">cleared</td><td>Then the procedure is complete</td></tr> <tr> <td style="vertical-align: top;">not cleared</td><td>the receive circuit pack is faulty. Replace the circuit pack reporting the alarm. Refer to the “Replacing an optical interface circuit pack” procedure in <i>Fault Management - Module Replacement</i>, 323-1851-545.</td></tr> </table>	cleared	Then the procedure is complete	not cleared	the receive circuit pack is faulty. Replace the circuit pack reporting the alarm. Refer to the “Replacing an optical interface circuit pack” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.
cleared	Then the procedure is complete				
not cleared	the receive circuit pack is faulty. Replace the circuit pack reporting the alarm. Refer to the “Replacing an optical interface circuit pack” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.				
29	If the alarm does not clear, contact your next level of support or your Ciena support group.				

—end—

Procedure 5-50

Loss of Frame Delineation

Alarm IDs: 353, 1976

Probable cause

This alarm is raised against the WAN facility of a 4xGE, 1x10GE EPL, 24x10/100BT, 20G L2SS, L2SS, PDH gateway, L2 MOTR, FLEX MOTR, 8xOTN Flex MOTR, (1+8)xOTN Flex MOTR, eMOTR, 16xFLEX OTN I/F, RPR, SuperMux, 10G OTR, 10G OTSC, 2x10G OTR, 4x10G OTR, (1+2) 100G PKT/OTN I/F, 100G PKT/OTN WL3n I/F, 200G (2x100G/5x40G) MUX, 10x10G MUX OCI, 100G (2xQSFP+/2xSFP+) MUX, or 40G MUX OCI circuit pack when the GFP layer cannot detect valid GFP frames.

For 10G OTR and 10G OTSC circuit packs, this condition can occur if the line-side interface is receiving an OTU2, ODU2, or OPU2 layer critical fault (that is, LOS, LOC, LOF, LOM, ODU2-AIS, ODU2-LCK, ODU2-OCI, OPU2-AIS, or OPU2 Payload Type Mismatch). Since these OTN faults are typically injected as a result of upstream faults, these faults should be cleared first. Specifically, clear any OPU2 Payload Type Mismatches by ensuring the GFP-F client packet mapping values for the 10G OTR and 10G OTSC circuit packs match at both ends.

Impact

Critical, service-affecting (C, SA) alarm if not protected
Minor, non-service-affecting (m, NSA) alarm if protected

Prerequisites

To perform this procedure, you must:

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0
- have the optical fiber connection information (that is, how the optical modules on each network element connect to other network elements)

Procedure 5-50 (continued)

Loss of Frame Delineation

Step	Action	
1	Identify the circuit pack and facility raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document.	
2	If the alarm is raised against one of the following Broadband circuit packs: 10G OTR, 10G OTSC, 2x10G OTR, 4x10G OTR, 10x10G MUX OCI, or 40G MUX OCI otherwise	Then go to step 10 step 3
3	Use the appropriate alarm clearing procedure to clear any STS/VC path alarms on the interface circuit pack that connects to the 4xGE, 1x10GE EPL, 24x10/100BT, 20G L2SS, L2SS, PDH gateway, L2 MOTR, FLEX MOTR, 8xOTN Flex MOTR, (1+8)xOTN FLEX MOTR, eMOTR, RPR, 16xFLEX OTN I/F, or SuperMux circuit pack. These include the Signal Degrade and Excessive Error Rate (STS/VC) alarms.	
4	Trace the cross-connect information to verify there are no errors in the STS/VC cross-connects (for example, verify that the same number of STS/VC cross-connects are provisioned on the 4xGE, 1x10GE EPL, 24x10/100BT, 20G L2SS, L2SS, PDH gateway, L2 MOTR, FLEX MOTR, 8xOTN Flex MOTR, (1+8)xOTN FLEX MOTR, eMOTR, RPR, 16xFLEX OTN I/F, or SuperMux circuit packs on both sides of the connection, and that there are no duplicate STS/VC connections within a VCAT group). Refer to the “Retrieving path connections” procedure in Part 1 of <i>Configuration - Bandwidth and Data Services</i> , 323-1851-320.	
5	Ensure that the (WAN port) VCAT and LCAS (if applicable) attributes are provisioned to the same setting at the near-end and far-end 4xGE, 1x10GE EPL, 24x10/100BT, 20G L2SS, L2SS, PDH gateway, L2 MOTR, FLEX MOTR, eMOTR, RPR, 16xFLEX OTN I/F, or SuperMux circuit packs. Refer to the “Retrieving equipment and facility details” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.	
6	If using a PDH gateway, ensure that the WAN provisioning has the correct value for the PDH type to match the far-end.	
7	Use the appropriate alarm clearing procedure to clear any SONET/SDH or G.709 layer alarms raised against the line port of the circuit pack reporting the Loss of Frame Delineation alarm.	
8	If using SuperMux circuit packs, ensure both ends are consistently provisioned to be GFP-F or GFP-T. This value is set on initial addition of the circuit pack and is the same for all WAN ports on the circuit pack	

Procedure 5-50 (continued)
Loss of Frame Delineation

Step	Action	Then go to
9	Ensure that the subtending client equipment is transmitting a valid GFP-F (for Gigabit Ethernet) signal, as required. Go to step 16 .	
10	If the alarm is raised against a 10G OTR or 10G OTSC circuit pack 2x10G OTR, 4x10G OTR, 10x10G MUX OCI, or 40G MUX OCI circuit pack	step 11 step 13
11	A Loss of Frame Delineation alarm can be raised on a 10G OTR or 10G OTSC circuit pack when the line-side interface is receiving an OTN fault. Since these OTN faults and maintenance signals are the result of upstream alarms/faults, identify if any upstream circuit pack has active alarms and then troubleshoot/clear these alarms first.	
12	Once all OTN faults are clear, use the Site Manager Equipment & Facility Provisioning application to verify the WAN facility OPU2 + 7 reserved bytes setting matches for all OTSCs involved. Refer to the “Retrieving equipment and facility details” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310. Go to step 16 .	
13	If the far-end 2x10G OTR, 4x10G OTR or 40G MUX OCI circuit pack has an OTM2 facility, clear any OTN faults (such as, LOS, LOC, LOF, LOM, ODU2-AIS, ODU2-LCK, ODU2-OCI, OPU2-AIS, or OPU2 Payload Type Mismatch) for all upstream OTM2 facilities. That is, clear all OTN alarms upstream from the far-end OTM2 port.	
14	In the Site Manager Equipment & Facility Provisioning application, verify the ETH10G facility Packet Mapping value matches at both the near-end and far-ends. Refer to the “Retrieving equipment and facility details” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.	

Step	Action	
15	If the Packet Mapping values are mismatched	Then determine if it is the near-end alarmed ETH10G facility or the far-end facility that has the incorrect Packet Mapping value. The incorrectly provisioned facility must be deleted and reprovisioned with the correct Packet Mapping value. Refer to the “Deleting a facility from an equipment” and “Adding a facility to an equipment” procedures in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310. Continue to step 16 .
	match	go to step 16

- 16 Ensure that the subtending client equipment is transmitting a valid GFP-F (for Gigabit Ethernet) If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-51

Loss Of Frame, Loss Of Multiframe, or Signal Fail alarms

Use this procedure to clear the Loss of Frame, Loss of Multiframe, or Signal Fail alarms.

ATTENTION

The G.709 protocol uses the OTU3 Multiframe Alignment Signal (MFAS) byte as alignment markers to support lane deskew when an OTU3 signal is transmitted across multiple physical lanes. This occurs on the NTK529SJ for any OTU3 facility that uses an NTTA12BA CFP as the physical equipment. Consequently, MFAS errors can occur in the bits used as lane markers, the deskew process cannot be performed, and it is impossible to reconstruct the OTU3 frame. As a result, a “Loss of Frame” (LOF) alarm is raised instead of a “Loss of Multiframe” (LOM) alarm.

Loss Of Frame (OCn/STMn)

Alarm ID: 4, 33, 247, 282, 893, 984, 1689

Probable cause

This alarm is raised when the interface receives repeatedly errored SONET sections or SDH RS overhead bytes (A1 or A2) for three consecutive ms or more.

For SONET WT and 40G OCI, 40/43G OCI, 40G+ CFP OCI circuit packs, the optional 3-ms integration timer dealing with intermittent SEF defects (when monitoring for LOF) is implemented as outlined in the GR-253 SONET standard.

This alarm is caused by one of the following conditions:

- excessive attenuation
- dirty optical fibers
- dirty connectors
- improper connector seating
- transmit laser degrade

The network element cannot clear a Loss Of Signal alarm until a framed OC-n/STM-n signal is detected. The first time an optical fiber/cable is disconnected, the Loss of Frame alarm clears and a Loss Of Signal alarm is raised that will not change back to Loss of Frame when the optical fiber/cable is re-attached.

Procedure 5-51 (continued)

Loss Of Frame, Loss Of Multiframe, or Signal Fail alarms

Impact

- Critical, service-affecting (C, SA) alarm for the UPSR/SNCP configuration with cross-connects
- Critical, service-affecting (C, SA) alarm, if active 1+1/MSP linear or unprotected with cross-connects
- Critical, service-affecting (C, SA) alarm, for unprotected 2-Fiber/4-Fiber BLSR/MS-SPRing/HERS with cross-connects
- Minor, non-service-affecting (m, NSA) alarm, if inactive 1+1/MSP linear, protected 1+1/MSP linear, or without cross-connects
- Minor, non-service-affecting (m, NSA) alarm, for protected 2-Fiber/4-Fiber BLSR/MS-SPRing/HERS

Loss Of Frame (ETH10G, ETH40G, ETH100G, FC1200)

Alarm ID: 677, 968, 1297

Probable cause

This alarm is raised when the client Rx interface 64/66B PCS is unable to frame on the client signal on the:

- ETH10G of 10x10G MUX OCI, 2x10G OTR, 4x10G OTR, 10G OTSC, 4x10G MUX, or 100G (2xQSFP+/2xSFP+) MUX circuit pack
- ETH40G of 40G OCI, or 100G (2xQSFP+/2xSFP+) MUX circuit pack
- ETH100G of 100G OCI and 100G WL3e OTR circuit pack
- FC1200 of 10G OTSC circuit pack

For the 100G WL3n MOTR circuit pack, this alarm is raised when the received client traffic rate does not match the provisioned client rate (provisioning mismatch).

Impact

- Critical, service-affecting (C, SA) alarm
- Minor, non-service-affecting (m, NSA) alarm

Procedure 5-51 (continued)

Loss Of Frame, Loss Of Multiframe, or Signal Fail alarms

Loss Of Frame (OTM1, OTM2, OTM3, OTM4, OTMC2, OTUTTP, ETTP, STTP, FLEX, PDH)

Alarm IDs: 666, 999, 1168, 1440, 1453, 1461, 1861, 2014, 2064

Probable cause

This alarm can be raised under the following conditions:

- when the optical link exceeds the guaranteed link budget (the OSNR or the distortion penalties are in excess of the allocated margin but the Rx power is above the LOS threshold).
- when there is a fiber break on a long haul system (LH1600, CPL, 6500 Photonic services) connected to 6500 network element. The alarm is raised because the noise that is amplified through the system is so great that the power at the receiver can be higher than the Loss Of Signal threshold. Since there is no signal for the card to lock to and the power is high enough, the Loss of Frame alarm can be raised.
- when the provisioned Rx FEC setting does not match that of the incoming signal.

Note that after removing a LOS or LOF fault condition on the 40G OCLD or Wavelength-Selective 40G OCLD Rx OTM3, 100G WL3/WL3e OCLD or 100G OCLD Rx OTM4 facility, traffic restoration can take up to nine seconds.

The OTM4 facility “Loss of Frame” alarm is raised against both FLEX4 WL3e OCLD circuit packs).

For an OTUTTP facility, this alarm is raised when the Rx interface repeatedly receives errored optical transport unit (OTU) overhead bytes (OA1 or OA2) for three consecutive ms or more.

For the WT 10x10G MUX OCI, 100G OCI, 40G OCLD and Wavelength-Selective 40G OCLD circuit packs, the optional 3-ms integration timer dealing with intermittent SEF defects (when monitoring for LOF) is implemented as outlined in the GR-253 SONET standard.

Note: The 100G WL3/WL3e OCLD (NTK539Ux), Flex2 WL3/WL3e OCLD (NTK539Bx), Flex3 WL3e OCLD (NTK539Qx), 100G WL3n MOTR (NTK538Bx), 100G WL3n OTR (NTK538Ex), and 100G WL3e OTR (NTK538Ux) circuit packs do not interwork with any variant of 100G OCLD (NTK539TxEx) circuit packs. The “Loss of Frame” alarm is raised against both end of the fiber.

Procedure 5-51 (continued)

Loss Of Frame, Loss Of Multiframe, or Signal Fail alarms

For the 8xSFP OTN FLEX MOTR circuit pack, if Low Latency Mapping Procedure (LLMP) is run and is cross-connected to an OTM1 line, the alarm is raised if the far-end OTM1 line is not cross-connected to an LLMP mapped client port. This is the case with LLMP clients because the cross-connected OTM1 line runs at a higher clock rate.

For the eMOTR circuit pack, the alarm is raised when 64B/66B PCS SYNC is lost on the incoming 10GE signal.

For the ETTP facility of eMOTR circuit pack, ETTP facility figures secondary state is Layer-2 port disabled. This phenomenon can happen due to VLLI port conditioning.

When VLLI UP MEP port conditioned due to FEND UP MEP failure, NEND ETTP facility will have Loss Of Data Synch (for GE port and GE LAG)/Loss Of Frame (for 10G port or 10G LAG), indicating FEND port having an issue.

If UP MEP VLLI belonging port created on LAG client port then only Lead member (known to be least numbered LAG member port) shows the alarm and all member ports will declare L2 port disabled.

Similarly in case of Inverse VLLI operations, destination port instance (10G port or 10G LAG) shuts off laser with Loss of Frame during normal operation of source port. This alarm clears when source port undergoes faults and destination port enabled by clearing LOF alarm and the same port will have “Service Defect Indication” alarm indicating Inverse VLLI conditioning is activated.

For an ETTP facility, this alarm is raised when 64B/66B PCS is unable to frame on the client signal.

For an STTP facility, this alarm is raised when a SONET LOF is detected in the Rx direction.

Any terrestrial variant of WL3 OCLD circuit packs (NTK539UA/UB/UC/UD/UH/UJ) can interwork with any other terrestrial variant of WL3 OCLD circuit packs (NTK539UA/UB/UC/UD/UH/UJ), but the performance will be limited to the WL3 OCLD circuit pack with the lesser performance specification. The submarine variant of WL3 OCLD circuit packs (NTK539UE/NTK539UN) does not interwork with any terrestrial variant of WL3 OCLD circuit packs (NTK539UA/UB/UC/UD/UH/UJ). The OTM4 facility “Loss of Frame” alarm is raised against both circuit packs.

Procedure 5-51 (continued)

Loss Of Frame, Loss Of Multiframe, or Signal Fail alarms

Any terrestrial variant of FLEX2 WL3 OCLD circuit packs (NTK539BH, and NTK539BB) can interwork with any other terrestrial variant of FLEX2 WL3 OCLD circuit packs (NTK539BH and NTK539BB), but the performance will be limited to the FLEX2 WL3 OCLD circuit pack with the lesser performance specification. The submarine variant of FLEX2 WL3/WL3e OCLD circuit packs (NTK539BE/NTK539BN) does not interwork with any terrestrial variant of FLEX2 WL3 OCLD circuit packs (NTK539BH, and NTK539BB). The OTM4 facility “Loss of Frame” alarm is raised against both circuit packs.

Any terrestrial variant of FLEX3 WL3e OCLD circuit packs (NTK539QJ, NTK539QK, NTK539QL, and NTK539QM) can interwork with any other terrestrial variant of FLEX3 WL3e OCLD circuit packs (NTK539QJ, NTK539QK, NTK539QL, and NTK539QM), but the performance will be limited to the FLEX3 WL3e OCLD circuit pack with the lesser performance specification. The submarine variant of FLEX3 WL3e OCLD circuit packs (NTK539QN) does not interwork with any terrestrial variant of FLEX3 WL3e OCLD circuit packs (NTK539QJ, NTK539QK, NTK539QL, and NTK539QM). The OTM4 facility “Loss of Frame” alarm is raised against both FLEX3 WL3e OCLD circuit packs.

Any terrestrial variant of 100G WL3e OTR circuit packs (NTK538UJ, NTK538UK, NTK538UL, and NTK538UM) or WLAi can interwork with any other terrestrial variant of 100G WL3e OTR (NTK538UJ, NTK538UK, NTK538UL, and NTK538UM) or WLAi circuit packs, but the performance will be limited to the 100G WL3e OTR or WLAi circuit pack with the lesser performance specification. The submarine variant of 100G WL3e OTR circuit packs (NTK538UN) does not interwork with any terrestrial variant of 100G WL3e OTR circuit packs (NTK538UJ, NTK538UK, NTK538UL, and NTK538UM). The OTM4 facility “Loss of Frame” alarm is raised against both 100G WL3e OTR circuit packs.

The submarine variant of FLEX4 WL3e OCLD circuit packs (NTK539FN) does not interwork with any terrestrial variant of FLEX4 WL3e OCLD circuit packs (NTK539FJ).

Impact

Critical, service-affecting (C, SA) alarm

The impact for the 10G AM1/AM2 circuit pack only is as follows:

Critical, service-affecting (C, SA) alarm for the UPSR/SNCP configuration with cross-connects

Critical, service-affecting (C, SA) alarm, if active 1+1/MSP linear or unprotected with cross-connects

Procedure 5-51 (continued)

Loss Of Frame, Loss Of Multiframe, or Signal Fail alarms

Critical, service-affecting (C, SA) alarm for an unprotected 2-Fiber/4-Fiber BLSR/MS-SPRing/HERS

Minor, non-service-affecting (m, NSA) alarm, if inactive 1+1/MSP linear, protected 1+1/MSP linear, or without cross-connects

Minor, non-service-affecting (m, NSA) alarm for a protected 2-Fiber/4-Fiber BLSR/MS-SPRing/HERS

Loss Of Multiframe (OTM1, OTM2, OTM3, OTM4, OTMC2, OTUTTP, PTP)

Alarm IDs: 667, 1000, 1169, 1441, 2015

Probable cause

This alarm is raised when the multiframe alignment signal (MFAS) byte is out of sequence with the expected multiframe number for more than 5 consecutive OTUk frames.

ATTENTION

An extraneous OPU Payload Type Mismatch alarm may be raised in conjunction with a Loss of Multiframe (LOM) alarm against the 10G OTR line and 10G OTSC line, but does not impact network element function or alarm troubleshooting. If this is the case, then ignore the OPU Payload Type Mismatch alarm, and troubleshoot the LOM condition to clear both alarms.

Impact

Critical, service-affecting (C, SA) alarm

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

Signal Fail (OC48/192/768/STM16/64/256 Broadband, STTP)

Alarm ID: 5, 283, 985, 1464

Probable cause

This alarm is raised when the client Rx interface error rate detected by the B2 BIP-8 parity byte exceeds 1E-3.

This alarm is raised on:

- OC-192/STM-64 facilities when using the ETH10G to GFP to STS-192c/ STM-64c to OTU2 mapping
- ODUTTP, ODUCTP, and TCM facilities of the 100G PKT/OTN XCIF circuit pack
- OTUTTP, ODUTTP, ODUCTP, and TCM facilities of the 10x10G PKT/OTN I/F
- OTUTTP facilities of the 100G OCLD, 100G OCI, and 10x10G MUX circuit packs

Procedure 5-51 (continued)

Loss Of Frame, Loss Of Multiframe, or Signal Fail alarms

- STTP facility of PTS MRO IF 2xSFP+/14xSFP, PTS PDH I/F 2xDIM 16xFLEX OTN I/F, 4x10G MUX, or 40G OCI circuit packs

Impact

Critical, service-affecting (C, SA) alarm

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

Prerequisites

To perform this procedure, you must

- have the optical fiber connection information (that is, how the circuit packs on each network element connect to other network elements)
- have an optical power meter with the same optical connectors as the network element
- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0
- have an antistatic wrist strap to dissipate electrostatic charges

Step	Action				
1	Identify the circuit pack and facility raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document.				
2	Use the optical fiber/cable connection information to identify the transmit and receive sites of the alarmed signal.				
3	Log into the remote network element at the transmit end.				
4	Retrieve all alarms at the transmit end. Clear any higher order alarms using the appropriate procedure.				
5	If the original alarm has Then <table border="0" style="width: 100%;"> <tr> <td style="width: 30%;">cleared</td> <td>the procedure is complete</td> </tr> <tr> <td>not cleared</td> <td>go to step 6</td> </tr> </table>	cleared	the procedure is complete	not cleared	go to step 6
cleared	the procedure is complete				
not cleared	go to step 6				
6	Verify that the provisioned line rate on the upstream circuit pack matches the line rate on the local circuit pack. Correct any mismatches. Refer to the “Retrieving OTM info” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.				
7	If the original alarm has Then <table border="0" style="width: 100%;"> <tr> <td style="width: 30%;">cleared</td> <td>the procedure is complete</td> </tr> <tr> <td>not cleared</td> <td>go to step 8</td> </tr> </table>	cleared	the procedure is complete	not cleared	go to step 8
cleared	the procedure is complete				
not cleared	go to step 8				

Procedure 5-51 (continued)

Loss Of Frame, Loss Of Multiframe, or Signal Fail alarms

Procedure 5-51 (continued)

Loss Of Frame, Loss Of Multiframe, or Signal Fail alarms

Step	Action
16	If the transmit power at the far-end is above the launch power (minimum) Then the optical fiber attenuation is too high, the optical fiber connections are dirty, or the optical fiber is damaged. Use your company procedure to determine and clear the problem. Go to step 27 .
	below the launch power (minimum) if the circuit pack at the transmit end supports SFPs/DPOs, replace the SFP/DPO that corresponds to the facility raising the alarm. Refer to the procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545. if the circuit pack at the transmit end does not support SFPs/DPOs, replace the required circuit pack at the transmit end. Refer to the procedures in <i>Fault Management - Module Replacement</i> , 323-1851-545. Go to step 27 .
	within the launch power range specified for the circuit pack go to step 27 .
17	Clean all connections at both ends of the optical fiber link following your company standards and re-attach the optical fibers. Refer to the cleaning connectors procedures in <i>Installation - General Information</i> , 323-1851-201.0.
18	If the original alarm has cleared the procedure is complete not cleared go to step 19
19	Review the optical plan to verify that the correct attenuator (if required) is installed between the associated DWDM source and the receiver on the alarmed circuit pack. If a photonic line system is used to transport the signal, the high optical power can be caused by the photonic line system. Clear any alarms on the photonic line associated with the Loss Of Signal alarm using the appropriate procedures.

Procedure 5-51 (continued)

Loss Of Frame, Loss Of Multiframe, or Signal Fail alarms

Step	Action	
20	If the original alarm has cleared not cleared	Then the procedure is complete go to step 21
21		CAUTION Risk of traffic loss A cold restart on an unprotected circuit pack causes traffic loss. A cold restart on an active protected circuit pack causes a protection switch that impacts traffic.
		Once the optical path is verified to be correct, perform a cold restart on the circuit pack raising the alarm. See “Restarting a circuit pack or shelf processor” procedure in Part 1 of this document.
22	If the original alarm has cleared not cleared	Then the procedure is complete go to step 23
23		CAUTION Risk of traffic loss Connecting a facility to a test set causes traffic loss on the facility.
24	Use a test set to determine if a valid signal is on the facility.	
25	If the test set shows a Loss Of Frame or incorrect framing condition otherwise	Then the problem is in the source. Go to step 26 . go to step 27

Procedure 5-51 (continued)

Loss Of Frame, Loss Of Multiframe, or Signal Fail alarms

Step	Action
26	If the source is connected to the alarmed circuit pack by a client interface Then Perform troubleshooting on the source system according to your company procedures. line interface Then Retrieve all alarms at the transmit end. Clear any higher order alarms using the appropriate procedure. If no alarms exist on the transmit end, then perform a warm restart on the transmit circuit pack. Refer to the “Restarting a circuit pack or shelf processor” procedure in Part 1 of this document. If the alarm still does not clear, then the transmit circuit pack is faulty. Replace the transmit circuit pack. Refer to the equipment replacement procedures in <i>Fault Management - Module Replacement</i> , 323-1851-545.
27	If the original alarm has cleared Then the procedure is complete not cleared Then perform a warm restart on the circuit pack reporting the alarm. “Restarting a circuit pack or shelf processor” procedure in Part 1 of this document.
28	If the original alarm has cleared Then the procedure is complete not cleared Then the receive circuit pack is faulty. Replace the circuit pack reporting the alarm. Refer to the “Replacing an optical interface circuit pack” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.
29	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-52

Loss of Lane Alignment

Alarm IDs: 1856

Probable cause

For the 100G WL3n MOTR, this event is raised against the aggregated 40GE facility of a 100G WL3n MOTR when a “Loss of Signal”, “Loss of Clock”, or “Loss of Frame” alarms exists on at least one of the four of its associated FLEX member facilities.

Impact

Warning

Prerequisites

To perform this procedure, you must:

- observe all safety requirements described in “Observing product and personnel safety guidelines” chapter in Part 1 of *Installation, 323-1851-201.0* or *Fault Management - Module Replacement, 323-1851-545*
- have the fiber connection information (that is, how the optical modules on each network element connect to other network elements)
- if required, obtain a replacement circuit pack
- use an account with at least a level 3 UPC

Step	Action
1	Identify the facility that raised the event. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document.
2	Identify all four member FLEX facilities associated with the aggregated 40GE facility identified in step 1 .

Procedure 5-52 (continued)

Loss of Lane Alignment

Step	Action	
3	Follow the procedure to clear the “Loss of Signal” for all four members of the FLEX facilities identified in step 2 .	
4	If the original event is	Then
	cleared	the procedure is complete
	not cleared	go to step 5
5	Follow the procedure to clear the “ Loss of Lock ” on page 5-132 for all four members of the FLEX facilities identified in step 2 .	
6	If the original event is	Then
	cleared	the procedure is complete
	not cleared	go to step 7
7	Follow the procedure to clear the “ Loss Of Frame, Loss Of Multiframe, or Signal Fail alarms ” on page 5-119 for all four members of the FLEX facilities identified in step 2 . Go to step 8 .	
8	chapter 1 of If the event does not clear, contact your next level of support or your Ciena support group.	

—end—

Procedure 5-53

Loss of Lock

Alarm IDs: 1254

Probable cause

This alarm is raised when the FLEX Mapper is unable to lock on to a signal at the provisioned protocol rate. One of the following conditions can cause the alarm:

- the FLEX facility client protocol does not match the actual signal being received
- an optical fiber connection is degraded
- an optical fiber is bent or coiled too tightly
- the connector is dirty at the receiving FLEX MOTR, 8xOTN Flex MOTR, or (1+8)xOTN Flex MOTR or at the transmitting circuit pack
- an optical patchcord is damaged
- the receiving FLEX MOTR, 8xOTN Flex MOTR, or (1+8)xOTN Flex MOTR is defective
- the transmitting subtending equipment is defective
- the optical fiber is the wrong type
- the wrong subtending equipment is connected to the client-side, or the client-side is provisioned wrong
- if there is a miniature VOA on the fiber to attenuate the signal, it may not be operating correctly

Impact

Critical, service-affecting (C, SA) alarm if not protected
Minor, non-service-affecting (m, NSA) alarm if protected

Prerequisites

To perform this procedure, you must

- have the optical fiber connection information (that is, how the circuit packs on each network element connect to other network elements)
- have an optical power meter with the same optical connectors as the network element
- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545.

Procedure 5-53 (continued)

Loss of Lock

Step	Action	
1	Identify the circuit pack and facility raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document.	
2	If the alarm is raised against a	Then go to
	client port	step 3
	line port	step 18
Client side		
3	Make sure the provisioned connection type and bit rate are correct.	
4	Make sure you are using the correct type of optical fiber.	
5	Make sure the optical fiber is connected correctly on the FLEX MOTR, 8xOTN Flex MOTR, or (1+8)xOTN Flex MOTR client-side Rx port and the subtending equipment Tx port.	
6	Make sure the FLEX MOTR, 8xOTN Flex MOTR, or (1+8)xOTN Flex MOTR circuit pack is the correct type.	
7	Measure the received power level at the client-side Rx port of the affected circuit pack. Check to see whether the power level is within the operational threshold. Write down the value. Refer to the “Technical specifications” chapter in Part 3 of <i>Planning</i> , NTRN10EG, for minimum and maximum Rx/Tx power levels.	
	Note: You can record the power level from the Equipment—Facility window in the Site Manager.	
8	If the power level is	Then go to
	not within the operational threshold	step 9
	within the operational threshold	step 16
9	Make sure the transmitting subtending equipment is functioning correctly and transmitting a valid signal (correct bit rate and protocol).	
10	Use an optical power meter to measure the transmit power on the subtending equipment. Make sure it is working correctly and that the power of the transmitted signal is at the correct power level according to the manufacturer’s specifications.	
	If the subtending equipment Tx laser is	Then
	out of specification	repair or replace the subtending equipment. Go to step 11 .
	within specification	go to step 12

Procedure 5-53 (continued)

Loss of Lock

Step	Action	
11	If the original alarm has cleared not cleared	Then this procedure is complete go to step 12
12	If there is a VOA attached to a fiber between the FLEX MOTR, 8xOTN Flex MOTR, or (1+8)xOTN Flex MOTR and the subtending equipment there is no VOA attached to a fiber between the FLEX MOTR, 8xOTN Flex MOTR, or (1+8)xOTN Flex MOTR and the subtending equipment	Then re-adjust, check for proper functionality, and, if necessary, replace the VOA. Go to step 13 . go to step 14
13	If the original alarm has cleared not cleared	Then this procedure is complete go to step 14
14	Use the proper cleaning kit to clean all the connectors between the subtending equipment Tx port and the FLEX MOTR, 8xOTN Flex MOTR, or (1+8)xOTN Flex MOTR Rx port, and vice-versa. For information on cleaning, refer to the cleaning connectors procedures in <i>Installation - General Information</i> , 323-1851-201.0. a. Clean each connector separately. b. Record the operating power level after you clean each connector and compare it to the value you wrote down in step 7 , this will allow you to see if there is any improvement to the Rx power. c. Make sure there is no problem with the optical fiber plant between the FLEX MOTR, 8xOTN Flex MOTR, or (1+8)xOTN Flex MOTR and the subtending equipment	
15	Clean every connector between the subtending equipment Tx port, the SC-to-LC patch panel, and the FLEX MOTR, 8xOTN Flex MOTR, or (1+8)xOTN Flex MOTR client-side Rx port.	
16	Reseat the FLEX MOTR, 8xOTN Flex MOTR, or (1+8)xOTN Flex MOTR circuit pack. Refer to the “Reseating a circuit pack” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.	
	If the original alarm has cleared not cleared	Then this procedure is complete go to step 17

Procedure 5-53 (continued)

Loss of Lock

Step	Action								
17	<p>Replace the FLEX MOTR, 8xOTN Flex MOTR, or (1+8)xOTN Flex MOTR circuit pack. Refer to the “Replacing an optical interface circuit pack” procedure in <i>Fault Management - Module Replacement</i>, 323-1851-545.</p> <table> <thead> <tr> <th style="text-align: left;">If the original alarm has</th><th style="text-align: left;">Then</th></tr> </thead> <tbody> <tr> <td>cleared</td><td>the removed circuit pack is faulty. This procedure is complete.</td></tr> <tr> <td>not cleared</td><td>the circuit pack is not the problem. Reseat the original FLEX MOTR, 8xOTN Flex MOTR, or (1+8)xOTN Flex MOTR circuit pack and contact your next level of support.</td></tr> </tbody> </table>	If the original alarm has	Then	cleared	the removed circuit pack is faulty. This procedure is complete.	not cleared	the circuit pack is not the problem. Reseat the original FLEX MOTR, 8xOTN Flex MOTR, or (1+8)xOTN Flex MOTR circuit pack and contact your next level of support.		
If the original alarm has	Then								
cleared	the removed circuit pack is faulty. This procedure is complete.								
not cleared	the circuit pack is not the problem. Reseat the original FLEX MOTR, 8xOTN Flex MOTR, or (1+8)xOTN Flex MOTR circuit pack and contact your next level of support.								
Line side									
18	<p>Make sure that the FEC settings of the far-end line side device matches the FEC settings on the FLEX MOTR, 8xOTN Flex MOTR, or (1+8)xOTN Flex MOTR circuit pack. Refer to the “Retrieving and editing TR control information” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i>, 323-1851-310. If the alarm does not clear, go to step 19.</p>								
19	<p>Check the corresponding upstream FLEX MOTR, 8xOTN Flex MOTR, or (1+8)xOTN Flex MOTR or, if applicable, Optical Fiber Amplifiers (OFA) for failures or alarms. Use a network topology diagram to determine the upstream FLEX MOTR, 8xOTN Flex MOTR, or (1+8)xOTN Flex MOTR circuit packs and OFAs. Troubleshoot these alarms/failures before proceeding.</p>								
20	<p>At the downstream shelf, use the System Manager to check if you are receiving “Loss of Lock” alarms on all (or most) FLEX MOTR, 8xOTN Flex MOTR, or (1+8)xOTN Flex MOTR circuit packs in the same east/west plane, or just on a single FLEX MOTR.</p> <table> <thead> <tr> <th style="text-align: left;">If the alarm appears</th><th style="text-align: left;">Then go to</th></tr> </thead> <tbody> <tr> <td>on the only FLEX MOTR, 8xOTN Flex MOTR, or (1+8)xOTN Flex MOTR in the east/west plane</td><td>step 21</td></tr> <tr> <td>on all (or most) FLEX MOTR, 8xOTN Flex MOTR, or (1+8)xOTN Flex MOTR circuit packs in the same east/west plane</td><td>step 24</td></tr> <tr> <td>on one of multiple FLEX MOTR, 8xOTN Flex MOTR, or (1+8)xOTN Flex MOTR circuit packs in the same east/west plane</td><td>step 27</td></tr> </tbody> </table>	If the alarm appears	Then go to	on the only FLEX MOTR, 8xOTN Flex MOTR, or (1+8)xOTN Flex MOTR in the east/west plane	step 21	on all (or most) FLEX MOTR, 8xOTN Flex MOTR, or (1+8)xOTN Flex MOTR circuit packs in the same east/west plane	step 24	on one of multiple FLEX MOTR, 8xOTN Flex MOTR, or (1+8)xOTN Flex MOTR circuit packs in the same east/west plane	step 27
If the alarm appears	Then go to								
on the only FLEX MOTR, 8xOTN Flex MOTR, or (1+8)xOTN Flex MOTR in the east/west plane	step 21								
on all (or most) FLEX MOTR, 8xOTN Flex MOTR, or (1+8)xOTN Flex MOTR circuit packs in the same east/west plane	step 24								
on one of multiple FLEX MOTR, 8xOTN Flex MOTR, or (1+8)xOTN Flex MOTR circuit packs in the same east/west plane	step 27								

Procedure 5-53 (continued)

Loss of Lock

Step	Action
21	<p>If</p> <p>there are amplifiers between the upstream and downstream FLEX MOTR, 8xOTN Flex MOTR, or (1+8)xOTN Flex MOTR circuit packs</p> <p>there are no amplifiers between the upstream and downstream FLEX MOTR, 8xOTN Flex MOTR, or (1+8)xOTN Flex MOTR circuit packs</p> <p>Then</p> <p>there is a problem at the amplifier site, the ring requires re-equalization, or both.</p> <p>Contact your next level of support to troubleshoot. If troubleshooting does not clear the alarm, go to step 27.</p> <p>there is a problem with the line fiber between the sites, go to step 22</p>
22	<p>Investigate the line fiber between the upstream FLEX MOTR, 8xOTN Flex MOTR, or (1+8)xOTN Flex MOTR circuit packs and the downstream FLEX MOTR, 8xOTN Flex MOTR, or (1+8)xOTN Flex MOTR circuit packs for loss or degrade.</p> <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <p>CAUTION</p> <p>Risk of loss of traffic across multiple wavelengths in the band</p>  <p>Disturbing the line fiber affects traffic on the entire band/direction. If the traffic is protected, follow the protection switching procedures in Part 2 of <i>Configuration - Provisioning and Operating</i>, 323-1851-310, to switch traffic for the FLEX MOTR, 8xOTN Flex MOTR, or (1+8)xOTN Flex MOTR circuit pack in the east/west plane before proceeding. If the traffic is not protected, you will drop traffic.</p> </div> <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <p>CAUTION</p> <p>Disable Automatic Laser Shutdown</p>  <p>If Automatic Laser Shutdown (ALS) is enabled, disable ALS for all shelves that will be affected by this maintenance activity. Use a network topology diagram and channel listing to determine the upstream and downstream sites that will be affected when the ring is opened. If you do not know if ALS is enabled or not, assume it is enabled. Follow the "Editing facility parameters" procedure in Part 1 of <i>Configuration - Provisioning and Operating</i>, 323-1851-310, to disable ALS.</p> </div>

Procedure 5-53 (continued)

Loss of Lock

Step	Action
<p>Using a power meter, a cleaning kit, and a network topology diagram, start at the upstream site and clean every connector on the path until you reach the downstream site. Measure the power with the power meter after each cleaning to check for improvements in the line power. Refer to the cleaning connectors procedures in <i>Installation - General Information</i>, 323-1851-201.0. Also, check for damaged, kinked, tightly bent fiber, or anything else that might impede the optical signal. This includes optical filters such as OMXs or C/L Splitter/Couplers. Replace any damaged fibers or filters.</p>	
23	If the original alarm has cleared Then this procedure is complete. Restore the traffic to both paths on a protected channel.
	If not cleared Then go to step 27
24	If there are amplifiers between the upstream and downstream FLEX MOTR, 8xOTN Flex MOTR, or (1+8)xOTN Flex MOTR circuit packs Then there is a problem at the amplifier site, the ring requires re-equalization, or both. Contact your next level of support.
	If there are no amplifiers between the upstream and downstream FLEX MOTR, 8xOTN Flex MOTR, or (1+8)xOTN Flex MOTR circuit packs Then there is a problem with the line fiber between the sites, go to step 25

Procedure 5-53 (continued)

Loss of Lock

Step	Action						
25	<p>The line fiber between the upstream FLEX MOTR, 8xOTN Flex MOTR, or (1+8)xOTN Flex MOTR circuit packs and the downstream FLEX MOTR, 8xOTN Flex MOTR, or (1+8)xOTN Flex MOTR circuit packs must be investigated for loss or degrade.</p> <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <p style="text-align: center;">CAUTION</p>  <p>Risk of loss of traffic across multiple wavelengths in the band</p> <p>Disturbing the line fiber affects traffic on the entire band/direction. If the traffic is protected, follow the protection switching procedures in Part 2 of <i>Configuration - Provisioning and Operating</i>, 323-1851-310, to switch traffic for the FLEX MOTR, 8xOTN Flex MOTR, or (1+8)xOTN Flex MOTR circuit pack in the east/west plane before proceeding. If the traffic is not protected, you will drop traffic.</p> </div>						
26	<div style="border: 1px solid black; padding: 10px; margin-bottom: 10px;"> <p style="text-align: center;">CAUTION</p>  <p>Disable Automatic Laser Shutdown</p> <p>If Automatic Laser Shutdown (ALS) is enabled, disable ALS for all shelves that will be affected by this maintenance activity. Use a network topology diagram and channel listing to determine the upstream and downstream sites that will be affected when the ring is opened. If you do not know if ALS is enabled or not, assume it is enabled. Follow the “Editing facility parameters” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i>, 323-1851-310, to disable ALS.</p> </div> <p>Using a power meter, a cleaning kit, and a network topology diagram, start at the upstream site and clean every connector on the path until you reach the downstream site. Measure the power with the power meter after each cleaning to check for improvements in the line power. Refer to the cleaning connectors procedures in <i>Installation - General Information</i>, 323-1851-201.0. Also, check for damaged, kinked, tightly bent fiber, or anything else that might impede the optical signal. This includes optical filters such as OMXs or C/L Splitter/Couplers. Replace any damaged fibers or filters.</p> <table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; width: 30%;">If the original alarm has</th> <th style="text-align: left; width: 70%;">Then</th> </tr> </thead> <tbody> <tr> <td style="vertical-align: top;">cleared</td> <td style="vertical-align: top;">this procedure is complete. Restore the traffic to both paths on a protected channel.</td> </tr> <tr> <td style="vertical-align: top;">not cleared</td> <td style="vertical-align: top;">contact your next level of support</td> </tr> </tbody> </table>	If the original alarm has	Then	cleared	this procedure is complete. Restore the traffic to both paths on a protected channel.	not cleared	contact your next level of support
If the original alarm has	Then						
cleared	this procedure is complete. Restore the traffic to both paths on a protected channel.						
not cleared	contact your next level of support						

Procedure 5-53 (continued)

Loss of Lock

Step	Action						
27	<p>If the path is</p> <table> <tr> <td style="width: 15%;">protected</td> <td>Then switch traffic off of the FLEX MOTR, 8xOTN Flex MOTR, or (1+8)xOTN Flex MOTR circuit pack. Refer to the “Protection Switching” procedures in Part 2 of <i>Configuration - Provisioning and Operating</i>, 323-1851-310.</td> </tr> <tr> <td>unprotected</td> <td>go to step 28.</td> </tr> </table>	protected	Then switch traffic off of the FLEX MOTR, 8xOTN Flex MOTR, or (1+8)xOTN Flex MOTR circuit pack. Refer to the “Protection Switching” procedures in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.	unprotected	go to step 28 .		
protected	Then switch traffic off of the FLEX MOTR, 8xOTN Flex MOTR, or (1+8)xOTN Flex MOTR circuit pack. Refer to the “Protection Switching” procedures in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.						
unprotected	go to step 28 .						
28	<p>CAUTION Risk of traffic loss Performing this step may affect traffic.</p> 						
	<p>If Automatic Laser Shutdown (ALS) is enabled, disable ALS for both the near-end and far-end shelves which contain the alarming FLEX MOTR, 8xOTN Flex MOTR, or (1+8)xOTN Flex MOTR circuit pack and its corresponding upstream FLEX MOTR, 8xOTN Flex MOTR, or (1+8)xOTN Flex MOTR circuit pack. Use a network topology diagram and channel listing to determine the near-end and far-end sites. If you do not know if ALS is enabled or not, assume it is enabled. Follow the “Editing facility parameters” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i>, 323-1851-310, to disable ALS.</p>						
29	<p>Using a power meter, a cleaning kit, and a network topology diagram, start at the upstream site and clean every connector on the path until you reach the downstream site. Measure the power with the power meter after each cleaning to check for improvements in the line power. Refer to the cleaning connectors procedures in <i>Installation - General Information</i>, 323-1851-201.0.</p>						
30	<p>Make sure the optical fiber is connected correctly on the FLEX MOTR, 8xOTN Flex MOTR, or (1+8)xOTN Flex MOTR circuit pack line-side Rx port at the near-end site and on the FLEX MOTR, 8xOTN Flex MOTR, or (1+8)xOTN Flex MOTR circuit pack line-side Tx port at the far-end site.</p> <p>Note: Use a network topology diagram to determine the near-end and far-end sites.</p>						
	<table> <thead> <tr> <th style="text-align: center;">If the alarm</th> <th style="text-align: center;">Then</th> </tr> </thead> <tbody> <tr> <td style="width: 15%;">clears</td> <td>you have completed the procedure. Restore the traffic to both paths on a protected channel.</td> </tr> <tr> <td>does not clear</td> <td>go to step 31</td> </tr> </tbody> </table>	If the alarm	Then	clears	you have completed the procedure. Restore the traffic to both paths on a protected channel.	does not clear	go to step 31
If the alarm	Then						
clears	you have completed the procedure. Restore the traffic to both paths on a protected channel.						
does not clear	go to step 31						

Procedure 5-53 (continued)

Loss of Lock

Step	Action				
31	<p>Check whether the FLEX MOTR, 8xOTN Flex MOTR, or (1+8)xOTN Flex MOTR circuit pack line-side Rx power level is within the operational threshold and write down the value. Refer to the “Technical specifications” chapter in Part 3 of <i>Planning</i>, NTRN10EG, for minimum and maximum Rx/Tx power levels for the line-side specifications.</p> <p>Note: Record the received power level on the FLEX MOTR, 8xOTN Flex MOTR, or (1+8)xOTN Flex MOTR circuit pack. You can record the power level from the Equipment—Facility window in the Site Manager.</p>				
32	<p>Check the transmitted power level on the corresponding upstream FLEX MOTR, 8xOTN Flex MOTR, or (1+8)xOTN Flex MOTR circuit pack. Check whether the transmitted power level is within the operational threshold. Refer to the “Technical specifications” chapter in Part 3 of <i>Planning</i>, NTRN10EG, for minimum and maximum Rx/Tx power levels for the line-side specifications.</p> <p>Note 1: You can record the power level from the Equipment—>Facility window in the Site Manager.</p> <p>Note 2: Use a network topology diagram to determine the upstream FLEX MOTR, 8xOTN Flex MOTR, or (1+8)xOTN Flex MOTR circuit pack.</p>				
33	<p>If the transmit power level is Then go to</p> <table> <tr> <td>not within the operational threshold</td> <td>step 34</td> </tr> <tr> <td>within the operational threshold</td> <td>step 38</td> </tr> </table>	not within the operational threshold	step 34	within the operational threshold	step 38
not within the operational threshold	step 34				
within the operational threshold	step 38				
34	Replace the upstream FLEX MOTR, 8xOTN Flex MOTR, or (1+8)xOTN Flex MOTR circuit pack. Refer to the “Replacing an optical interface circuit pack” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.				
35	<p>If the alarm Then</p> <table> <tr> <td>clears</td> <td>the removed circuit pack is faulty. This procedure is complete. Restore the traffic to both paths on a protected channel.</td> </tr> <tr> <td>does not clear (and the new circuit pack is within operational specifications)</td> <td>the circuit pack is not the entire problem. Go to step 36.</td> </tr> </table>	clears	the removed circuit pack is faulty. This procedure is complete. Restore the traffic to both paths on a protected channel.	does not clear (and the new circuit pack is within operational specifications)	the circuit pack is not the entire problem. Go to step 36 .
clears	the removed circuit pack is faulty. This procedure is complete. Restore the traffic to both paths on a protected channel.				
does not clear (and the new circuit pack is within operational specifications)	the circuit pack is not the entire problem. Go to step 36 .				
36	Reseat the near-end FLEX MOTR, 8xOTN Flex MOTR, or (1+8)xOTN Flex MOTR circuit pack. Refer to the “Reseating a circuit pack” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.				
37	<p>If the alarm Then</p> <table> <tr> <td>clears</td> <td>this procedure is complete. Restore the traffic to both paths on a protected channel.</td> </tr> <tr> <td>does not clear</td> <td>go to step 38</td> </tr> </table>	clears	this procedure is complete. Restore the traffic to both paths on a protected channel.	does not clear	go to step 38
clears	this procedure is complete. Restore the traffic to both paths on a protected channel.				
does not clear	go to step 38				

Procedure 5-53 (continued)

Loss of Lock

Step	Action						
38	<p>Use the proper cleaning kit to clean all the connectors attached to the receiving (near-end) FLEX MOTR, 8xOTN Flex MOTR, or (1+8)xOTN Flex MOTR circuit pack line-side Rx port and to the corresponding line-side Tx port on the transmitting (far-end) FLEX MOTR, 8xOTN Flex MOTR, or (1+8)xOTN Flex MOTR circuit pack. Refer to the cleaning connectors procedures in <i>Installation - General Information</i>, 323-1851-201.0. Use a network topology diagram to determine the transmitting (far-end) FLEX MOTR, 8xOTN Flex MOTR, or (1+8)xOTN Flex MOTR circuit pack.</p> <p>Note 1: If you are using the OMX 4CH + Fiber Manager, clean both ends of the patch-cord between the OMX and the line-side FLEX MOTR, 8xOTN Flex MOTR, or (1+8)xOTN Flex MOTR port.</p> <p>Note 2: Clean between the FLEX MOTR, 8xOTN Flex MOTR, or (1+8)xOTN Flex MOTR circuit pack, the SC-to-LC patch panel, and the OMX.</p> <ul style="list-style-type: none"> a. Clean each connector separately. b. Record the operating power level after you clean each connector and compare it to the value you wrote down in step 31, this will allow you to see if there is any improvement to the Rx power. 						
39	<table> <thead> <tr> <th>If the alarm</th> <th>Then</th> </tr> </thead> <tbody> <tr> <td>clears</td> <td>this procedure is complete. Restore the traffic to both paths on a protected channel.</td> </tr> <tr> <td>does not clear</td> <td>go to step 40</td> </tr> </tbody> </table>	If the alarm	Then	clears	this procedure is complete. Restore the traffic to both paths on a protected channel.	does not clear	go to step 40
If the alarm	Then						
clears	this procedure is complete. Restore the traffic to both paths on a protected channel.						
does not clear	go to step 40						
40	<div style="border: 1px solid black; padding: 10px; margin-bottom: 10px;"> <p>CAUTION</p>  <p>Risk of loss of traffic across multiple bands</p> <p>Do not clean any optical fibers on the optical fiber plant, or on connections to the OMX. This affects traffic over multiple bands. Clean only the connections at the specified FLEX MOTR, 8xOTN Flex MOTR, or (1+8)xOTN Flex MOTR circuit packs.</p> </div> <p>Replace the near-end FLEX MOTR, 8xOTN Flex MOTR, or (1+8)xOTN Flex MOTR circuit pack. Refer to the “Replacing an optical interface circuit pack” procedure in <i>Fault Management - Module Replacement</i>, 323-1851-545.</p>						
41	<table> <thead> <tr> <th>If the alarm</th> <th>Then</th> </tr> </thead> <tbody> <tr> <td>clears</td> <td>the removed circuit pack is faulty. This procedure is complete. Restore the traffic to both paths on a protected channel.</td> </tr> <tr> <td>does not clear</td> <td>the circuit pack is not the problem. Reseat the original circuit pack. Go to step 42.</td> </tr> </tbody> </table>	If the alarm	Then	clears	the removed circuit pack is faulty. This procedure is complete. Restore the traffic to both paths on a protected channel.	does not clear	the circuit pack is not the problem. Reseat the original circuit pack. Go to step 42 .
If the alarm	Then						
clears	the removed circuit pack is faulty. This procedure is complete. Restore the traffic to both paths on a protected channel.						
does not clear	the circuit pack is not the problem. Reseat the original circuit pack. Go to step 42 .						

5-142 Alarm clearing procedures—I to Z

Procedure 5-53 (continued)

Loss of Lock

Step	Action
42	Repeat step 36 to step 40 for the far-end site.
43	If the alarm does not clear, contact your next level of support. Note: If you set a forced switch on the path, make sure you remove the switch when the procedure is completed. If you are using ALS and disabled it during this procedure, re-enable it for each site.
	—end—

Procedure 5-54 **Loss Of Multiframe (WAN)**

Alarm IDs: 357, 358, 683, 684, 727, 728, 729

Probable cause

This alarm is raised when the multiframe indicator for a VT/STS/VC/PDH member of a virtually concatenated group cannot be located. This alarm is raised against an VT/STS/VC that connects to the WAN port of a 4xGE, 1x10GE EPL, 24x10/100BT, 20G L2SS, L2SS, PDH gateway, L2 MOTR, RPR, or SuperMux circuit pack.

Impact

Critical, service-affecting (C, SA) alarm

Prerequisites

To perform this procedure, you must

- use an account with at least a level 3 UPC
 - have the fiber connection information (that is, how the optical modules on each network element connect to other network elements)

—end—

Procedure 5-55 **Loss of Multiframe - VCAT**

Alarm IDs: 928, 931, 1379

Probable cause

This alarm is raised against a WAN facility of a PDH gateway circuit pack when the multiframe indicator of a VT/STS/VC/PDH in a virtually concatenated group (VCAT) cannot be located.

Impact

Critical, service-affecting (C, SA) alarm

Prerequisites

To perform this procedure, you must

- use an account with at least a level 3 UPC
 - have the fiber connection information (that is, how the optical modules on each network element connect to other network elements).

—end—

Procedure 5-56 Loss of OPU Multiframe Identifier

Alarm IDs: 2035

Probable cause

This alarm is raised when loss of OPU Multiframe Identifier (OMFI) for an OPUCn frame is detected.

The value of bits 4 to 8 of the OMFI byte will be incremented each OPUCn frame to provide a 20 frame multiframe for the multiplexing of ODUk signals into the OPUCn.

Impact

Critical, service-affecting (C, SA) alarm if not protected
Minor, non-service-affecting (m, NSA) alarm if protected

Prerequisites

To perform this procedure, you must

- have the optical fiber connection information (that is, how the circuit packs on each network element connect to other network elements)
 - have an optical power meter with the same optical connectors as the network element
 - observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0
 - have an antistatic wrist strap to dissipate electrostatic charges

Step	Action
1	Identify the circuit pack and facility raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document.
2	Use the optical fiber/cable connection information to identify the transmit and receive sites of the alarmed signal.
3	Log into the remote network element at the transmit end.
4	Retrieve all alarms at the transmit end. Clear any higher order alarms using the appropriate procedure.
5	If the original alarm has Then
cleared	the procedure is complete
not cleared	go to step 6

Procedure 5-56 (continued) Loss of OPU Multiframe Identifier

Procedure 5-56 (continued)
Loss of OPU Multiframe Identifier

Step	Action	
14	If the Rx Actual Power value or measured optical power is below the receiver sensitivity specified for the circuit pack above the receiver sensitivity specified for the circuit pack within the receiver sensitivity range specified for the circuit pack	Then go to step 15 step 17 step 23
15	Remove the Tx fiber from the far-end circuit pack, and use the optical power meter to measure the transmit power at the far-end.	
16	If the transmit power at the far-end is	
	above the launch power (minimum)	the optical fiber attenuation is too high, the optical fiber connections are dirty, or the optical fiber is damaged. Use your company procedure to determine and clear the problem. Go to step 27 .
	below the launch power (minimum)	Replace the required circuit pack at the transmit end. Refer to the procedures in <i>Fault Management - Module Replacement</i> , 323-1851-545. Go to step 27 .
	within the launch power range specified for the circuit pack	go to step 27 .
17	Clean all connections at both ends of the optical fiber link following your company standards and re-attach the optical fibers. Refer to the cleaning connectors procedures in <i>Installation - General Information</i> , 323-1851-201.0.	
18	If the original alarm has	Then
	cleared	the procedure is complete
	not cleared	go to step 19
19	Review the optical plan to verify that the correct attenuator (if required) is installed between the associated DWDM source and the receiver on the alarmed circuit pack.	

Procedure 5-56 (continued)
Loss of OPU Multiframe Identifier

Step	Action	
	If a photonic line system is used to transport the signal, the high optical power can be caused by the photonic line system. Clear any alarms on the photonic line associated with the Loss Of Signal alarm using the appropriate procedures.	
20	If the original alarm has	Then
	cleared	the procedure is complete
	not cleared	go to step 21
21		<div style="border: 1px solid black; padding: 10px;"> <p>CAUTION Risk of traffic loss A cold restart on an unprotected circuit pack causes traffic loss. A cold restart on an active protected circuit pack causes a protection switch that impacts traffic.</p> </div>
	Once the optical path is verified to be correct, perform a cold restart on the circuit pack raising the alarm. See “Restarting a circuit pack or shelf processor” procedure in Part 1 of this document.	
22	If the original alarm has	Then
	cleared	the procedure is complete
	not cleared	go to step 23
23		<div style="border: 1px solid black; padding: 10px;"> <p>CAUTION Risk of traffic loss Connecting a facility to a test set causes traffic loss on the facility.</p> </div>
24	Use a test set to determine if a valid signal is on the facility.	
25	If the test set shows	Then
	a Loss Of Frame or incorrect framing condition	the problem is in the source.
		Go to step 26 .
	otherwise	go to step 27

Procedure 5-56 (continued)
Loss of OPU Multiframe Identifier

Step	Action				
26	<p>If the source is connected to the alarmed circuit pack by a</p> <table> <tr> <td style="vertical-align: top;">client interface</td><td>Then Perform troubleshooting on the source system according to your company procedures.</td></tr> <tr> <td style="vertical-align: top;">line interface</td><td> <p>Retrieve all alarms at the transmit end. Clear any higher order alarms using the appropriate procedure.</p> <p>If no alarms exist on the transmit end, then perform a warm restart on the transmit circuit pack. Refer to the “Restarting a circuit pack or shelf processor” procedure in Part 1 of this document.</p> <p>If the alarm still does not clear, then the transmit circuit pack is faulty. Replace the transmit circuit pack. Refer to the equipment replacement procedures in <i>Fault Management - Module Replacement</i>, 323-1851-545.</p> </td></tr> </table>	client interface	Then Perform troubleshooting on the source system according to your company procedures.	line interface	<p>Retrieve all alarms at the transmit end. Clear any higher order alarms using the appropriate procedure.</p> <p>If no alarms exist on the transmit end, then perform a warm restart on the transmit circuit pack. Refer to the “Restarting a circuit pack or shelf processor” procedure in Part 1 of this document.</p> <p>If the alarm still does not clear, then the transmit circuit pack is faulty. Replace the transmit circuit pack. Refer to the equipment replacement procedures in <i>Fault Management - Module Replacement</i>, 323-1851-545.</p>
client interface	Then Perform troubleshooting on the source system according to your company procedures.				
line interface	<p>Retrieve all alarms at the transmit end. Clear any higher order alarms using the appropriate procedure.</p> <p>If no alarms exist on the transmit end, then perform a warm restart on the transmit circuit pack. Refer to the “Restarting a circuit pack or shelf processor” procedure in Part 1 of this document.</p> <p>If the alarm still does not clear, then the transmit circuit pack is faulty. Replace the transmit circuit pack. Refer to the equipment replacement procedures in <i>Fault Management - Module Replacement</i>, 323-1851-545.</p>				
27	<p>If the original alarm has</p> <table> <tr> <td style="vertical-align: top;">cleared</td><td>Then the procedure is complete</td></tr> <tr> <td style="vertical-align: top;">not cleared</td><td>perform a warm restart on the circuit pack reporting the alarm. “Restarting a circuit pack or shelf processor” procedure in Part 1 of this document.</td></tr> </table>	cleared	Then the procedure is complete	not cleared	perform a warm restart on the circuit pack reporting the alarm. “Restarting a circuit pack or shelf processor” procedure in Part 1 of this document.
cleared	Then the procedure is complete				
not cleared	perform a warm restart on the circuit pack reporting the alarm. “Restarting a circuit pack or shelf processor” procedure in Part 1 of this document.				
28	<p>If the original alarm has</p> <table> <tr> <td style="vertical-align: top;">cleared</td><td>Then the procedure is complete</td></tr> <tr> <td style="vertical-align: top;">not cleared</td><td>the receive circuit pack is faulty. Replace the circuit pack reporting the alarm. Refer to the “Replacing an optical interface circuit pack” procedure in <i>Fault Management - Module Replacement</i>, 323-1851-545.</td></tr> </table>	cleared	Then the procedure is complete	not cleared	the receive circuit pack is faulty. Replace the circuit pack reporting the alarm. Refer to the “Replacing an optical interface circuit pack” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.
cleared	Then the procedure is complete				
not cleared	the receive circuit pack is faulty. Replace the circuit pack reporting the alarm. Refer to the “Replacing an optical interface circuit pack” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.				
29	If the alarm does not clear, contact your next level of support or your Ciena support group.				

—end—

Procedure 5-57 Loss of Pointer

Alarm IDs: 16, 47, 64, 113, 128, 194, 243, 274, 459, 465, 2084

Probable cause

This alarm is raised when one of the following conditions occurs:

- the pointer value in the SONET/SDH overhead of an STS/HO VC or VT/LO VC is out of a valid range or is not stable
- improper network synchronization
- improper or no connection provisioned (STS/HO VC or VT/LO VC signal received is at a different rate to the provisioned STS/HO VC or VT/LO VC signal)

Note: If the remote end is not provisioned with a corresponding STS/HO VC or VT/LO VC cross-connect, the local end raises this alarm when it receives a STS/HO VC or VT/LO VC signal of a different rate. For example, this often occurs while provisioning.

- a circuit pack has been provisioned for concatenated signals but an unequipped signal is sent
- there are unequipped connections at the far-end. This occurs since the far-end could be sending VT1.5/VC11 or VT2/VC12 unequipped, while the near-end is not provisioned to accept this connection. If the near-end was provisioned to expect a VT1.5/VC11 or VT2/VC12 connection, then an Unequipped alarm would be raised.

Impact

Major, service-affecting (M, SA) alarm, if on an active path

Minor, non-service-affecting (m, NSA) alarm, if on an inactive path in a UPSR/SNCP configuration

Critical, service-affecting (C, SA) alarm

Prerequisites

To perform this procedure, you must

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545
- use an account with at least a level 3 UPC
- have the optical fiber/cable connection information (that is, how the optical circuit packs on each network element connect to other network elements and how each OC-3 connects to the DSM)

Procedure 5-57 (continued)

Loss of Pointer

Step	Action
1	Verify if there are alarms of higher order from the alarm hierarchy. Refer to the “Alarm hierarchies and alarm severities” chapter in Part 1 of this document. Clear any alarms of higher order on the hierarchy first using the appropriate procedures.
2	If the original alarm has Then
	cleared the procedure is complete
	not cleared go to step 3
3	Identify the circuit pack raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document.
4	Use the optical fiber/cable connection information to identify the transmit and receive sites of the alarmed signal.
5	Log into the remote network element at the transmit end. If you cannot log in remotely from the local network element, you must travel to the remote site.
6	Retrieve all alarms from the transmit end. If the network element at the transmit end is not a 6500 network element, use the alarm system of the far-end network element to find the problem.
7	Look for an alarm message for the circuit pack connected to the original shelf. If Then
	there are no alarms or only a STS/VT/VC go to step 8
	RFI/RDI alarm at the transmit end
	there are additional alarms of a higher order refer to the “Alarm hierarchies from the alarm hierarchy at the transmit end and alarm severities” chapter in Part 1 of this document.
	the alarm did not clear go to step 8 .
8	Check that a cross-connect has been provisioned at the far-end network element, provision a cross-connect if required. Refer to the “Retrieving path connections” procedure in Part 1 of <i>Configuration - Bandwidth and Data Services</i> , 323-1851-320.
9	At the local network element, 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 10

Procedure 5-57 (continued)

Loss of Pointer

—end—

Procedure 5-58

Loss of Sequence - VCAT

Alarm IDs: 355, 356, 685, 686, 730, 731, 732, 929, 932, 1380

Probable cause

This alarm is raised when the received sequence number of an VT/STS/VC/PDH in a virtually concatenated group (VCG) does not match the expected sequence number. This alarm is raised against a VT/STS/VC/PDH that connects to the WAN port of a 4xGE, 1x10GE, 24x10/100BT, 20G L2SS, L2SS, PDH gateway, L2 MOTR, FLEX MOTR, RPR, or SuperMux circuit pack.

Sequence numbers specify the order of the VT/STS/VC/PDH members in a VCG. For a VCG of n members (where the sequence numbers are from 0 to n-1), when a middle member m is deleted, the sequence numbers from m+1 to n-1 shift downward to m to n-2 at the local end. Since the far-end has not changed, Loss of Sequence - VCAT alarms are raised at the local end on members from the sequence number m to n-2. All members of the WAN VCG must be examined to see if there are missing members associated with the far-end, not only the ones raising the alarms, as the incrementing timeslot order of the VT/STS/VC/PDH members may not be aligned with the sequence numbers.

Impact

Critical, service-affecting (C, SA) alarm

Prerequisites

To perform this procedure, you must:

- use an account with at least a level 3 UPC
- have the network connection information (that is, how the optical modules on each network element connect to other network elements)

Step	Action
------	--------

- 1 Log into each of the network elements on the VT/STS/VC/PDH path as required and retrieve the impacted WAN VCG cross-connects. Refer to the "Retrieving path connections" procedure in Part 1 of *Configuration - Bandwidth and Data Services*, 323-1851-320.

Procedure 5-58 (continued)

Loss of Sequence - VCAT

Step	Action
2	Verify the connection information for the entire path to ensure that the path is provisioned correctly. Examine all members of the VCG to see if there are missing members associated with the far-end. If the path provisioning is incorrect, modify the cross-connects as necessary. Refer to the “Retrieving path connections” procedure in Part 1 of <i>Configuration - Bandwidth and Data Services</i> , 323-1851-320.
3	If the original alarm has cleared not cleared
	Then the procedure is complete go to step 4
4	Ensure that all VT/STS/VC/PDH members of the virtually concatenated group originate from the same 4xGE, 1x10GE EPL, 24x10/100BT, 20G L2SS, L2SS, PDH gateway, L2 MOTR, FLEX MOTR, RPR, or SuperMux circuit pack.
5	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-59

Loss of Service Delineation

Alarm IDs: 1249

Probable cause

This alarm is raised when there is a lack of data frames from the network in the egress direction resulting in a client service interruption.

Impact

Major, service-affecting (M, SA) alarm if not protected

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

Prerequisites

To perform this procedure, you must:

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545
- have the optical fiber connection information (that is, how the optical modules on each network element connect to other network elements)

Step	Action
1	Identify the circuit pack and facility raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document.
2	Identify if any upstream circuit pack has active alarms and then troubleshoot/ clear these alarms first. If the far-end FLEX MOTR circuit pack has an OTM2 facility, clear any OTN faults (such as, LOS, LOC, LOF, LOM, ODU2-AIS, ODU2-LCK, ODU2-OCI, OPU2-AIS, or OPU2 Payload Type Mismatch) for all upstream OTM2 facilities. That is, clear all OTN alarms upstream from the far-end OTM2 port.
3	In the Site Manager Equipment & Facility Provisioning application, verify the ETH10G facility Packet Mapping value matches at both the near-end and far-ends. Refer to the “Retrieving equipment and facility details” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.

Procedure 5-59 (continued)

Loss of Service Delineation

Step	Action	
4	If the Packet Mapping values are mismatched	Then determine if it is the near-end alarmed ETH10G facility or the far-end facility that has the incorrect Packet Mapping value. The incorrectly provisioned facility must be deleted and reprovisioned with the correct Packet Mapping value. Refer to the “Deleting a facility from an equipment” and “Adding a facility to an equipment” procedures in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310. Go to step 5.
	match	go to step 5
5	Ensure that the subtending client equipment is transmitting a valid GFP-F (for Gigabit Ethernet) signal, as required.	
6	If the alarm does not clear, contact your next level of support or your Ciena support group.	

—end—

Procedure 5-60

Loss Of Signal (Ethernet)

Alarm IDs: 347, 824

Probable cause

This alarm is raised against an Ethernet facility of a 4xGE EPL, 1x10GE EPL, 24x10/100BT EPL, 20G L2SS, L2SS, PDH gateway, L2 MOTR, FLEX MOTR, RPR, or SuperMux circuit pack when the circuit pack cannot detect an input signal on the LAN-side facility.

There are two variants of the 24x10/100BT EPL circuit pack. One provides only electrical (10/100BT) interfaces, and the other provides a choice of electrical (10/100BT) and/or optical (FE/100FX SFP) interfaces.

This alarm is caused by one of the following conditions:

- an optical fiber cut
- an RJ45 cable cut (for 10/100BT interfaces)
- dirty optical fibers
- dirty connectors
- excessive attenuation

When this alarm is raised, the Link Down alarm is also raised.

Impact

Critical, service-affecting (C, SA) alarm

Prerequisites

To perform this procedure, you must

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545
- have an antistatic wrist strap to dissipate electrostatic charges
- have the optical fiber connection information (that is, how the optical modules on each network element connect to other network elements)
- have an optical power meter with the same optical connectors as the network element
- if required, obtain a supported SFP optical transceiver module

Procedure 5-60 (continued) **Loss Of Signal (Ethernet)**

Step	Action												
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	If the interface is optical electrical												
	Then go to												
	step 3												
	step 15												
3	<p>CAUTION</p>  <p>Risk of traffic loss</p> <p>Ensure that the correct module is identified. Removing the wrong optical fiber causes a traffic loss on an in-service facility.</p>												
	<p>CAUTION</p>  <p>Risk of laser radiation exposure</p> <p>Laser radiation is present on the optical fiber. Do not look into the optical fiber.</p>												
4	<p>Use the optical power meter to measure the receive power at the LAN port. For information about technical specifications (minimum and maximum receive optical power) for the SFPs supported on the alarmed circuit pack, refer to the “Technical specifications” chapter in Part 3 of the <i>6500 Planning, NTRN10EG</i>.</p> <table border="1"> <thead> <tr> <th data-bbox="527 1303 564 1320">If</th> <th data-bbox="527 1303 977 1320">the receive power at the LAN port is</th> <th data-bbox="1269 1303 1312 1320">Then go to</th> </tr> </thead> <tbody> <tr> <td data-bbox="527 1336 564 1353"></td><td data-bbox="527 1336 977 1353">below the minimum receive optical power</td><td data-bbox="1269 1336 1312 1353">step 5</td></tr> <tr> <td data-bbox="527 1370 564 1387"></td><td data-bbox="527 1370 977 1387">between the minimum and maximum receive optical power</td><td data-bbox="1269 1370 1312 1387">step 9</td></tr> <tr> <td data-bbox="527 1404 564 1421"></td><td data-bbox="527 1404 977 1421">above the maximum receive optical power</td><td data-bbox="1269 1404 1312 1421">step 10</td></tr> </tbody> </table>	If	the receive power at the LAN port is	Then go to		below the minimum receive optical power	step 5		between the minimum and maximum receive optical power	step 9		above the maximum receive optical power	step 10
If	the receive power at the LAN port is	Then go to											
	below the minimum receive optical power	step 5											
	between the minimum and maximum receive optical power	step 9											
	above the maximum receive optical power	step 10											

Receive power is below the minimum receive optical power

- | | | |
|---|---|-------------------|
| 5 | Decrease the local attenuation, if equipped, to try to increase the receive power to a value above the minimum receive optical power (but below the maximum receive optical power). | |
| 6 | If the adjusted receive power is | Then go to |
| | still below the minimum receive optical power | step 7 |
| | within range (between the minimum and the maximum receive optical power) | step 9 |

Procedure 5-60 (continued)
Loss Of Signal (Ethernet)

Step	Action				
7	Remove the Tx optical fiber from the far-end subtending client equipment.				
8	Measure the transmit power at the far-end subtending client equipment. <ul style="list-style-type: none"> • If the transmit power of the far-end equipment is above the minimum launch power, the optical fiber attenuation is too high, the optical fiber connections are dirty, or the optical fiber is damaged. • If the transmit power of the far-end equipment is below the minimum launch power, there is a problem with the far-end equipment. Use your company procedure to determine and clear the problem. Then go to step 11 .				
	<i>If receive power is between the minimum and the maximum receive optical power</i>				
9	Clean all connections at both ends of the optical fiber link following your company standards and re-attach the optical fibers. Go to step 11 .				
	<i>If receive power is above the maximum receive optical power</i>				
10	Add the necessary attenuation to reduce the receive optical power to a value between the minimum and maximum receive optical power.				
Determining if the alarm cleared					
11	If the original alarm has Then <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">cleared</td> <td>the procedure is complete</td> </tr> <tr> <td>not cleared</td> <td>replace the SFP that corresponds to the facility raising the alarm. Refer to the “Replacing a Pluggable module” procedure in <i>Fault Management - Module Replacement</i>, 323-1851-545.</td> </tr> </table>	cleared	the procedure is complete	not cleared	replace the SFP that corresponds to the facility raising the alarm. Refer to the “Replacing a Pluggable module” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.
cleared	the procedure is complete				
not cleared	replace the SFP that corresponds to the facility raising the alarm. Refer to the “Replacing a Pluggable module” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.				
12	If the original alarm has Then <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">cleared</td> <td>the procedure is complete</td> </tr> <tr> <td>not cleared</td> <td>replace the circuit pack reporting the alarm. Refer to the “Replacing a 4xGE, 4xGE EPL EFM, or 1x10GE EPL circuit pack” procedure in <i>Fault Management - Module Replacement</i>, 323-1851-545.</td> </tr> </table>	cleared	the procedure is complete	not cleared	replace the circuit pack reporting the alarm. Refer to the “Replacing a 4xGE, 4xGE EPL EFM, or 1x10GE EPL circuit pack” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.
cleared	the procedure is complete				
not cleared	replace the circuit pack reporting the alarm. Refer to the “Replacing a 4xGE, 4xGE EPL EFM, or 1x10GE EPL circuit pack” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.				
13	Clean and re-attach the optical fibers. Refer to the cleaning connectors procedures in <i>Installation - General Information</i> , 323-1851-201.0.				
14	If the original alarm has Then <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">cleared</td> <td>the procedure is complete</td> </tr> <tr> <td>not cleared</td> <td>go to step 17</td> </tr> </table>	cleared	the procedure is complete	not cleared	go to step 17
cleared	the procedure is complete				
not cleared	go to step 17				

Step	Action						
15	<p>CAUTION</p> <p>Risk of traffic loss</p> <p>Ensure that the correct module is identified. Removing the wrong cable causes a traffic loss on an in-service facility.</p>						
	<p>Inspect the cabling and connectors on the I/O panel. The cabling may be loose or damaged. Repair any damage.</p>						
16	<table style="width: 100%; border-collapse: collapse;"><thead><tr><th style="width: 50%;">If the original alarm has</th><th style="width: 50%;">Then</th></tr></thead><tbody><tr><td>cleared</td><td>the procedure is complete</td></tr><tr><td>not cleared</td><td>go to step 17</td></tr></tbody></table>	If the original alarm has	Then	cleared	the procedure is complete	not cleared	go to step 17
If the original alarm has	Then						
cleared	the procedure is complete						
not cleared	go to step 17						
17	If the alarm does not clear, contact your next level of support or your Ciena support group.						

—end—

Procedure 5-61

Loss Of Signal (OC/STM, ETH10G, ETH40G, ETH100G, FC, OTM1, OTM2, OTM3, OTM4, PTP, FLEX)

Use this procedure to clear alarms associated with the Loss Of Signal alarms.

Note that when a Loss Of Signal condition occurs on the 40G OCI circuit pack, detection and signal conditioning takes place based on Loss of Frame detection rather than on LOS. When the LOS recovers at the near-end 40G OCI, some transient alarms such as LOS, OOF, and LOF will be experienced by the subtending equipment or test set connected to the far-end 40G OCI prior to traffic recovery.

For 40G/100G OCLD circuit packs, the power level must be above the LOS clear threshold value for traffic to recover. For 40G/100G OCLD circuit packs, traffic can run below the LOS threshold value. However, if traffic is lost, traffic will not recover until the power level is above the LOS clear threshold. See the “Technical specifications” tables in *WaveLogic Ai, Flex, 100G+, 40G, OSIC ISS, and SLIC10 Circuit Packs*, 323-1851-102.4 for the 40G/100G OCLD expected LOS alarm clear threshold values.

ATTENTION

For electrical SFPs (NTTP61BA), if this alarm is raised and the traffic cannot be brought up, change the TXCON state to Disabled.

Loss Of Signal (OC1/OC3/12/STM1/4)

Alarm ID: 32, 248, 894, 1688

Probable cause

This alarm is raised when the circuit pack:

- can no longer detect a signal on the optical fiber/cable
- detects a receiver overload condition (10G DWDM circuit packs only)

This alarm is caused by one of the following conditions on the network element or DS1 service module (DSM):

- circuit pack missing
- circuit pack mismatch
- optical fiber/cable cut
- dirty optical fibers
- dirty connectors

Procedure 5-61 (continued)

Loss Of Signal (OC/STM, ETH10G, ETH40G, ETH100G, FC, OTM1, OTM2, OTM3, OTM4, PTP, FLEX)

- incorrect attenuation
- incorrect optical fiber cross-connect

A Loss Of Signal alarm will not clear until a framed OC-n/STM-n or DS1 (DS1 from the DSM 84xDS1 termination module) signal is detected.

ATTENTION

If ALS is enabled, a Loss Of Signal will be raised at both ends of the link, as the laser is turned off under a Loss Of Signal condition. To help determine on which end the Loss Of Signal alarm must be cleared, temporarily disable ALS at both ends. Refer to the “Editing facility parameters” procedure in Part 1 of *Configuration - Provisioning and Operating*, 323-1851-310.

Note: If a 10G signal (ETH10G or OC192/STM64) is applied to the 40G OCI (NTK529SA or NTK529SDE5) circuit pack, a “Loss Of Signal” alarm could be raised instead of the expected “Loss of Clock” alarm, due to a limitation of the 40G transponders. When an incorrect 40G signal is applied, the “Loss of Clock” alarm will be raised.

Impact

Critical, service-affecting (C, SA) alarm for UPSR/SNCP configuration with cross-connects

Critical, service-affecting (C, SA) alarm, if active 1+1/MSP linear or unprotected with cross-connects

Critical, service-affecting (C, SA) alarm for an unprotected 2-Fiber/4-Fiber BLSR/MS-SPRing/HERS

Minor, non-service-affecting (m, NSA) alarm, if inactive 1+1/MSP linear, protected 1+1/MSP linear, or without cross-connects

Minor, non-service-affecting (m, NSA) alarm for a protected 2-Fiber/4-Fiber BLSR/MS-SPRing/HERS

Loss Of Signal (OC48/OC192/OC768/STM16/STM64/STM256)

Alarm ID: 1, 279, 982

Loss Of Signal (ETH10G/ETH40G/ETH100G)

Alarm ID: 673, 1295

Loss Of Signal (FC100/FC200/FC400, FC800, FC1200, FLEX)

Alarm ID: 365, 1252

Probable cause

This alarm is raised when the client Rx interface detects no light, low power or no DC (no 0/1 transition).

Procedure 5-61 (continued)

Loss Of Signal (OC/STM, ETH10G, ETH40G, ETH100G, FC, OTM1, OTM2, OTM3, OTM4, PTP, FLEX)

For ETH10G, ETH40G, and ETH100G clients using parallel optics, this alarm is raised when a Loss of Frame and low optical input power on any of the CFP optical carriers is detected.

Impact

Critical, service-affecting (C, SA) alarm

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

Loss Of Signal (OTM1, OTM2, OTM3, OTM4, PTP)

Alarm ID: 668, 1001, 1170, 1586

Probable cause

This alarm is raised when the Rx interface detects a Loss of Frame and the optical power is below the Loss Of Signal threshold.

The network element cannot clear a Loss Of Signal alarm until the optical power level goes above the LOS clear threshold.

Note that after removing a LOS or LOF fault condition on the 40G OCLD, Wavelength-Selective 40G OCLD Rx OTM3, or 100G OCLD Rx OTM4 facility, traffic restoration can take up to nine seconds.

Impact

Critical, service-affecting (C, SA) alarm

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

The impact for the 10G AM1/AM2 and 1xOC-192/STM-64 DWDM circuit packs only is as follows:

Critical, service-affecting (C, SA) alarm for UPSR/SNCP configuration with cross-connects

Critical, service-affecting (C, SA) alarm, if active 1+1/MSP linear, 1+1 port TPT, or 1+1 TPT configuration or unprotected with cross-connects

Critical, service-affecting (C, SA) alarm for an unprotected 2-Fiber/4-Fiber BLSR/MS-SPRing/HERS

Minor, non-service-affecting (m, NSA) alarm, if inactive 1+1/MSP linear, 1+1 port TPT, or 1+1 TPT configuration, protected 1+1/MSP linear, 1+1 port TPT, or 1+1 TPT configuration, or without cross-connects

Minor, non-service-affecting (m, NSA) alarm for a protected 2-Fiber/4-Fiber BLSR/MS-SPRing/HERS

Minor, non-service-affecting (m, NSA) alarm when there are no L2 components provisioned on the port

Procedure 5-61 (continued)

Loss Of Signal (OC/STM, ETH10G, ETH40G, ETH100G, FC, OTM1, OTM2, OTM3, OTM4, PTP, FLEX)

Prerequisites

To perform this procedure, you must

- have the optical fiber connection information (that is, how the circuit packs on each network element connect to other network elements)
 - have an optical power meter with the same optical connectors as the network element
 - observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545
 - have an antistatic wrist strap to dissipate electrostatic charges

Step	Action
1	Identify the circuit pack and facility raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document.
2	If the alarm is raised against a Then go to
	line port step 3
	client port step 27
3	If a photonic line system is used to transport the signal of the circuit pack raising the alarm, retrieve all alarms on the photonic line system. Clear any alarms associated with the Loss Of Signal alarm using the appropriate procedures.
	If the signal for this circuit pack is the only signal dropping on a CMD44, check the WSS switch Out to CMD44 Common In fiber, and the CMD44 channel out to OCLD Rx fiber.
	Note: Use optical terminators on unused input faceplate connectors of installed WSS w/OPM circuit packs. If dust caps are used instead of optical terminators on “Switch In” ports, PMs can be reported against the ports and the ports may appear in-service.
4	If the original alarm has Then
	cleared the procedure is complete
	not cleared go to step 5
5	Use the optical fiber/cable connection information to identify the transmit and receive sites of the alarmed signal.
6	Log into the remote network element at the transmit end.

Procedure 5-61 (continued)

Loss Of Signal (OC/STM, ETH10G, ETH40G, ETH100G, FC, OTM1, OTM2, OTM3, OTM4, PTP, FLEX)

Procedure 5-61 (continued)

Loss Of Signal (OC/STM, ETH10G, ETH40G, ETH100G, FC, OTM1, OTM2, OTM3, OTM4, PTP, FLEX)

Step	Action
16	Determine the optical power level into the Rx interface using one of the following methods: <ul style="list-style-type: none"> • Using the Site Manager Equipment & Facility Provisioning application under the Configuration menu, retrieve the Rx Actual Power (dBm) value for the facility reporting the alarm. Refer to the “Retrieving optical power, wavelength, and dispersion ranges” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i>, 323-1851-310. • Use the optical power meter to measure the optical power level into the Rx interface, and verify it is within technical specifications. Refer to the “Technical specifications” chapter in Part 3 of the <i>6500 Planning</i>, NTRN10EG.
<div style="border: 1px solid black; padding: 10px; text-align: center;">  <p>CAUTION Risk of traffic loss If MPO cables are used, ensure there is no traffic on the MPO cables before removing the cables.</p> </div>	
17	If the measured optical power is
	below the receiver sensitivity specified for the circuit pack
	above the receiver sensitivity specified for the circuit pack
	within the receiver sensitivity range specified for the circuit pack
18	Then go to
	step 18
	step 20
	step 24
	Remove the Tx fiber from the far-end circuit pack, and use the optical power meter to measure the transmit power at the far-end.

Procedure 5-61 (continued)

Loss Of Signal (OC/STM, ETH10G, ETH40G, ETH100G, FC, OTM1, OTM2, OTM3, OTM4, PTP, FLEX)

Step	Action
19	If the transmit power at the far-end is above the launch power (minimum) Then the optical fiber attenuation is too high, the optical fiber connections are dirty, or the optical fiber is damaged. Use your company procedure to determine and clear the problem. If a photonic line system is used to transport the signal, the attenuation can be caused by the line system. Clear any alarms on the photonic line associated with the Loss Of Signal alarm using the appropriate procedures. Go to step 26.
	below the launch power (minimum) if the circuit pack at the transmit end supports SFPs/DPOs, replace the SFP/DPO that corresponds to the facility raising the alarm. Refer to the “Replacing a Pluggable module” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545. if the circuit pack at the transmit end does not support SFPs/DPOs, replace the required circuit pack at the transmit end. Refer to the “Replacing a Pluggable module” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545. Go to step 26.
	within the launch power range specified for the circuit pack go to step 26 .
20	Clean all connections at both ends of the optical fiber link following your company standards and re-attach the optical fibers. Refer to the cleaning connectors procedures in <i>Installation - General Information</i> , 323-1851-201.0.
21	If the original alarm has cleared Then the procedure is complete not cleared go to step 22

Procedure 5-61 (continued)

Loss Of Signal (OC/STM, ETH10G, ETH40G, ETH100G, FC, OTM1, OTM2, OTM3, OTM4, PTP, FLEX)

Procedure 5-61 (continued)

Loss Of Signal (OC/STM, ETH10G, ETH40G, ETH100G, FC, OTM1, OTM2, OTM3, OTM4, PTP, FLEX)

Step	Action
30	If the original alarm has cleared Then the procedure is complete not cleared go to step 31
31	For multi lane interfaces, if possible, check on both the subtending circuit pack (transmit direction) and locally (receive direction) individual lane power. For Rx/Tx power values for pluggables, refer to the pluggables summary and reference tables in “Pluggables Datasheets and Reference”, 323-1851-180. Note: Validate the individual lane power using Site Manager “Equipment & Facility Provisioning” application by selecting the equipment and client facility in question and clicking the “Lane Power” button.
32	If on the transmit interface only a subset of the lanes exhibit power outside of the expected range, then it is recommended that the transmit interface be replaced.
33	If on the receive interface only a subset of the lanes exhibit power outside of the expected range, then the hardware issue might be on either the transmitter or the receiver.
34	Determine the optical power level into the Rx interface using one of the following methods: <ul style="list-style-type: none"> • Using the Site Manager Equipment & Facility Provisioning application under the Configuration menu, retrieve the Rx Actual Power (dBm) value for the facility reporting the alarm. Refer to the “Retrieving OTM info” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i>, 323-1851-310. • Use the optical power meter to measure the optical power level into the Rx interface, and verify it is within technical specifications. Refer to the “Technical specifications” chapter in Part 3 of the <i>6500 Planning</i>, NTRN10EG.
35	If the measured optical power is below the Rx minimum power (dBm) value Then go to step 36 above the Rx maximum power (dBm) value step 37 between the Rx minimum power (dBm) and Rx maximum power (dBm) values step 38
36	Check the fiber and fiber cleanliness between the subtending equipment and the port reporting the alarm. Correct any issues found. Go to step 38 .

Procedure 5-61 (continued)

Loss Of Signal (OC/STM, ETH10G, ETH40G, ETH100G, FC, OTM1, OTM2, OTM3, OTM4, PTP, FLEX)

Step	Action											
37	The signal may require padding, or you are not using the correct pluggable type on the circuit pack reporting the alarm or on the subtending equipment. Contact your next level of support for more information.											
	Go to step 38 .											
38	If the original alarm has	Then										
	cleared											the procedure is complete
	not cleared											perform a warm restart on the circuit pack reporting the alarm. Refer to the “Restarting a circuit pack or shelf processor” procedure in Part 1 of the <i>Fault Management - Alarm Clearing</i> , 323-1851-543.
39	If the alarm does not clear, contact your next level of support or your Ciena support group.											

—end—

Procedure 5-62 Loss Of Signal (OPTMON, VOA)

Alarm IDs: 560, 553

Probable cause

This alarm is raised against an OPTMON or VOA facility when:

- the optical power transmitted and/or optical power received 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.

For CDC configurations, this alarm is raised on CCMD8x16, RLA 5x1 or CCMD12 circuit packs.

The conditions that can cause this alarm include:

- a disconnected, or defective fiber optic patchcord
- a dirty optical fiber connector
- a defective module
- defective transmitting subtending equipment
- a provisioning error in the LOS threshold of the alarmed facility

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.

Procedure 5-62 (continued)

Loss Of Signal (OPTMON, VOA)

In rare cases of SP restarts, the WSS w/OPM AINS state is lost and this alarm is raised against ports that have never received a valid optical signal. To clear this alarm, you can edit the Auto In-Service Time of the OPTMON facilities to re-enable the AINS state or change the primary state of the OPTMON facilities to OOS. This can be done using the Configuration->Equipment and Facility Provisioning application in Site Manager or by enabling AINS and editing the AINS Time Out parameter from the Site Manager Node Information application Edit System dialog box. Refer to the “Editing facility parameters” procedure in Part 1 of *Configuration - Provisioning and Operating*, 323-1851-310, or the “Editing the nodal system parameters” and “Editing the AINS default period” procedures in *Administration and Security*, 323-1851-301.

ATTENTION

In a single-channel photonic network, network level alarm correlation is unable to distinguish the following: In the Mux direction: cannot distinguish the difference between CMD44 channel input port LOS and WSS switch in LOS. In the Demux direction: cannot distinguish the difference between a CMD44 Common in LOS and a OTM facility LOS; manual fault isolation may be required to find the root cause of the fault.

ATTENTION

When the NTK592NGE5 SFP is used in spans with a span loss greater than 20.5 dB, due to SFP's lower Tx output power, a permanent LOS alarm will be active against the LIM port 4 OPTMON facility (since this SFP can support span losses up to 31.5 dB). To avoid this condition, software automatically puts the LIM port 4 OPTMON facility (OPTMON-bay-shelf-slot-4) in the OOS state (OOS-MA) when the NTK592NGE5 SFP is provisioned. This will prevent the Loss of Signal alarm from being raised. As a result, since the LIM port 4 OPTMON facility alarm never gets raised, it is not possible to infer if the problem is before the LIM or after. When the NTK592NVE5 SFP is used, the OSC Rx power can be very low under normal operating conditions (compared to the NTK592NPE6, NTK592NBE6 and NTK592NHE6 SFPs) and a permanent LOS alarm may be active against the LIM port 4 OPTMON facility even though there is no problem (since this SFP can support span losses up to 42 dB). To avoid this condition, software automatically puts the LIM port 4 OPTMON facility (OPTMON-bay-shelf-slot-4) in the OOS state (OOS-MA) when the NTK592NGE5 SFP is provisioned. This will prevent the Loss of Signal alarm from being raised. As a result, since the LIM port 4 OPTMON facility alarm never gets raised, it is not possible to infer if the problem is before the LIM. The LIM port 4 OPTMON will have a LOS threshold of “N/A”.

Procedure 5-62 (continued)

Loss Of Signal (OPTMON, VOA)

In Release 9.1 and earlier, there had to be two SPLI compliant receivers with provisioned far-end addresses reporting LOS before the OTM LOS would be masked by “Loss Of Signal” (OPTMON). As of Release 9.2, even if there is only one receiver provisioned (and with a far-end address), the OTM LOS is masked and replaced with a “Loss Of Signal” (OPTMON) on the common input port of that demux.

Additionally, any CMD with no channels will set the upgrade in port of its upstream CMD to a faulted state.

Impact

Major, service-affecting (M, SA) alarm (OPTMON and VOA)

Minor, non-service-affecting (m, NSA) alarm, if inactive (OPTMON)

Prerequisites

To perform this procedure, you must:

- use an account with at least a level 3 UPC
- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0
- have a network and site diagram
- have a fiber cleaning kit
- obtain a replacement circuit pack, if required

Step	Action
1	This condition may be caused by an upstream fault. Before following this procedure, check for and clear any upstream alarms.
2	Check for and clear any of the following alarms before clearing this alarm: <ul style="list-style-type: none"> • Automatic Power Reduction Active • Automatic Shutoff • Input Loss Of Signal • Optical Line Fail • Output Loss Of Signal • Shutoff Threshold Crossed

1 This condition may be caused by an upstream fault. Before following this procedure, check for and clear any upstream alarms.

2 Check for and clear any of the following alarms before clearing this alarm:

- Automatic Power Reduction Active
- Automatic Shutoff
- Input Loss Of Signal
- Optical Line Fail
- Output Loss Of Signal
- Shutoff Threshold Crossed

Procedure 5-62 (continued)
Loss Of Signal (OPTMON, VOA)

Step	Action	
3	Verify that the OPTMON or VOA facility parameters are provisioned correctly. If necessary, correct any discrepancies. This can be done using the Configuration->Equipment and Facility Provisioning screen in Site Manager. Refer to the “Retrieving equipment and facility details” and “Editing facility parameters” procedures and the OPTMON facility parameter table or VOA facility parameter table in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.	
4	If the alarm is raised against a OMD4, OMDF4, OMDF8, BS1, BS2, BS3, BS5, OMX, OBB, OBMD 1x8, CMD 64, CMD96, CCMD8x16, CCMD12, or CMD44 channel input port an RLA 5x1 any other port	Then go to step 5 step 14 step 13
5	If this is a single-channel photonic network, verify the optical patchcords between the CMD44 Common Out and the RLA 5x1 or WSS input port, and between the WSS Common Out and the LIM Line B Input: <ul style="list-style-type: none">ensure it is connected at both ends and that there is no problem with the optical patchcordclean the connectors. Refer to the cleaning connectors procedures in <i>Installation - General Information</i>, 323-1851-201.0.ensure the transmitting equipment is functioning correctly and transmitting a valid signal	
6	<p>Note: Use optical terminators on unused input faceplate connectors of installed WSS w/OPM circuit packs or RLA 5x1 module. If dust caps are used instead of optical terminators on “Switch In” ports, PMs can be reported against the ports and the ports may appear in-service.</p> Verify the optical patchcord between the subtending equipment and the OMD4, OMDF4, OMDF8, BS1, BS2, BS3, BS5, OMX, OBB, OBMD 1x8, CMD 64, CMD96, CCMD8x16, CCMD12, or CMD44 channel input port: <ul style="list-style-type: none">ensure it is connected at both ends and that there is no problem with the optical patchcordclean the connectors. Refer to the cleaning connectors procedures in <i>Installation - General Information</i>, 323-1851-201.0.ensure the transmitting subtending equipment is functioning correctly and transmitting a valid signal	

Procedure 5-62 (continued)
Loss Of Signal (OPTMON, VOA)

Step	Action	Then
7	If the original alarm has cleared not cleared	the procedure is complete go to step 8
8	Verify the optical patchcord connected to the port reporting the alarm: <ul style="list-style-type: none">• ensure it is connected at both ends and that there is no problem with the optical patchcord• clean the connectors. Refer to the cleaning connectors procedures in <i>Installation - General Information</i>, 323-1851-201.0.	
9	If the original alarm has cleared not cleared	the procedure is complete go to step 10
10	Using the Performance->Performance Monitoring->New screen of Site Manager, compare the untimed OPR-OTS 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 “Editing facility parameters” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.	
11	Wait at least one minute for the Loss Of Signal alarm to clear. Change the LOS Threshold value back to the original value.	
12	If the original alarm has cleared not cleared	the procedure is complete go to step 13
13	If the alarm is raised against an unused WSS or RLA 5x1 ingress port (the port with no adjacency provisioned) any other port	Then go to step 14 step 16
14	Set the secondary state of the port to AINS using the Configuration->Equipment and Facility provisioning screen of Site Manager. Refer to the “Editing facility parameters” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.	
15	Run another OTDR trace on the faulted RLA 5x1. Refer to “Performing a manual OTDR trace” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.	
16	If the alarm does not clear, contact your next level of support or your Ciena support group.	

—end—

Procedure 5-63

Loss Of Synchronization Messaging Channel

Alarm IDs: 2009

Probable cause

This alarm is raised against a facility when:

- the facility is a SyncE reference
- the Sync Status Message (SSMTRANSMIT) is not disabled on the facility
- the circuit pack does not detect ESMC messages for more than 5 seconds. The missing ESMC message happens in the following scenarios:
 - when the circuit pack does not detect the signal on the fiber/cable
 - far end does not transmit ESMC packets
 - the fiber/cable cut
 - dirty fiber, cable, or connectors
 - incorrect attenuation

Impact

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

Prerequisites

To perform this procedure, you must:

- use an account with at least a level 3 UPC
- observe all safety requirements described in Part 1 of *Installation*, 323-1851-201, or *Fault Management - Module Replacement*, 323-1851-545
- have the engineering documentation package (EDP)
- have a fiber cleaning kit

Step	Action
1	Identify the module that raised the alarm. See “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document.
2	If you do not require the Sync Status Message (SSMTRANSMIT), disable the Sync Status Messaging.
3	Verify the alarm causes from the probable cause list above and clear the issue using the appropriate procedures.

- | | |
| --- | --- |
| 1 | Identify the module that raised the alarm. See “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document. |
| 2 | If you do not require the Sync Status Message (SSMTRANSMIT), disable the Sync Status Messaging. |
| 3 | Verify the alarm causes from the probable cause list above and clear the issue using the appropriate procedures. |
-

Procedure 5-63 (continued)

Loss Of Synchronization Messaging Channel

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

—end—

Procedure 5-64

Low Optical Return Loss at Input

Alarm IDs: 1760

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 input, which can be caused by:

- dirty optical connectors
- improper optical cable mating
- a disconnected optical fiber at the SRA input
- an optical fiber cut
- a degraded optical fiber

Impact

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

Prerequisites

To perform this procedure, you must:

- use an account with at least a level 3 UPC
- observe all the safety requirements described in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545
- have an antistatic wrist strap to dissipate electrostatic charges
- have the engineering documentation package (EDP)
- have a fiber cleaning kit
- have a replacement module

Procedure 5-64 (continued)
Low Optical Return Loss at Input

Step	Action
1	<p>If this alarm</p> <p>was raised as a result of a maintenance activity or during SLAT, and is expected</p> <p>is unexpected</p> <p>Then</p> <p>no action is required. The alarm will clear when the maintenance activity or SLAT is completed.</p> <p>The procedure is complete.</p> <p>See the Attention box, then go to step 2</p>
	<p>ATTENTION</p> <p>Continuing with this procedure triggers Automatic Laser Shut Off (ALSO) and will cause traffic loss in both directions.</p>
2	<p>Place the RAMAN facility corresponding to the alarm and the Line A amplifier connected to the SRA circuit pack OOS.</p>
	<p>DANGER</p>  <p>Risk of laser radiation exposure</p> <p>Do not look directly into the optical beam. Invisible light can severely damage your eyes.</p>
	<p>CAUTION</p>  <p>Risk of damage to modules</p> <p>Never disconnect an optical fiber that is connected to an active or powered up optical amplifier or SRA circuit pack. To disconnect or reconnect an optical fiber, make sure the optical amplifier is out of service (OOS), then disconnect or reconnect the fiber.</p>
	<p>CAUTION</p>  <p>Risk of damage to modules</p> <p>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.</p>

Procedure 5-64 (continued)

Low Optical Return Loss at Input

Step	Action
	<div style="border: 1px solid black; padding: 10px; text-align: center;"><p>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 input fiber of the SRA will impact traffic in both directions, as it triggers ALSO.</p></div>
3	Inspect and clean the input fiber and place the facilities back to IS.
4	If the alarm has not cleared, place the facilities back to OOS and check any upstream patch panel connectors at that site.
5	Place the facilities back to IS.
6	If the alarm is not cleared, 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 the “Locating a reflective event” procedure in Part 1 of this document.
7	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-65

Low Optical Return Loss at Output

Alarm IDs: 559, 1033, 1684, 1796

Probable cause

This alarm is raised against:

- an AMP or RAMAN facility of a LIM, RLA 5x1, or XLA circuit pack when the optical return loss (ORL) at the output drops below a fixed threshold
- an AMPMON facility of a LIM, XLA, SRA or FGA module/circuit pack
- a VOA facility of a LIM module

Low ORL indicates high reflection at the amplifier output, which 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
- misprovisioning of an amplifier resulting in excessive power being injected into the mid-stage DSCM or fiber-plant

Impact

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

Prerequisites

To perform this procedure, you must:

- use an account with at least a level 3 UPC
- observe all the safety requirements described in *Installation - General Information*, 323-1851-201.0
- have an antistatic wrist strap to dissipate electrostatic charges
- have the engineering documentation package (EDP)
- have a fiber cleaning kit
- have a replacement module

Procedure 5-65 (continued)

Low Optical Return Loss at Output

Step	Action
1	If this alarm was raised as a result of a maintenance activity or during SLAT, and is expected is unexpected
	Then no action is required. The alarm will clear when the maintenance activity or SLAT is completed. The procedure is complete. go to step 2
2	Check the alarmed amplifier power level defined in your EDP against the provisioned AMP or RAMAN facility parameter values. Edit the power level values as required. Refer to the “Retrieving equipment and facility details” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
3	If the original alarm has cleared not cleared
	Then the procedure is complete go to step 4
4	If the alarmed amplifier is a pre-amplifier otherwise
	Then go to step 5 step 8
5	 DANGER Risk of laser radiation exposure Do not look directly into the optical beam. Invisible light can severely damage your eyes.
	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 cleared not cleared
	Then the procedure is complete go to step 8

Procedure 5-65 (continued)
Low Optical Return Loss at Output

Step	Action						
8	<p>CAUTION Risk of damage to modules</p>  <p>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 out of service (OOS), then disconnect or reconnect the fiber.</p>						
	<p>CAUTION Risk of damage to modules</p>  <p>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.</p>						
	<p>Place the alarmed AMP or RAMAN facility out of service (OOS). Refer to the “Changing the primary state of a facility” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i>, 323-1851-310.</p> <p>Note: An AMPMON facility is a child facility of the corresponding AMP facility and its primary state always follows the primary state of the parent AMP. The parent AMP refers to the AMP facility on the input port of the same Line. An AMPMON facility is auto-created or deleted subsequently after the creation or deletion of the parent AMP facility.</p>						
9	<p>CAUTION Risk of traffic loss</p>  <p>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 Laser Shut Off (ALSO).</p>						
	<p>Disconnect the output fiber of the alarmed optical amplifier, clean the output fiber and connectors at the amplifier, then reconnect the fiber.</p>						
10	<p>Place the AMP or RAMAN facility back in-service (IS). Refer to the “Changing the primary state of a facility” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i>, 323-1851-310.</p>						
11	<table style="width: 100%; border-collapse: collapse;"> <tr> <th style="width: 40%;">If the original alarm has</th> <th style="width: 60%;">Then</th> </tr> <tr> <td>cleared</td> <td>the procedure is complete</td> </tr> <tr> <td>not cleared</td> <td>go to step 12</td> </tr> </table>	If the original alarm has	Then	cleared	the procedure is complete	not cleared	go to step 12
If the original alarm has	Then						
cleared	the procedure is complete						
not cleared	go to step 12						

Procedure 5-65 (continued)

Low Optical Return Loss at Output

Step	Action
12	You may need 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 the “Locating a reflective event” procedure in Part 1 of this document.
13	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-66

Low Order Bandwidth Near Limit

Alarm ID: 613

Probable cause

This alarm is raised against the shelf to indicate that the provisioned low-order bandwidth is approaching the maximum allowed for low-order traffic.

The alarm is raised when 90% of the 20G low-order capacity is reached on the NTK557PA, NTK557QA, and NTK557TB cross-connects or when 90% of the 80G low-order capacity is reached on the NTK557NA cross-connect.

Impact

Warning

Prerequisites

To perform this procedure, you require an account with at least a level 3 UPC.

Step	Action
1	<p>Delete any low-order cross-connects that are not required. Refer to the “Deleting path connections” procedure in Part 1 of <i>Configuration - Bandwidth and Data Services</i>, 323-1851-320.</p> <p>For information about how to calculate the number of cross-connects depending on the connection rate, refer to the “Connection and Bandwidth Management” section in Part 1 of the <i>6500 Planning</i>, NTRN10EG.</p>
2	If more low-order bandwidth is required, contact your network administrator to determine your course of action.

—end—

Procedure 5-67

Low Received Span Loss

Alarm ID: 1284

Probable cause

This alarm is raised against the LIM (at the tail end of the span), SRA, SAM, RLA 5x1, or ESAM circuit packs when the incoming estimated OSC/Telemetry Gain Span Loss for the span is lower than the Minimum Span Loss less the Span Loss Margin (Minimum Span Loss - Span Loss Margin).

The alarm clears when the Span Loss is greater than (Minimum Span Loss - Span Loss Margin) + 1 dB.

Note: Span Loss for an optical span is stored as a PM with full retrievable history. Refer to the “Retrieving performance monitoring data” in the *Fault Management - Performance Monitoring*, 323-1851-520.

For RAMAN amplifiers, the Telemetry Gain Signal value is used for Span Loss calculation. Refer to the *Photonic Layer Guide*, NTRN15DA, for more information.

It is recommended that the Low Received Span Loss detection and alarming be disabled. This alarm becomes redundant as a result of the amplifier “Minimum Gain” alarm.

Impact

Major, service-affecting (M, SA) alarm

Prerequisites

To perform this procedure, you must:

- use an account with at least a level 3 UPC
- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545
- have an antistatic wrist strap to dissipate electrostatic charges
- have a fiber cleaning kit
- obtain a fiber patchcord, if required

Procedure 5-67 (continued)

Low Received Span Loss

Step	Action						
1	<p>CAUTION Risk of damage to modules</p>  <p>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.</p>						
2	<p>Add attenuator pads as needed until the Span Loss for the link is within the Span Loss Margin by at least 1 dB (hysteresis). Note that the alarm will clear when:</p> <p>Measured Span Loss > Minimum Span Loss - Span Loss Margin + 1 dB (hysteresis)</p> <p>Note: Fixed attenuators should be added to the patch panel or within a fiber storage tray and not on the optical interface circuit packs.</p>						
3	<table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; width: 40%;">If the original alarm has</th> <th style="text-align: left; width: 60%;">Then</th> </tr> </thead> <tbody> <tr> <td>cleared</td> <td>the procedure is complete</td> </tr> <tr> <td>not cleared</td> <td>go to step 4</td> </tr> </tbody> </table>	If the original alarm has	Then	cleared	the procedure is complete	not cleared	go to step 4
If the original alarm has	Then						
cleared	the procedure is complete						
not cleared	go to step 4						
4	<table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; width: 40%;">If</th> <th style="text-align: left; width: 60%;">Then go to</th> </tr> </thead> <tbody> <tr> <td>you want to clear the alarm (and disable detection) without addressing the fault</td> <td>step 5</td> </tr> <tr> <td>otherwise</td> <td>step 6</td> </tr> </tbody> </table>	If	Then go to	you want to clear the alarm (and disable detection) without addressing the fault	step 5	otherwise	step 6
If	Then go to						
you want to clear the alarm (and disable detection) without addressing the fault	step 5						
otherwise	step 6						
5	Provision the Minimum Span Loss to 0. Refer to the “Editing facility parameters” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.						
6	Contact your next level of support or your Ciena support group.						

—end—

Procedure 5-68

Low Voltage (DSM)

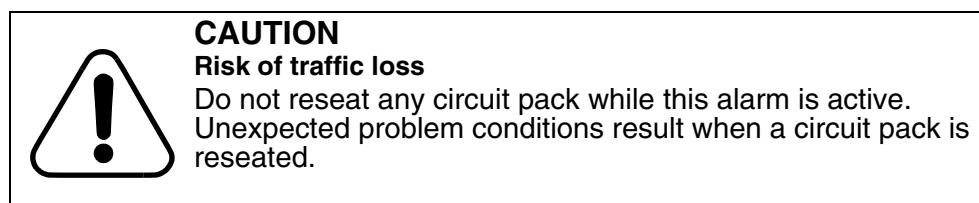
Alarm ID: 132

Probable cause

This alarm is raised when an active DS1 service module (DSM) detects the power input is above -38 V. The DSM enters or exits this brownout state regardless of the power status on the host shelf or on other DSMs attached to the shelf. When the DSM is in a brownout state it will not report any other alarms on the DSM to the shelf.

Impact

Critical, service-affecting (C, SA) alarm



Prerequisites

To perform this procedure, you must observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545.

Step	Action
1	<p>Verify the power supply to the DSM box raising the alarm. Use your company procedure to clear the power supply problem. This alarm is cleared when the DSM monitor input power is below -42 V.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> ATTENTION When the DSM detects that the input power has recovered to below -42 V, the DSM will automatically perform a cold restart on the slot 2 DSM 84xDS1 termination module (TM) and then the slot 1 DSM 84xDS1 TM. </div>
2	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-69

MAC Database Near Capacity

Alarm ID: 937

Probable cause

This alarm is raised against an L2SS or PDH gateway circuit pack forwarding database (FDB) when the FDB exceeds 95% of the maximum number of dynamic entries permissible.

Note: 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 excessive flooding, which can occur at 100% capacity.

Impact

Warning

Enabled by default

Step	Action
1	This is a network problem. Contact your network planning group. —end—

- 1 This is a network problem. Contact your network planning group.

—end—

Procedure 5-70 MAC Flapping Detected

Alarm ID: 938

Probable cause

This alarm is raised against an L2SS or PDH gateway circuit pack forwarding database (FDB) when a MAC address has been frequently learned on different ports. MAC flapping can indicate a network loop resulting from network misconfiguration.

Impact

Warning

Enabled by default

Prerequisites

To perform this procedure, you must

- have the network topology information
- use an account with at least a level 3 UPC

Step	Action
------	--------

- 1 Examine the network topology to identify and rectify the misconfiguration. As a temporary measure (until the misconfiguration is resolved), you can override each flapping MAC address with a static entry to prevent MAC flapping. Refer to the “Editing the nodal system parameters” procedure in *Administration and Security*, 323-1851-301.
- 2 If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-71

MAC Status Defect

Alarm ID: 1210

Probable cause

This alarm is raised against a Maintenance Association (MA) entity when a Maintenance End Point (MEP) receives a valid Continuity Check Message (CCM) in which it contains either an Interface Status “Type, Length, and Value” (TLV) reporting a state of anything other than “isUp” or a Port Status TLV from all known RMEP reports “psBlocked”.

This alarm indicates that the peer node is experiencing an issue.

Impact

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

Prerequisites

To perform this procedure, you must use an account with at least a level 3 UPC.

Step	Action
1	Verify the alarms and logs raised against the peer node. See the “Retrieving active alarms for one or more network elements in Part 1 of this document. Note: If there are multiple RMEPs, use the "RTRV-MEP-DEFECTS2" TL1 command (or) the 'Defects' tab in Ethernet OAM provisioning window in Site Manager to isolate the alarm condition against a specific RMEP.
2	Use the appropriate alarm clearing procedure in this document to clear the active alarm.
3	Retrieve alarms again and verify if the alarm has been cleared.
4	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-72

Manual Area Address Dropped from area

Alarm ID: 804

Probable cause

This alarm is raised when a provisioned manual area address is dropped from the computed area address set of the network. Each network element supports a maximum of three manual area addresses at one time. All network elements in the network share this information. Each network element independently calculates a set of computed area addresses from the union of all the manual area addresses provisioned on the network. The computed set is recalculated in the following situations:

- addition of a new network element to the network
- manual deletion or addition of an area address from any network element
- expiration of a local timer (maximum delay is every 10 to 15 minutes, and minimum delay is every few seconds)

This alarm can indicate a network-wide error condition in the provisioning of data communication. If an area address is dropped on a network element, isolation of the network element and a loss of OAM&P capability on the network element can occur.

Impact

Minor, non-service-affecting (m, NSA)
Enabled by default.

Prerequisites

To perform this procedure, you must have the network plan.

Step	Action
------	--------

Determine the manual area addresses provisioned in the network

- 1 To determine the manual area addresses provisioned in the network you must log into one of the network element in the system.
- 2 Query all area addresses. Refer to the “Retrieving communications settings” procedure in Part 1 of *Configuration - Provisioning and Operating*, 323-1851-310.
A list of up to three addresses appears.
- 3 Record the list of addresses in the computed set.

Procedure 5-72 (continued)

Manual Area Address Dropped from area

Step	Action
------	--------

Determine if the manual area addresses belong in the network

Note: Determine if the area addresses belong in the network by referring to the network plan.

4	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 5

Delete the manual area addresses that do not belong in the network

- 5 Log into the network element where the manual area address(es) that is not configured properly, is provisioned.
- 6 Delete the manual area address that does not belong in the network. Refer to the “Deleting an entry in the communications settings” procedure in Part 1 of *Configuration - Provisioning and Operating*, 323-1851-310.
- 7 Repeat [step 5](#) and [step 6](#) to delete each manual area address that is not configured properly.

—end—

Procedure 5-73

Mapping Mismatch

Alarm ID: 1378, 1778

Probable cause

The alarm point is identified at the G.709 level on the 40G OCI, 40G+ CFP OCI, provisioned with an OTM3 client, when the payload mapped in the G.709 signal at the upstream 40G OCI or 40G+ CFP OCI is not compatible with the expected one at the downstream 40G OCI or 40G+ CFP OCI circuit pack. The G.709 payload structure identifier (PSI) byte is used for this purpose. This condition can occur as a result of crossed fibers or as a result of incorrect provisioning. For example on a 40G OCI (NTK529SDE5), the near-end client facility is provisioned to be OTM3 and the far-end client facility is provisioned to be OC-768.

On the 40G+ CFP OCI (NTK529SJE5), OC768 or 40GE to OTU3 handoff mappings are supported. While the 40G+ CFP OCI can support handoff mappings to OTU3, it requires the payload of the OTU3 to include the correct payload type. If an OTU3 facility at one end of a link is connected to an OC768 facility at the far-end, the OPU3 feeding the OTU3 facility must contain an OC768 Bit synchronous CBR mapped as defined in G.709, PT = 03 hex. If an OTU3 facility at one end of a link is connected to a 40GE facility at the other end, the OPU3 must contain a 40GE signal GMP mapped, PT = 07 hex.

For the 40G+ CFP OCI, this alarm is raised:

- for any Payload Type (PT) received from the line side that is not defined for this circuit pack (for example, not = 8A, 8B, 89, 20)
- if OTM3 facility mapping is ODU Transparent and the PT received is different than the PT expected
- in the event of a mismatch between the PT received on the OTU3 client port and that received from the line side
- if the NTK529SJ is used at the near-end and the NTK525CF is used at the far-end and the NTK525CF ODU2 rate is not 10.7G

This alarm is also raised on the ODUCTP facility of a 40G OTN XCIF circuit pack when the far-end PT is unsupported (not = 0x89, 0x8B or 0x8A).

Procedure 5-73 (continued)

Mapping Mismatch**ATTENTION**

In a 40G client card back-to-back configuration when a 40G+ CFP OCI circuit pack (NTK529SJE5) is mated with a 40G MUX OCI circuit pack (NTK525CFE5 variant), a “Mapping Mismatch” alarm is raised on the OTU3 port of the 40G+ CFP OCI circuit pack when the 40G MUX OCI ODU2 rate is not 10.7G to help highlight that this is an unsupported configuration. See *WaveLogic Ai, Flex, 100G+, 40G, OSIC ISS, and SLIC10 Circuit Packs*, 323-1851-102.4, for details of the 40G client card back-to-back configuration.

Impact

Critical, service-affecting (C, SA) alarm, if on an active path
 Minor, non-service-affecting (m, NSA) alarm, if on an inactive path

Prerequisites

To perform this procedure, you must

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545
- have the optical fiber connection information (that is, how the modules on each network element connect to other network elements)
- have the provisioning information for the client type on the 40G OCI cards

Step	Action	
1	If the alarm is raised against a 40G OTN XCIF, 40G OCI or 40G+ CFP OCI circuit pack another circuit pack	Then go to step 2 step 3
2	Ensure that the 40G client circuit packs and associated 40G OCLD or Wavelength-Selective 40G OCLD circuit packs are connected properly.	

Procedure 5-73 (continued)

Mapping Mismatch

Step	Action				
3	Using connection records, determine the far-end module connected to the alarmed module. Retrieve the equipment and Facility Details for both the alarmed and remote module. Refer to the “Retrieving equipment and facility details” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310. A 40G OTN XCIF, 40G OCI, 40G+ CFP OCI/40G OCLD or Wavelength-Selective 40G OCLD pair must be connected to a 40G OTN XCIF, 40G OCI or 40G+ CFP OCI/40G OCLD or Wavelength-Selective 40G OCLD pair. From your company records, validate that the local client facility is supposed to be provisioned as an OTM3 or ODUCTP facility.				
4	If a handoff is provisioned between two 40G+ CFP OCI circuit packs, verify that the remote equipment feeding the OTU3 to one 40G+ CFP OCI circuit pack does not have an incorrect payload.				
5	Ensure that the corresponding client facility at the far-end is also provisioned as an OTM3 or ODUCTP facility.				
6	Delete and re-add the incorrect facility. Refer to the “Deleting a facility from an equipment” and “Adding a facility to an equipment” procedures in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.				
7	If the original alarm has Then <hr/> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">cleared</td> <td style="width: 70%;">the procedure is complete</td> </tr> <tr> <td>not cleared</td> <td>go to step 8</td> </tr> </table>	cleared	the procedure is complete	not cleared	go to step 8
cleared	the procedure is complete				
not cleared	go to step 8				
8	Ensure that no fibers are crossed. The OTU/ODU trail trace can be used to identify crossed fibers. If the OTU/ODU trail trace is provisioned, the “ ODU OTU Trace Identifier Mismatch ” alarm is raised to indicate crossed fibers. Refer to the “Retrieving and editing trail trace messages” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.				
9	If the original alarm has Then <hr/> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">cleared</td> <td style="width: 70%;">the procedure is complete</td> </tr> <tr> <td>not cleared</td> <td>go to step 10</td> </tr> </table>	cleared	the procedure is complete	not cleared	go to step 10
cleared	the procedure is complete				
not cleared	go to step 10				
10	If the alarm does not clear, contact your next level of support or your Ciena support group.				

—end—

Procedure 5-74

Max Stations Exceeded

Alarm ID: 812

Probable cause

This alarm is raised when the number of stations on the RPR exceed the maximum limit.

Impact

Major, service-affecting (M, SA) alarm

Enabled by default.

Prerequisites

To perform this procedure, you require an account with at least a level 3 UPC.

Step	Action
1	Verify the number of stations on the ring and compare it to the MAX_STATION number. Refer to the “Viewing information for resilient packet rings” procedure in Part 2 of <i>Configuration - Bandwidth and Data Services</i> , 323-1851-320.
2	Remove one or more RPR stations from the Resilient Packet Ring until the number of stations is equal or less than the maximum allowed. Refer to the “Deleting a resilient packet ring” procedure in Part 2 of <i>Configuration - Bandwidth and Data Services</i> , 323-1851-320.
3	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-75 Member Release Misaligned

Alarm ID: 1685

Probable cause

This alarm is raised to identify a member shelf that is running a different release than the primary shelf.

Impact

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

Prerequisites

Before you perform this procedure, you must:

- use an account with at least a level 3 UPC
- have the IP address of all shelves within the consolidated TID
- have a network plan, or other documentation identifying all shelf provisioning information, including shelf function

Step	Action
------	--------

Note: If a TIDc site is upgraded (First Invoke) shelf by shelf and the First Invoke is issued on member shelves prior to the primary shelf, this alarm is raised for all member shelves. In these cases, this alarm can be ignored.

- 1 Upgrade the member shelf to a software version supported by the primary shelf. Refer to the “Software Upgrade Procedures” section in *Planning - Ordering Information*, 323-1851-151.
- 2 If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-76

Member Shelf Mismatch

Alarm ID: 718

Probable cause

This alarm is raised on the primary shelf of a consolidated node when the member shelf's **Function provisioned** parameter seen by the primary shelf does not match the **Function actual** parameter of the member shelf. This alarm is masked by the Member Shelf Unreachable alarm.

When a member shelf is auto-enrolled into a consolidated node, the member's **Function provisioned** parameter set on the primary is equal to the **Function actual** parameter of the member shelf.

When a member shelf is manually added to a consolidated node, the **Function provisioned** parameter is provisioned in the **Node Information** application. Refer to the "Displaying member shelf information of a consolidated node" procedure in *Administration and Security*, 323-1851-301.

Impact

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

Prerequisites

Before you perform this procedure, you must:

- use an account with at least a level 3 UPC
- have the IP address of all shelves within the consolidated TID
- have a network plan, or other documentation identifying all shelf provisioning information, including shelf function

Step	Action
1	Log into the primary shelf raising the alarm.
2	Verify that each member shelf's Function provisioned parameter detected by the primary shelf matches the corresponding Function actual parameter of the member shelf. The Secondary state parameter for the mismatched member shelf indicates "MEA". Refer to the "Displaying member shelf information of a consolidated node" procedure in <i>Administration and Security</i> , 323-1851-301.
3	After identifying the member shelf with the mismatched Function provisioned parameter, Record all the provisioning information required to re-add the incorrectly provisioned member shelf to the consolidated node.

Procedure 5-76 (continued)

Member Shelf Mismatch

Step	Action
4	Delete the member shelf from the consolidated node.
5	Refer to the network plan, and re-add the member shelf to the consolidated node with the correct Function provisioned . Refer to the “Adding a shelf to a consolidated node” procedure in <i>Administration and Security</i> , 323-1851-301.
6	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-77

Member Shelf Unknown

Alarm ID: 719

Probable cause

This alarm is raised on the primary shelf of a consolidated node during the addition of a member shelf when a member shelf does not respond to messages from the primary shelf related to the addition. Low level communication between the shelves is still available.

Communication between a primary and member shelf can be interrupted when:

- a duplicate primary shelf exists. The Member Shelf Unknown alarm is raised on the primary shelf, which attempted to communicate with a member shelf that is already associated with another primary shelf.
- the member shelf is running a software version that is unsupported by the primary shelf
- the member shelf is provisioned with a provisioned function that is unsupported by the primary shelf

Note: If a primary or member shelf is restarted, the Member Shelf Unknown alarm is briefly raised.

Impact

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

Prerequisites

To perform this procedure, you must:

- use an account with at least a level 3 UPC
- have the IP address of all shelves within the consolidated node
- have an available network plan, or other documentation identifying all shelf provisioning information, including upgrade plans

Step	Action
------	--------

- 1 Clear any Duplicate Primary Shelf alarms present. Refer to the “Duplicate Primary Shelf” alarm clearing procedure in Part 1 of this document.
- 2 Log into the primary shelf.

Procedure 5-77 (continued)

Member Shelf Unknown

Step	Action						
3	<p>Identify which shelf/shelves is/are causing the alarm.</p> <p>The Secondary state parameter for the unreachable member shelf indicates “MEA”. The affected shelf/shelves may have ‘?’ next to the shelf number and be highlighted in cyan. Refer to the “Displaying member shelf information of a consolidated node” in <i>Administration and Security</i>, 323-1851-301. Verify the node information is synchronized and/or supported by the primary shelf.</p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 60%; vertical-align: top; padding-right: 10px;">If the member shelf has a</td> <td style="width: 40%; vertical-align: top; text-align: right;">Then go to</td> </tr> <tr> <td>Software version unsupported by the primary shelf</td> <td style="text-align: right;">step 4</td> </tr> <tr> <td>Function provisioned unsupported by the primary shelf</td> <td style="text-align: right;">step 5</td> </tr> </table>	If the member shelf has a	Then go to	Software version unsupported by the primary shelf	step 4	Function provisioned unsupported by the primary shelf	step 5
If the member shelf has a	Then go to						
Software version unsupported by the primary shelf	step 4						
Function provisioned unsupported by the primary shelf	step 5						
4	<div style="border: 1px solid black; padding: 10px; width: fit-content; margin: auto;"> <p>CAUTION</p>  <p>Risk of communication loss</p> <p>Failure to synchronize the software release can result in commands not being recognized or interpreted properly by the software system, which may affect management or communications to that member shelf.</p> </div> <p>Upgrade the member shelf to a software version supported by the primary shelf. Refer to the “<i>Software Upgrade Procedures</i>” section in <i>Planning - Ordering Information</i>, 323-1851-151.</p> <p>Go to step 7.</p>						
5	<div style="border: 1px solid black; padding: 10px; width: fit-content; margin: auto;"> <p>CAUTION</p>  <p>Risk of loss of functionality</p> <p>Traffic and data communications will be lost</p> <p>Decommissioning a shelf results in a loss of all traffic and data communications associated with the shelf that is being decommissioned.</p> </div>						
6	<p>Record all of the provisioning information required to recommission the shelf. Decommission the shelf and re-add it with the correct Function provisioned. Refer to the “Deleting all shelf provisioning” procedure in <i>Administration and Security</i>, 323-1851-301.</p>						
7	<p>If the alarm does not clear, contact your next level of support or your Ciena support group.</p>						

—end—

Procedure 5-78

Member Shelf Unreachable

Alarm ID: 717

Probable cause

This alarm is raised on a primary shelf of a consolidated node when the primary shelf cannot communicate with one or more member shelves. This can occur when the member shelf has an incorrect IP address provisioned.

Note: When a member shelf is restarted, the Member Shelf Unreachable alarm is raised for the duration of the member restart. When a primary shelf is restarted, the Member Shelf Unreachable alarm is raised briefly.

Impact

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

Prerequisites

To perform this procedure, you must:

- use an account with at least a level 3 UPC
- have a valid primary shelf provisioned for the consolidated node
- have the IP address of all shelves within the consolidated node
- have an available network plan, or other documentation identifying shelf provisioning within the consolidated node

Step	Action
1	Clear any Primary Shelf Unreachable alarm present. Refer to Procedure 5-140, "Primary Shelf Unreachable" alarm procedure.
2	Log into the primary shelf raising the alarm.
3	Retrieve the Node Information table for the consolidated node. Refer to the "Displaying member shelf information of a consolidated node" in <i>Administration and Security</i> , 323-1851-301.
4	Identify which shelf/shelves is/are causing the alarm.

The **Secondary state** parameter for the unreachable member shelf indicates "UNEQ". The affected shelf/shelves may have '(?)' next to the shelf number and be highlighted in cyan. Refer to the "Displaying member shelf information of a consolidated node" procedure in *Administration and Security*, 323-1851-301.

Procedure 5-78 (continued)

Member Shelf Unreachable

Step	Action
5	<p>If within the consolidated node</p> <p>only one shelf displays a fault</p> <p>all shelves display the same fault</p> <p>Then the issue is with</p> <p>that member shelf. Go to step 6.</p> <p>the primary shelf. Go to step 7.</p>
6	<p>Log in directly into the affected member shelf, and ensure all provisioning required for the member shelf of a consolidated node to operate is correct and without issue. Direct shelf access may be required. Refer to the “Consolidated node (TIDc)” section and the “Logging into a network element using a direct network connection to the LAN port on the shelf processor” procedure in <i>Administration and Security</i>, 323-1851-301, for more information.</p> <p>For example, verify and if necessary correct:</p> <ul style="list-style-type: none">• Primary state of member shelf• IP address provisioning• IP route provisioning• OAM communication• LAN/ILAN port status• OSPF provisioning• consolidated node parameter provisioning• Software release and upgrade state is applicable <p>Refer to the “Displaying member shelf information of a consolidated node” procedure in <i>Administration and Security</i>, 323-1851-301, and the “Retrieving communications settings” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i>, 323-1851-310. If the alarm does not clear, go to step 7.</p>

Procedure 5-78 (continued)
Member Shelf Unreachable

Step	Action
7	<p>Ensure all provisioning required for the primary shelf of a consolidated node to operate is correct and without issue.</p> <p>For example, verify and if necessary correct:</p> <ul style="list-style-type: none">• Primary state of primary shelf• IP address provisioning• IP route provisioning• OAM communication• LAN/ILAN port status• OSPF provisioning• consolidated node parameter provisioning• Software release and upgrade state is applicable <p>Refer to the “Displaying member shelf information of a consolidated node” procedures in <i>Administration and Security</i>, 323-1851-301, and the “Retrieving communications settings” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i>, 323-1851-310.</p>
8	<p>If the alarm does not clear, contact your next level of support or your Ciena support group.</p>

—end—

Procedure 5-79 Minimum Gain

Alarm ID: 1583

Probable cause

This alarm is raised when an amplifier is at its minimum extended range gain setting and the peak channel power overshoots the provisioned peak power target by 2 dB due to one of the following:

- the actual span loss is less than designed value
- wrong pad/DCSM placement at the amplifier site or upstream sites
- faulty pads which results in incorrect padding value (for example, faulty 10 dB pad only yields 5 dB attenuation)
- improper provisioning of the amplifier or upstream amplifier peak power targets (TARGPKPOW)
- the MLA2v or RLA 5x1 VOA has not been optimized by DOC or has not been provisioned properly if manual provisioning is being used
- upstream DOC faults

Note: DOC checks for the Minimum Gain condition on each Auto Monitor cycle.

ATTENTION

There may be Minimum Gain alarms present at other line amplifiers on the link. Minimum Gain alarms do not mask downstream Minimum Gain alarms.

Impact

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

Prerequisites

To perform this procedure, you must:

- use an account with at least a level 3 UPC
- have a valid primary shelf provisioned for the consolidated node
- have the IP address of all shelves within the consolidated node
- have an available network plan, or other documentation identifying shelf provisioning within the consolidated node

Procedure 5-79 (continued)

Minimum Gain

Step	Action
1	If there are more than one Minimum Gain alarms in the span, begin troubleshooting upstream of the first amplifier with the alarm.
2	Check if upstream DOCs have faults. If so, troubleshoot the upstream DOC faults first.
3	Check if the equipment is deployed according to network design (for example, the design requires an MLA, but an MLA2 was deployed). Make sure the correct equipment is used.
4	Check if the Peak Power Target is provisioned as designed. If not, correct it. Refer to the “Provisioning photonic parameters” and “Provisioning adjacencies” procedures in the <i>Commissioning and Testing</i> , 323-1851-221.
5	For line facing amplifiers, check if the actual span loss (measured OSC span loss includes the pads and DSCMs placed on the line) is less than the design value. If it is less, pad the span to the designed value. Refer to the “Retrieving equipment and facility details” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
6	If there is an MLA2v amp upstream, reset the VOA on the MLA2v.
7	Check if the pads and DSCMs are deployed in the designed places. If not, correct them.
8	If the alarm does not clear, replace the pads.
9	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-80

Modem Class Mismatch

Alarm IDs: 2023

Probable cause

This alarm is raised on the PTP facility of the WLAI circuit pack when line port detects mismatch of modem class between the two ends of the link.

Modem class is used to allow the user to provision the appropriate license type for Submarine or Terrestrial applications on WLAI line port. Modem class license is released when WLAI line port is deleted.

Impact

Critical, service-affecting (C, SA) alarm if not protected
Minor, non-service-affecting (m, NSA) alarm if protected

Prerequisites

To perform this procedure, you must use an account with at least a level 3 UPC

Step	Action
1	Verify the Modem class at each side of the link to be the same. Refer to “Retrieving equipment and facility details” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
2	If they are different, re-provision the WLAI line port PTP to make sure the Modem Class are the same on both ends of the link. Refer to “Editing facility parameters” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.

—end—

Procedure 5-81

MSI Mismatch (ODUTTP, ODUCTP, OTM0, OTM1, OTM2, OTM3, ODU0, ODU1, ODUFLEX, OTMFLEX)

Alarm ID: 1475, 1584, 1607, 1733, 1739, 1848

Probable cause

For OTM facilities, this alarm is raised on the client mapping layer when the client has a cross connection to an OTM port. This can be caused by:

- incorrect MSI received for the service provisioned
- incorrect BW for the Service ID
- no connection or “msi=unused” received for a service provisioned on this client port

For ODUTTP and ODUCTP facilities, this alarm is raised when the Rx interface detects no MSI is provisioned for the ODUTTP or ODUCTP. This could be caused when a far-end ODUTTP or ODUCTP is not provisioned yet or is provisioned but has a different tribPort than the local ODUTTP or ODUCTP. The tribPort for an ODUTTP or ODUCTP must be the same at both ends of the network.

This alarm is not applicable to ODUTTP/ODUCTP facilities on the OTN I/F Flex 16xSFP (NTK622AA) circuit pack.

For the (1+8)xOTN Flex MOTR (NTK532DA, NTK532DE) circuit pack, this alarm is raised when the expected Rx MSI does not match the actual Rx MSI for the corresponding facility (when the tributary slot assignment is in manual mode). In this case, conditioning is also applied in the off-ramp direction for the corresponding connection.

When the tributary slot assignment is in automatic mode, the alarm is raised against the ODU connection if the correct number of tributary port number and ODU payload type (ODTU type) cannot be found in the incoming OPU2 payload. In this case, you only have to specify the tributary port number for each ODU connection. All other relevant attributes are either derived or retrieved from the system.

The alarm is also raised when the Tributary Slot Provisioning parameter is provisioned to MANUAL and at least one Rx tribSlot matches the expected Rx tribPort, but at least one other Rx tribSlot doesn't match what is expected.

For the 100G (2xQSFP+/2xSFP+) MUX circuit pack, this alarm is raised when one end is provisioned with a 4x10G ETH facility and the other end is provisioned with a 40G ETH facility.

Procedure 5-81 (continued)

MSI Mismatch (ODUTTP, ODUCTP, OTM0, OTM1, OTM2, OTM3, ODU0, ODU1, ODUFLEX, OTMFLEX)

Impact

Critical, service-affecting (C, SA) alarm

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

Prerequisites

To perform this procedure, you require an account with at least a level 3 UPC.

Step	Action
1	Identify the port where this alarm is being raised. Identify the OTM, ODU, ODUTTP, or ODUCTP port to which it is currently connected.
2	Identify all the connections to the OTM, ODU, ODUTTP or ODUCTP port.
3	If the original alarm is raised against an Then go to
	OTM or ODU facility step 4
	ODUTTP or ODUCTP facility step 14
4	Choose one connection and identify its payload index.
5	At both ends of this fiber:
	<ul style="list-style-type: none">Verify that the payload index used for the ODU0, ODU1, ODUFLEX connection to the OTM facility is the same at both the near-end and far-end. If it is not, then change one end.If the identified far-end is an OTM to OTM facility connection, verify that the connection rate (for example, ODU0, ODU1, ODUFLEX) for this payload index is the same at this site and the near-end site. If the connection rate is different at each end then correct the connection provisioning at the OTM to OTM or ODU to ODU connection site.
6	If the original alarm has
	Then
	cleared the procedure is complete
	not cleared go to step 7
7	If the connection rate is the same at each end, then identify the OTM port at the site upstream from this one and go to step 5 .
8	If the identified far-end is a OTM to FLEX or OTM1 facility connection, verify that the connection rate (for example, ODU0, ODU1, or ODUFLEX) with the payload index is the same at both ends of the fiber.

Procedure 5-81 (continued)

MSI Mismatch (ODUTTP, ODUCTP, OTM0, OTM1, OTM2, OTM3, ODU0, ODU1, ODUFLEX, OTMFLEX)

—end—

Procedure 5-82 **Multiplexed Rate Mismatch**

Alarm ID: 1031

Probable cause

This alarm is raised against:

- an OTM2 facility of a 40G MUX OCI, 100G (2xQSFP+/2xSFP+) MUX, 200G (2x100G/5x40G) MUX, or 10x10G MUX circuit pack when a rate mismatch is detected between the local OTM2 facility and the OTM2 demultiplexed from the OTM3 or OTM4 facility. This occurs when the OTM2 rate of the 10G client provisioning at the near-end 40G MUX OCI, 100G (2xQSFP+/2xSFP+) MUX, 200G (2x100G/5x40G) MUX, or 10x10G MUX does not match the OTM2 rate of the 10G client provisioning of the same port at the far-end 40G MUX OCI, 100G (2xQSFP+/2xSFP+) MUX, 200G (2x100G/5x40G) MUX, or 10x10G MUX OCI.
 - a 40G XCIF OTM2 facility when the OTU2 rate received from the backplane side does not match the expected backplane OTU2 rate.

Impact

Critical, service-affecting (C, SA) alarm

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

Prerequisites

To perform this procedure, you require an account with at least a level 3 UPC.

Step	Action
1	Identify the OTM2 facility raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document.
2	Verify if there is a difference between the Received rate from OTM2 and the Expected rate from OTM2 values in the OTM Info dialog box. Refer to the “Retrieving OTM info” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
3	If the values Then
	match contact your next level of support or Ciena support group. The procedure is complete.
	do not match go to step 4
4	Determine if it is the Received rate from OTM2 or the Expected rate from OTM2 value that is incorrect.

Procedure 5-82 (continued)
Multiplexed Rate Mismatch

Step	Action	
5	If the incorrect value is the Expected rate from OTM3/ OTM4	Then delete and reprovision the local OTM2 client facility to the correct rate. Refresh the OTM Info dialog box to verify the correct Expected rate from OTM2 value is displayed. Refer to the “Retrieving OTM info” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
6	Received rate from the OTM3/ OTM4	delete and reprovision the far-end OTM2 client facility to the correct rate. Refresh the OTM Info dialog box to verify the correct Received rate from OTM2 value is displayed. Refer to the “Retrieving OTM info” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
	If the alarm does not clear, contact your next level of support or your Ciena support group.	

—end—

Procedure 5-83

NE Mode Unknown

Alarm ID: 530

Probable cause

This alarm is raised when the network element mode has not been set and is unknown. The alarm is cleared when the user sets the network element mode during the commissioning process.

For Broadband services, this alarm can also be raised after a shelf processor replacement.

Before the shelf can be fully provisioned, the **NE mode** must be changed to SONET, SDH or SDH-J, as appropriate:

- for MSPP services, the mode can either be SONET, SDH or SDH-J
- for MSPP and Broadband services, the mode can either be SONET or SDH
- for Broadband services, the mode can either be SONET or SDH
- for converged Broadband and Photonic services, the mode can either be SONET or SDH
- for Photonic services, (even though the mode is not relevant to Photonics) the mode can either be SONET or SDH

Impact

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

Prerequisites

To perform this procedure, you require an account with at least a level 3 UPC.

Step	Action
1	Provision the network element mode. Refer to the “Editing the nodal general parameters” procedure in <i>Administration and Security</i> , 323-1851-301.
2	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-84

Network Trace Identifier Mismatch (FLEX)

Alarm IDs: 1244

Probable cause

This alarm is raised against a FLEX facility when the incoming and expected Network Trace values are different.

For a FLEX MOTR circuit pack, this alarm will result in the client port being conditioned with the user defined signal and RDI to be sent to the far-end of the connection.

This alarm can also be raised on the FLEX MOTR (NTK531YAE5) circuit pack when a fiber loopback is present on the 10G line port at the local node or when a facility loopback is performed on the 10G line port at the remote node.

Impact

Major, non-service-affecting (M, SA) alarm

Prerequisites

To perform this procedure, you must

- have the optical fiber connection information (that is, how the modules on each network element connect to other network elements)
- use an account with at least a level 3 UPC

Step	Action
1	Verify if there are alarms of higher order from the alarm hierarchy. Refer to the “Alarm hierarchies and alarm severities” chapter in Part 1 of this document.
2	Clear any alarms of higher order using the appropriate procedures.
3	If the original alarm has Then
	cleared the procedure is complete
	not cleared go to step 4
4	Identify the circuit pack raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document.
5	Use the optical fiber connection information to identify the near-end and far-end ports of the port trace.

Procedure 5-84 (continued)

Network Trace Identifier Mismatch (FLEX)

Step	Action
6	For a FLEX facility, retrieve and record the network trace messages at both ends. Refer to the “Retrieving equipment and facility details” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
7	Ensure that network trace is provisioned correctly at each network element. Ensure that the outgoing network trace string (Transmitted) at the transmit end matches the incoming expected network trace string (Expected Rx) at the receive end. Refer to the “Adding a facility to an equipment” procedure, “Editing facility parameters” procedure, and the “FLEX facility parameters for FLEX MOTR, 8xOTN Flex MOTR, and (1+8)xOTN Flex MOTR” table in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
8	If this alarm is present on the Flex MOTR 8xSFP, 2xXFP (NTK531YAE5) circuit pack, then ensure that there are no fiber loopbacks on the 10G line ports at the local node and that there are no facility loopbacks on the 10G line ports at the remote node.
9	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-85

Node ID Mismatch

Alarm IDs: 324, 527, 1128

Probable cause

This alarm is raised when:

- the source and destination node IDs are not a neighboring pair according to the provisioned 2-Fiber/4-Fiber BLSR/MS-SPRing/HERS configuration on the OC-48/STM-16 or OC-192/STM-64 circuit pack
- the node ID does not match any other entry in the 2-Fiber/4-Fiber BLSR/MS-SPRing/HERS configuration
- a network element detects a message sent by another network element that is not identified as a neighbor according to the locally stored 2-Fiber/4-Fiber BLSR/MS-SPRing/HERS configuration
- an invalid 2-Fiber/4-Fiber BLSR/MS-SPRing/HERS configuration
- an incorrect fiber-optic cable connection

Impact

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

Prerequisites

To perform this procedure, you must

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545
- have an antistatic wrist strap to dissipate electrostatic charges
- use an account with at least a level 3 UPC

Step	Action
1	Identify the circuit pack raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document. The circuit pack raising the alarm is the receiving network element.
2	Verify the 2-Fiber/4-Fiber BLSR/MS-SPRing/HERS provisioning at each node. Correct any 2-Fiber/4-Fiber BLSR/MS-SPRing/HERS provisioning errors. Refer to the “Editing a BLSR/MS-SPRing/HERS configuration for a node” procedure in Part 1 of <i>Configuration - Bandwidth and Data Services</i> , 323-1851-320.

-
- | | |
|---|--|
| 1 | Identify the circuit pack raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document. The circuit pack raising the alarm is the receiving network element. |
| 2 | Verify the 2-Fiber/4-Fiber BLSR/MS-SPRing/HERS provisioning at each node. Correct any 2-Fiber/4-Fiber BLSR/MS-SPRing/HERS provisioning errors. Refer to the “Editing a BLSR/MS-SPRing/HERS configuration for a node” procedure in Part 1 of <i>Configuration - Bandwidth and Data Services</i> , 323-1851-320. |

5-218 Alarm clearing procedures—I to Z

Procedure 5-85 (continued)

Node ID Mismatch

Step	Action
3	If the original alarm has cleared Then the procedure is complete
	not cleared go to step 4
4	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
5	Replace the local OC-48/STM-16 or OC-192/STM-64 circuit pack. Refer to the “Replacing an optical interface circuit pack” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.
6	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-86 SP SP Number of Level 1 NEs Exceeded

Alarm ID: 805

Probable cause

This alarm is raised when the number of network elements supported in the data communication channel (GCC/DCC) domain exceeds the maximum supported. The maximum number of network elements supported in the GCC/DCC domain is 150. This alarm applies only when iISIS is provisioned on the GCC/DCC channels.

Impact

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

Step	Action
------	--------

- | | |
|---|---|
| 1 | Re-engineer the network to reduce the number of network elements in the Level 1 routing area. |
| 2 | If the alarm does not clear, contact your next level of support or your Ciena support group. |

—end—

Procedure 5-87

OAM Not Available

Alarm ID: 18

Probable cause

This alarm is raised when neither direct connection between the host shelf and a DSM 84xDS1 termination module (TM) exists, nor indirect connection (through the mate DSM 84xDS1 TM). The following common examples illustrate cases when this alarm is raised:

- In an unprotected system, a fiber is cut between a DSM 84xDS1 TM and its host OC-3.
- In a protected system, both fibers are cut between a DSM 84xDS1 TM and their host OC-3 cards.
- In an unprotected system, the host OC-3 circuit pack experience any type of restart.
- In a protected system, both host OC-3 circuit packs experience a cold restart.
- The fiber link may be intact, but SDCC is not functioning because of a circuit pack failure or mismatch.
- A host OC-3 experiences an SDCC failure.
- In a protected system, one of the host OC-3 or a DSM 84xDS1 TM is misconnected. For example, it is connected to another network element or to a different DSM 84xDS1 TM.

ATTENTION

Following a restart, the likelihood of OAM Not Available alarms being raised is high. If the alarm is raised following a restart, allow five to six minutes for the condition to clear prior to troubleshooting the alarm.

Loss of an OAM link to a provisioned DSM 84xDS1 TM while the OAM link of the mate remains intact masks all alarms against the circuit pack except the Circuit Pack Missing alarm. A Circuit Pack Missing alarm against a DSM 84xDS1 TM masks this alarm provided it has a mate with an OAM link (the mate informs the shelf processor that the circuit pack is missing).

During the second invoke of an upgrade process, the DSM 84xDS1 module restarts and the “OAM Not Available” alarm will rise. The DSM 84xDS1 module will not be visible in Shelf Inventory and the Slot Upgrade tab until the DSM 84xDS1 module restart completes. The alarm clears when the DSM 84xDS1 module restart is completed.

Procedure 5-87 (continued)

OAM Not Available**Impact**

Critical, service-affecting (C, SA) alarm, if carrying traffic
 Minor, non-service-affecting (m, NSA) alarm, if carrying no traffic

Prerequisites

To perform this procedure, you must

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545
- have an antistatic wrist strap to dissipate electrostatic charges
- use an account with at least a level 3 UPC

Step Action

- 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 host OC-3 circuit pack and DSM 84xDS1 TM raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document.
- 3 If the shelf processor, OC-3 circuit pack, or DSM 84xDS1 TM have been replaced or have undergone a restart, wait at least seven minutes for the discovery process to complete.
- 4 Retrieve alarms and look for an OC-n/STM-n Rx Loss Of Signal (C, SA) alarm or SDCC link failure alarm on the host OC-3. The presence of these alarms indicate a fiber cut.
- 5 If the fibers have been cut, replace the fibers. If the fibers are not linked, connect them as required.
- 6 If this is a protected scenario and the alarm has not cleared, verify that the provisioned OC-n/STM-n line facilities in both the working and mate host slots are linked by fiber to the OC-n/STM-n line facilities of the appropriate DSM 84xDS1 TM. Ensure there is no misconnection.
- 7 If this is an unprotected scenario and the alarm has not cleared, verify that the provisioned OC-n/STM-n line facilities in the host slot are linked by fiber to the OC-n/STM-n line facilities of the appropriate DSM 84xDS1 TM. Ensure there is no misconnection.
- 8 Ensure there is SDCC on the host OC-3 circuit packs. Refer to the “Retrieving communications settings” procedure in Part 1 of *Configuration - Provisioning and Operating*, 323-1851-310. If not, create a SDCC on the host OC-3. Refer to the “Adding a new entry in the communications settings” procedure in Part 1 of *Configuration - Provisioning and Operating*, 323-1851-310.

Procedure 5-87 (continued)

OAM Not Available

Step	Action
9	Verify the LEDs on the circuit packs to ensure none are failed. If one or both circuit packs have failed, replace the circuit pack. Refer to the “Replacing the DSM 84xDS1 TM circuit pack” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.
10	If the alarm does not clear, restart the DSM 84xDS1 TM in slot 1. If the alarm does not clear, restart the protection DSM 84xDS1 TM in slot 2.
11	If the alarm does not clear, restart the host OC-3 connected to the DSM 84xDS1 TM in slot 1. If the alarm does not clear, restart the host OC-3 connected to the DSM 84xDS1 TM in slot 2.
12	Select Shelf Inventory from the Configuration menu to verify the existence of an OAM link to a DSM 84xDS1 TM in the Inventory window.
13	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-88

OCH Link Data Retrieval In Progress

Alarm IDs: 1529

Probable cause

This event is raised when there is a Link Data retrieval session in progress.

Impact

Warning

Step	Action
------	--------

- 1 No action is required. The alarm clears once the retrieval session is complete.
- 2 If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-89

OCH Link Data Save In Progress

Alarm IDs: 1530

Probable cause

This event is raised when there is a Link Data save in progress.

Impact

Warning

Step	Action
------	--------

- 1 No action is required. The event clears once the save session is complete.
- 2 If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-90 ODU LCK

Alarm IDs: 962, 994, 1162, 1470, 1481, 1482, 1497, 1498, 1610, 1731

Probable cause

This alarm is raised when the Rx interface detects an ODU layer (path monitoring) LCK (locked). The upstream Tx interface is sending ODU layer LCK. This can occur when the upstream OTM1 (for OTN Flex MOTR circuit packs), facility is in the OOS state.

Impact

Critical, service-affecting (C, SA) alarm

Major, service-affecting (M, SA) alarm

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

Step	Action
1	Verify if any upstream facilities are Out Of Service.
2	If the facilities are supposed to be In Service and are OOS, place them In-Service. Placing the facilities In Service will clear the alarm.
3	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-91

ODU Loss of Frame and Multiframe

Alarm IDs: 1474, 1489, 1490, 1734

Probable cause

This alarm is raised when there is a mismatch in the configuration of the equipment at the near end and far end of the network.

Impact

Critical, service-affecting (C, SA) alarm

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

Step	Action
1	Verify if the ODU services are provisioned for the same rate at both ends of the network and correct the rate accordingly. For example you cannot have a service provisioned for an ODU2 at one end and an ODU2e at the other end, or an ODU Flex at one end and a different ODU rate at the other end. Refer to the “Retrieving equipment and facility details” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
2	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-92

ODU OCI

Alarm IDs: 963, 995, 1163, 1471, 1485, 1486, 1499, 1500, 1609, 1732

Probable cause

This alarm is raised when the Rx interface detects that there is a cross-connection missing along the connection path for this service. The upstream Tx interface is sending ODU layer OCI. This can occur when the upstream, ODUCTP, ODU0, ODU1, ODUFLEX, TCM, OTM0, OTM1, facility is not connected.

This alarm can also be raised when proper payload index assignment is not used for circuit packs that interwork with the 2.5G MOTR circuit packs (NTK530NAE5 and NTK530NCE5). For more information about proper payload index assignment when interworking with these circuit packs, refer to the Part 1 of *Configuration - Bandwidth and Data Services*, 323-1851-320.

Impact

- Minor, non-service-affecting (m, NSA) alarm
- Major, service-affecting (M, SA) alarm
- Critical, service-affecting (C, SA) alarm

The L2 MOTR will raise a Minor, non-service-affecting alarm on the OTM2 line port if no L2 VCE or EVPL connection is configured on the 10GE child facility of the OTM2 line port.

Step	Action
1	Ensure that there are cross-connects provisioned at every piece of equipment along the path.
2	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-93

ODU Skew Out Of Range

Alarm ID: 1948

Probable cause

This alarm is raised against the OTM3 facility of a 200G (2x100G/5x40G) MUX (NTK529HA) circuit pack when the system detects that the virtual lane skew exceeds the specified skew range from G.798.

Impact

Critical, service-affecting (C, SA) alarm, unprotected
Minor, non-service-affecting (m, NSA) alarm, protected

Prerequisites

To perform this procedure, you must:

- observe all safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545
- have the fiber connection information (that is, how the optical modules on each network element connect to other network elements)
- if required, obtain the replacement fiber for connection between the subtending equipment and the QSFP28
- if required, obtain a replacement QSFP28 module
- use an account with at least a level 3 UPC

Step	Action
1	Determine the type of the connection fiber between the subtending equipment and the QSFP28 module based on QSFP28 type.
2	If the fiber type is Then go to
	SMF step 3
	MMF step 8
3	Ensure the Integrated Test Feature (ITS) is available on the 200G (2x100G/5x40G) MUX and operating in Test Set mode. Refer to the “Performing a test with the Integrated Test Set” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.

Procedure 5-93 (continued)
ODU Skew Out Of Range

Step	Action
4	Ensure the Rx/Tx port on the QSFP28 is fiber loop backed using a patch cord fiber.
5	If the alarm does not clear, replace the QSFP28. Refer to the “Replacing a Pluggable module” in the <i>Fault Management - Module Replacement</i> , 323-1851-545.
6	If the original alarm has cleared, then restore the original configuration and the procedure is complete. Otherwise, go to step 7 .
7	If the original alarm does not clear, it indicates the problem is caused by subtending equipment. Troubleshoot the subtending equipment. Go to step 14 .
8	Ensure that all parallel fibers connected between the subtending equipment and QSFP28 have the same length. If not, then replace them to make them comply with this requirement.
9	If the original alarm does not clear, ensure the Integrated Test Feature (ITS) is available on the 200G (2x100G/5x40G) MUX OCI circuit pack and operating in Test Set mode.
10	Ensure the Rx/Tx port on the QSFP28 is fiber loop backed using a special MPO24 loopback fiber.
11	If the alarm does not clear, replace the QSFP28. Refer to the “Replacing a Pluggable module” in the <i>Fault Management - Module Replacement</i> , 323-1851-545.
12	If the original alarm has cleared, then restore the original configuration with the new QSFP28 and the procedure is complete. Otherwise, go to step 13 .
13	If the original alarm does not clear, it indicates the problem is caused by subtending equipment. Troubleshoot the subtending equipment.
14	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-94 ODU Signal Degrade

Alarm ID: 1476, 1491, 1492, 1503, 1504, 1611, 1762, 1781, 1787, 1863

Probable cause

This alarm is raised when the Rx interface detects an ODU layer signal degrade.

For ODU port types on eMOTR in Layer 2 Extended mode and PKT/OTN S-series circuit packs crossing the Signal Degrade threshold could be configured to trigger a switchover within an MPLS/MPLS-TP network. For details refer to *SAOS-based Packet Services Configuration*, 323-1851-630.

For 6500 Release 10.05 and higher, a Signal Degrade on a line port triggers a switch in TPT and SNCP Protection configurations for 4x10G OTR (NTK530QA, NTK530QM) and 1+8xOTN Flex MOTR (NTK532DA, NTK532DE) circuit packs. A Signal Degrade on the client ports only triggers an alarm (no protection switch occurs). The ODU Signal Degrade threshold is fixed at 10E-9 or 10E-8.

Impact

Major, service-affecting (M, SA) alarm

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

Critical, service-affecting (C, SA) alarm

The alarm will become Critical, service-affecting if:

- a single VCE has been configured on the VCS
- the L2 VCE or EVPL is configured only at one end (the end that has the L2 VCE or EVPL connection) of the OTM2 line
- the L2 VCE endpoint map has not been configured on both 10GE child facilities of the OTM2 line

Procedure 5-94 (continued)

ODU Signal Degrade**Prerequisites**

To perform this procedure, you must

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0
- have an antistatic wrist strap to dissipate electrostatic charges
- have the network connection information (that is, how the interface circuit packs on each network element connect to other network elements)

Step	Action
1	Verify if there are alarms of higher order from the alarm hierarchy. Refer to the “Alarm hierarchies and alarm severities” chapter in Part 1 of this document. First, clear any alarms of higher order in the hierarchy on the 6500 system or the subtending equipment using the appropriate procedures. You can also refer to the signal conditioning section in chapter 1 of this document to help troubleshoot secondary alarms.
2	At the local network element, retrieve all alarms to determine if the original alarm has cleared.
3	Identify the circuit pack raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document.
4	Use the optical fiber/cable connection information to identify the transmit and receive sites of the alarmed signal. Remove the optical fiber from the circuit pack raising the alarm and use the optical power meter to measure the receive power.
5	If the power is below the receiver sensitivity for this circuit pack above the receiver sensitivity for this circuit pack
	Then go to
	step 6
	step 9
	For information about circuit pack technical specifications, refer to the <i>Planning - Ordering information</i> , 323-1851-151.

Power is below the receiver sensitivity

- 6 Adjust the local attenuation, if equipped, to try to get the receive power above the receiver sensitivity level.

Procedure 5-94 (continued)

ODU Signal Degrade

Step	Action	
7	If the receive power after adjustment is still below the receiver sensitivity above the receiver sensitivity but below the maximum receiver power	Then go to step 8 step 9
8	Remove the Tx optical fiber from the far-end circuit pack and measure the transmit power at the far-end. If the transmit power at the far-end is above the launch power (minimum) below the launch power (minimum)	Then the optical fiber attenuation is too high, the optical fiber connections are dirty, or the optical fiber is damaged. Use your company procedure to determine and clear the problem. Go to step 10 . replace the module that corresponds to the facility raising the alarm. Refer to the “Replacing a Pluggable module” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545. Go to step 10 .

Power is above the receiver sensitivity

- 9** Clean all connections at both ends of the optical fiber link following your company standards and re-attach the optical fibers.

Determining if the alarm has cleared

10	If the original alarm has	Then
	cleared	the procedure is complete
	not cleared	replace the module that corresponds to the facility raising the alarm. Refer to the “Replacing a pluggable module” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545. Then, clean and re-attach both optical fibers. Refer to the cleaning connectors procedures in <i>Installation - General Information</i> , 323-1851-201.0.

Procedure 5-94 (continued)

ODU Signal Degrade

Step	Action
11	If the original alarm has Then
cleared	the procedure is complete
not cleared	replace the circuit pack reporting the alarm. Refer to the equipment replacement procedures in <i>Fault Management - Module Replacement</i> , 323-1851-545. Then, clean and re-attach both optical fibers. Refer to the cleaning connectors procedures in <i>Installation - General Information</i> , 323-1851-201.0.
12	Retrieve all alarms from the remote network element at the transmit end.
13	Look for an alarm message for the remote network element circuit pack connected to the original shelf.
14	If there are Then
no alarms at the transmit end	ensure that the equipment and facility or the client and line facilities of the remote circuit pack are in-service and connected. Refer to the "Retrieving equipment and facility details" procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310. Go to step 15 .
additional alarms at the transmit end	refer to the appropriate alarm clearing procedures. Go to step 15 .
15	At the local network element, retrieve all alarms to determine if the original alarm has cleared.
16	If the original alarm Then
has cleared	the procedure is complete
raised was against OTUTTP or ODUTTP facility and the alarm has not cleared	go to step 17
raised was otherwise, and the alarm has not cleared	go to step 18
17	Verify that the provisioned line rate on the upstream circuit pack matches the line rate on the local circuit pack. Correct any mismatches.
18	Contact your next level of support or your Ciena support group.

—end—

Procedure 5-95

ODU Signal Fail

Alarm ID: 1761, 1782, 1786, 1789, 1790, 1791, 1792, 1793, 1794, 1862

Probable cause

This alarm is raised when the BIP-8 error is higher than the provisioned value on the alarmed circuit pack.

Impact

Critical, service-affecting (C, SA) alarm
Major, service-affecting (M, SA) alarm
Minor, non-service-affecting (m, NSA) alarm

Prerequisites

To perform this procedure, you must

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0
- have an antistatic wrist strap to dissipate electrostatic charges
- have the network connection information (that is, how the interface circuit packs on each network element connect to other network elements)

Step	Action
1	Verify if there are alarms of higher order from the alarm hierarchy. Refer to the “Alarm hierarchies and alarm severities” chapter in Part 1 of this document. First, clear any alarms of higher order in the hierarchy on the 6500 system or the subtending equipment using the appropriate procedures. You can also refer to the signal conditioning section in chapter 1 of this document to help troubleshoot secondary alarms.
2	At the local network element, retrieve all alarms to determine if the original alarm has cleared.
3	Identify the circuit pack raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document.
4	Use the optical fiber/cable connection information to identify the transmit and receive sites of the alarmed signal. Remove the optical fiber from the circuit pack raising the alarm and use the optical power meter to measure the receive power.

Procedure 5-95 (continued)

ODU Signal Fail

Step	Action	
5	If the power is	Then go to
	below the receiver sensitivity for this circuit pack	step 6
	above the receiver sensitivity for this circuit pack	step 9
	For information about circuit pack technical specifications, refer to the <i>Planning - Ordering information</i> , 323-1851-151.	
Power is below the receiver sensitivity		
6	Adjust the local attenuation, if equipped, to try to get the receive power above the receiver sensitivity level.	
7	If the receive power after adjustment is	Then go to
	still below the receiver sensitivity	step 8
	above the receiver sensitivity but below the maximum receiver power	step 9
8	Remove the Tx optical fiber from the far-end circuit pack and measure the transmit power at the far-end. If the transmit power at the far-end is	
	above the launch power (minimum)	the optical fiber attenuation is too high, the optical fiber connections are dirty, or the optical fiber is damaged. Use your company procedure to determine and clear the problem. Go to step 10 .
	below the launch power (minimum)	replace the module that corresponds to the facility raising the alarm. Refer to the “Replacing a Pluggable module” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545. Go to step 10 .

Power is above the receiver sensitivity

- 9** Clean all connections at both ends of the optical fiber link following your company standards and re-attach the optical fibers.

Procedure 5-95 (continued)

ODU Signal Fail

Procedure 5-95 (continued)

ODU Signal Fail

Step	Action	Then
15	At the local network element, retrieve all alarms to determine if the original alarm has cleared.	
16	If the original alarm has cleared	the procedure is complete
	raised was against OTUTTP or ODUTTP facility and the alarm has not cleared	go to step 17
	raised was otherwise, and the alarm has not cleared	go to step 18
17	Verify that the provisioned line rate on the upstream circuit pack matches the line rate on the local circuit pack. Correct any mismatches.	
18	Contact your next level of support or your Ciena support group.	

—end—

Procedure 5-96 ODU/OTU Trace Identifier Mismatch

Alarm IDs: 670, 836, 1003, 1010, 1172, 1180, 1447, 1472, 1483, 1501, 1502, 1743

Probable cause

This alarm is raised when the trail trace identifier (TTI) value received by the facility differs from the expected provisioned TTI value. This can be caused by incorrect fibering or incorrect provisioning of the TTI value.

ODU/OTU TTI mismatch detection are independent of each other.

Mismatches of TTI can be declared based on the comparison of the Actual received TTI and Expected received TTI values of the following components:

- Source Access Point Identifier (SAPI) only
- Destination Access Point Identifier (DAPI) only
- SAPI + DAPI
- Operator specific (default)

The TCM TTI mismatch detection is based on the comparison of the Actual received TTI and Expected received TTI values of the following components:

- Source Access Point Identifier (SAPI) only (default)
- Destination Access Point Identifier (DAPI) only
- SAPI + DAPI

For the (1+8)xOTN FLEX MOTR circuit pack, a low order ODU Trace Identifier Mismatch alarm can be raised against the low order ODU facilities.

For the eMOTR circuit pack, the alarm can be raised against the ODUTTP and OTUTTP facilities when the following is true:

TFMODE=ALMONLY
TIMEN=SAPI, DAPI, SAPI+DAPI, or OPERATOR

Critical alarm will raise when there is mismatch in expected and receive trace of either of the following when:

TFMODE=ALMONLY
TIMEN=SAPI, DAPI, SAPI+DAPI, or OPERATOR

Procedure 5-96 (continued)

ODU/OTU Trace Identifier Mismatch

For the 16xFLEX OTN I/F circuit pack, BDI is sent in response to TTI Mismatch if the following is true:

TFMODE=LINEFAIL or ALMONLY
TIMEN=SAPI, DAPI, SAPI+DAPI, or OPERATOR

For the 40G OTN XCIF circuit pack, BDI is sent in response to TTI Mismatch if the following is true:

TFMODE=LINEFAIL
TIMEN=SAPI, DAPI, SAPI+DAPI

For the 10x10G PKT/OTN I/F and 100G PKT/OTN XCIF circuit packs, BDI is sent in response to TTI Mismatch at the PM and TCM layers if the following is true:

TFMODE=LINEFAIL or ALMONLY
TIMEN=SAPI, DAPI, or SAPI+DAPI

Note: The LINEFAIL mode for SAPI and DAPI mismatch is only supported on 16xFLEX OTN I/F and 40G OTN XCIF circuit packs.

Impact

Critical, service-affecting (C, SA) alarm
Major, service-affecting (M, SA) alarm
Minor, non-service-affecting (m, NSA) alarm

The default severity for the “ODU Trace Identifier Mismatch” alarm is:

- m, NSA when ODUTIMEN is set to OPERATOR and ODUTFMODE is ALMONLY
- m, NSA when ODUTIMEN is set to SAPI and/or DAPI and ODUTFMODE is ALMONLY
- m, NSA when ODUTIMEN is set to SAPI and/or DAPI and ODUTFMODE is LINEFAIL on a protected path
- C, SA when ODUTIMEN is set to SAPI and/or DAPI and ODUTFMODE is LINEFAIL on an active/working path

The default severity for the “OTU Trace Identifier Mismatch” alarm is:

- m, NSA when OTUTIMEN is set to OPERATOR and TFMODE is ALMONLY or LINEFAIL
- m, NSA when OTUTIMEN is set to SAPI and/or DAPI and TFMODE is ALMONLY

Procedure 5-96 (continued)

ODU/OTU Trace Identifier Mismatch

- m, NSA when OTUTIMEN is set to SAPI and/or DAPI and TFMODE is LINEFAIL on a protected path
- C, SA when OTUTIMEN is set to SAPI and/or DAPI and TFMODE is LINEFAIL on an active/working path

Prerequisites

To perform this procedure, you must

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0
- have the optical fiber connection information (that is, how the modules on each network element connect to other network elements)
- use an account with at least a level 3 UPC

Step	Action						
1	Use the optical fiber connection information to identify the transmit and receive sites of the alarmed signal.						
2	Verify that the optical fiber connections are correct on the circuit pack that is raising the alarm and on the upstream circuit pack.						
3	From the Site Manager Configuration menu, select the Equipment & Facility Provisioning application, and use the Trail Trace dialog box to retrieve the TTI values for the optical facilities at the transmit network element and at the alarmed receive network element. Refer to the “Retrieving and editing trail trace messages” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.						
4	Click Refresh in the Trail Trace dialog box.						
5	Select your next step. <table border="1"><thead><tr><th>If the alarm</th><th>Then</th></tr></thead><tbody><tr><td>clears</td><td>this procedure is complete</td></tr><tr><td>does not clear</td><td>go to step 6</td></tr></tbody></table>	If the alarm	Then	clears	this procedure is complete	does not clear	go to step 6
If the alarm	Then						
clears	this procedure is complete						
does not clear	go to step 6						
6	Compare the outgoing TTI value of the transmit signal at the transmit network element with the expected TTI value of the receive signal at the receive network element. If the values are different, change the expected TTI value of the receive signal to match the outgoing TTI value of the transmit signal. Refer to the “Retrieving and editing trail trace messages” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.						

Procedure 5-96 (continued)

ODU/OTU Trace Identifier Mismatch

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

—end—

Procedure 5-97

Optical Line Fail

Alarm IDs: 541, 610, 1718

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 RAMAN, OPTMON and AMP facilities optically downstream of the fiber cut/disconnect.

For the SRA amplifiers, this alarm is raised when no OSC and no Telemetry Gain (TG) signal is received. Depending on the OSRP SNC configuration, the Optical Line Fail alarm can trigger a restoration of SNC services.

ATTENTION

For SRA and ESAM circuit packs, when there is an “optical line” condition on the “Line A In Port”, an “Automatic OTDR Trace” is triggered and a short and long trace OTDR is performed. During the OTDR Trace, an “OTDR Trace in Progress” alarm is raised. If there is an issue in the first 20 km of the Line A In (port 8), the “Line A Input OTDR High Reflection Detected” or “Line A Input OTDR High Loss Detected” alarm is raised.

The alarm is masked when you place the AMP and/or RAMAN facilities OOS.

The Optical Line Failure condition invokes “Automatic Laser 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 will also be 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.

DANGER



Risk of radiation exposure

If light is used to test the broken fiber (for example, with a light source or an OTDR), certain Automatic Laser Shut Off (ALSO) and 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 out of service (OOS) when performing fiber repairs.

Procedure 5-97 (continued)

Optical Line Fail**Impact**

Major, service-affecting (M, SA) alarm

Prerequisites

To perform this procedure, you must:

- use an account with at least a level 3 UPC
- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0
- have an antistatic wrist strap to dissipate electrostatic charges
- have a fiber cleaning kit
- have a power meter and a power source

Step Action

- 1 Use system design data to determine the controlling DOC instance for the link that is raising the alarm. Note that in case of bidirectional failures, there will be one DOC instance for each direction and both should be taken OOS.
Change the DOC **Primary state** to out of service (OOS). Refer to the “Editing the DOC Settings” procedure in Part 2 of *Configuration - Provisioning and Operating*, 323-1851-310.

Manually disabling the required facilities in the opposite direction

2

**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, ensure the optical amplifier is OOS, then disconnect or reconnect the fiber.

Step	Action
	<p style="text-align: center;">CAUTION</p>  <p>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.</p>
<p>3</p> <p>4</p>	<p>For the node with the OLF alarm (the downstream node), select the AMP and the SRA (if present) circuit pack showing the associated "Automatic Shutoff" alarm from the Configuration, Facility & Provisioning screen in the Site Manager.</p> <p>In the Facility Type drop-down box, select "AMP" if not already selected. Select the specific AMP facility showing the "Automatic Shutoff" alarm. Click the Edit button and change the primary state to OOS.</p> <p>If there is an SRA circuit pack at the same site, place the RAMAN facility OOS</p>
	<p>Determining the neighboring node</p> <p>5</p> <p>6</p>

- 5 Select the circuit pack that has the OLF alarm (if the OLF is raised against an OPTMON facility, then this will be a different circuit pack than selected in [step 2](#)).
- 6 In the Facility Type drop-down box, select "ADJ-LINE". Record the node name (TID) reported for the "Actual Far-End Address" of this facility. This is the neighboring (upstream) node.

Manually disabling the required facilities upstream

- 7 Log into the node identified in [step 6](#). Select the AMP showing the Automatic Shutoff alarm from the Configuration, Facility & Provisioning screen in Site Manager.
- 8 In the Facility Type drop-down box, select "AMP" if not already selected. Select the specific AMP facility showing the Automatic Shutoff alarm, click the edit button and change the primary state to OOS.
- 9 If there is an SRA circuit pack at the same site, place the RAMAN facility OOS.

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 steps [step 2](#) to [step 9](#) again.

The amplifiers and RAMAN 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).

Procedure 5-97 (continued)

Optical Line Fail

Step	Action	
<i>Locating the fiber fault</i>		
10	Select your next step.	
	If an	
	OTDR is available	Then go to
	step 11	
	ESAM or SRA is available	step 12
	OTDR is not available	step 14
11	Locate the fiber break using the OTDR. This can be performed from the downstream node by connecting the OTDR to the fiber coming into port 8 of the AMP in OLF, or from upstream by connecting the OTDR to the fiber coming from port 5 of the AMP in Automatic Shutoff. Go to step 13 .	
12	Using the OTDR functionality built into the circuit pack, view the OTDR trace. Refer to the “Downloading a SOR file” and “Displaying an OTDR trace graphically” procedures in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310, to locate the fault.	
13	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 14
14	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 8 of the AMP showing the OLF alarm. Replace any obviously damaged patchcords.	
15	Use a separate power source and power meter to measure the loss between the fiber plant ingress and port 8 of the AMP.	
16	Check the fiber connections at the upstream node. At the upstream node, systematically clean each optical connection between port 5 of the AMP showing the Automatic Shutoff alarm and the fiber plant ingress / patch panel. Replace any obviously damaged patchcords.	
17	Use a separate power source and power meter to measure the loss between port 5 of the AMP and the ingress of the fiber plant / patch panel.	
18	Reconnect, replace, or repair the fiber. If there is an AMP present, run manual OTDR traces to validate the fault. Refer to the “Performing a manual OTDR trace” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310, to locate the fault.	

Procedure 5-97 (continued)

Optical Line Fail

Step	Action
19	For the ESAM or SRA, once the fault has been cleared, run a manual OTDR trace, and reset the baseline. Refer to the “Setting a SOR file as baseline” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
20	For the AMP and RAMAN (if present) facilities in step 2 and step 9 , change the primary state to IS using the same method.
21	Select your next step. If the affected fiber span is on a stretched span otherwise Then go to “Recovering from a fiber cut on a stretched span” on page 5-246 step 22
22	Change the DOC Primary state back to in service (IS). Refer to the “Editing the DOC Settings” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
23	Verify if the alarm has cleared. If the DOC Automation Mode is not set to Auto Re-optimize as Necessary, click on the Re-Optimize button in the DOC facility screen. Refer to the “Re-optimizing channels” procedure in Part 2 of the <i>Configuration - Provisioning and Operating</i> , 323-1851-310. 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 Procedure 5-100, “OSC Loss Of Signal” on page 5-254 , keeping in mind that the OSC Loss Of Signal will be masked in this situation by the Optical Line Fail alarm.
24	If the alarm does not clear and the special case above has been ruled out, contact your next level of support or your Ciena support group. This procedure is complete.

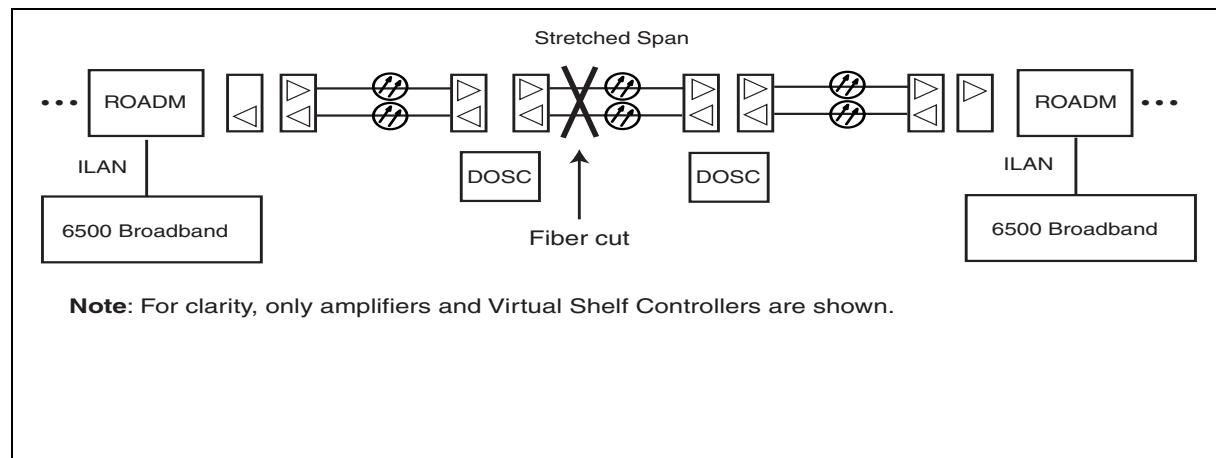
Recovering from a fiber cut on a stretched span

Note: The following procedure is used to recover line traffic after a fiber cut has been repaired on a span where the span loss exceeds the OSC budget. On such spans, the OSC cannot be used for communication across the span, so the data communication traffic that is normally carried by the OSC is usually carried over an out-of-band link, such as 6500 GCC0 or an OM5000 MOTR channel being carried as traffic. Since the link is down, this communications channel is also down. Because of this, the amplifiers cannot coordinate between themselves to bring the line up safely. See [Figure 5-1](#) for a configuration example. To bring this span back up, the amplifiers on the span must be manually restored by performing this procedure.

Procedure 5-97 (continued)

Optical Line Fail

Step	Action
This procedure requires either remote communication to the NEs on both ends of the span that does not require the link between them or personnel on site at each site to perform the following steps.	

Figure 5-1**Recovering from a fiber cut on a stretched span**

Procedure 5-97 (continued)

Optical Line Fail

Step	Action
	<p>DANGER 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.</p>
	<p>If the fiber downstream of the MLA2 C-Band, MLA2 w/ VOA, SRA, SAM, ESAM, XLA, or MLA3 C-Band Line A output connector becomes disconnected accidentally while the Amp Auto Shutoff Disabled feature 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).</p> <p>The ORL based APR safety mechanism remains active.</p>
25	<p>Make sure communications are available to the network elements on either side of the stretched span, and resources are deployed on each side of the stretched span, where the data communications are bridged over to the terminal (6500/OM5000) shelves.</p>
26	<p>Note that Shutdown Thresholds cannot be edited using the GUI interface; therefore TL1 commands must be used. Have the following information available:</p> <ul style="list-style-type: none"> • IP address and Shelf number of each shelf where an amplifier is to be modified • Slot number where each amplifier is located <p>Log into the network elements on each side of the stretched span and disable automatic shutoff on the stretched span as follows:</p> <ol style="list-style-type: none"> a. Using Hyperterm or an equivalent program, open a telnet session on each network element in the stretched span and log into the NE using the following command: <pre>ACT-USER::<ADMIN Level User>:1::<ADMIN Level password>;</pre> b. Set the Line A (port 8) pre-amplifier shutoff threshold to -60 dB (temporary shutoff disable, which overrides the automatic shutoff condition) by entering: <pre>ED-AMP::AMP-<shelf>-<slot>-8:2:::SHUTTHRES=-60:;</pre> c. Log out using the following command: <pre>CANC-USER::<ADMIN Level User>:3;</pre>

Procedure 5-97 (continued)

Optical Line Fail

Step	Action
27	When the post-amplifiers on each side of the stretched span have come out of the automatic shutoff condition, use the Performance Monitoring application to calculate the span loss after the repair (Head end amplifier output power - Tail end amplifier input power). Span Loss for an optical span is also stored as a PM. Make sure the span loss is within specifications; if not, take the appropriate actions.
28	Allow the system a few minutes to provide complete internal communications restoration and visibility of the domain from both sides of the stretched span. To verify data communication continuity, log into the network elements on the two ends of the stretched span and confirm all GCC and SONET DCC communications alarms have cleared.
29	<p>After the link has been restored in both directions, enable automatic shutoff on the stretched span as follows:</p> <ul style="list-style-type: none"> a. Using Hyperterm or an equivalent program, open a telnet session on each network element in the stretched span and log into the NE using the following command: <pre>ACT-USER::<ADMIN Level User>:1::<ADMIN Level password>;</pre> <ul style="list-style-type: none"> b. Set the Line A (port 8) amplifier shutoff threshold back to their initial values by entering: <pre>ED-AMP::AMP-<shelf>-<slot>-8:<CTAG>:::SHUTTHRES=-40;;</pre> <p>For normal operation of stretched span applications with valid optical safety feature operation, the shutoff thresholds for the Line A AMP facilities must be provisioned to -40 dBm. Do not provision this threshold below -40 dBm.</p> <ul style="list-style-type: none"> c. Log out using the following command: <pre>CANC-USER::<ADMIN Level User>:<CTAG>;</pre>
30	Change the DOC Primary state back to in service (IS). Refer to the “Editing the DOC Settings” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
31	If the DOC Automation Mode is not set to Enhanced, click on the Re-Optimize button in the DOC facility screen. Refer to the “Re-optimizing channels” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
32	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-98

Optimization Scanning in Progress

Alarm ID: 1813, 1877

Probable cause

This event is raised when there is a Tx dispersion pre-compensation optimization scanning session in progress.

Impact

Warning

Step	Action
1	No action is required. The alarm clears once the optimization scanning session is complete.
2	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-99

OPU Payload Type Mismatch

Alarm IDs: 837, 1012, 1182, 1473, 1484, 1622, 1669

Probable cause

The alarm point is identified at the G.709 level and is raised when the payload mapped in the G.709 signal is not the same in the Tx and Rx direction. The G.709 payload structure identifier (PSI) byte is used for this purpose. This condition can occur as a result of crossed fibers or as a result of incorrect provisioning (for example, the near-end client facility is provisioned to be OC-192 and the far-end client facility is provisioned to be ETH10G).

The alarm is raised when the far-end client facility does not match. For example, if a 40G OCI/40G OCLD pair is connected to a 40G MUX OCI/40G OCLD pair, or if a 40G MUX OCI NTK525CAE5/40G OCLD pair is connected to a 40G MUX OCI NTK525CFE5/40G OCLD pair, the alarm will be raised on both client circuit packs.

For the 40G XCIF OTM2 facility this alarm is raised when the incoming Payload Type (PT) does not match the expected PT.

For the 10X10GE MUX (NTK529BA), this alarm will be raised if a new ODU4 connection is created in Release 9.0 and above and if the remote 10X10GE MUX has a ODU4 connection that was created pre-Release 9.0.

ATTENTION

For OTM4 facilities, some 100G OCI circuit packs use a Ciena proprietary mapping while others use a standard G.709 GMP mapping. The Ciena proprietary mapping and the standard GMP mapping use different OPU4 overhead bytes definitions. As a result, OCI mismatch scenarios involving a mix of the two mapper types will result in the "Payload type actual received (in Hex)" value (displayed in the OTM INFO window of Site Manager) equal to 0, and not the value transmitted by the far-end OCI. Circuit packs which use the standard GMP mapping include the 10x10G MUX (NTK529BB), the 100G OCI (NTK529AC), and the 100GE OCI (NTK529AA) in R9.0. Circuit packs which use the Ciena proprietary mapping include the 10x10GE MUX (NTK529BA) and the 100GE OCI (NTK529AA) prior to R9.0. The current mapping being used on a 100G OCI can be found in the "Packet Mapping" attribute of the ETH100G facility. Refer to the "Retrieving equipment and facility details" procedure in Part 1 of *Configuration - Provisioning and Operating*, 323-1851-310.

Procedure 5-99 (continued) **OPU Payload Type Mismatch**

Note: An extraneous OPU Payload Type Mismatch alarm may be raised in conjunction with a Loss of Multiframe (LOM) alarm against the 10G OTR line and 10G OTSC line, but does not impact network element function or alarm troubleshooting. If this is the case, then ignore the OPU Payload Type Mismatch alarm, and troubleshoot the LOM condition to clear both alarms.

Impact

Critical, service-affecting (C, SA) alarm
Minor, non-service-affecting (m, NSA) alarm

Prerequisites

To perform this procedure, you must

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0
 - have the optical fiber connection information (that is, how the modules on each network element connect to other network elements)

Step	Action
1	If the alarm is raised against a 40G circuit pack another circuit pack
	Then go to step 2 step 4
2	Ensure that the 40G client circuit packs are the same type. A 40G OCI/40G OCLD or Wavelength-Selective 40G OCLD pair must be connected to a 40G OCI/40G OCLD or Wavelength-Selective 40G OCLD pair and a 40G MUX OCI NTK525CAE5/40G OCLD or Wavelength-Selective 40G OCLD must be connected to the same 40G MUX OCI NTK525CAE5/40G OCLD or Wavelength-Selective 40G OCLD pair at the far-end (same for NTK525CF OCI). OCI to MUX interworking is not supported.
3	Check the MUX OCI PEC type, you can check the equipment inventory screen in Site Manager or the faceplate of the circuit pack (Do not check by looking at the equipment provisioning screen in Site Manager.)
4	For a 10X10GE MUX (NTK529BA), if a new ODU4 connection is created in Release 9.0 and above, delete and re-add the ODU4 connection associated with the remote 10X10GE MUX.

Procedure 5-99 (continued)
OPU Payload Type Mismatch

Step	Action				
5	Ensure that the remote NE also has Release 9.0 or above installed when the connection is deleted and re-added. If both ends do not have the Release 9.0 or above software load, contact your next level of support or your Ciena support group. Using fiber and connection records, determine the far-end module connected to the alarmed module. Retrieve the equipment and Facility Details for both the alarmed and remote module. Refer to the “Retrieving equipment and facility details” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.				
6	Ensure that the corresponding client facility at the far-end is provisioned as either the same type (ETH10G, OC192, STM64) as the client facility at the end reporting the OPU Payload Type Mismatch alarm or is provisioned as an OTU facility. Note that if the OTSC at the remote end is provisioned for an OTU facility, then the remote facility setting the OPU Payload type will not be that module, but the upstream equipment where the OPU is generated and access to it will be required to clear the alarm.				
7	If the facility types are not OTU facility and are different, determine the incorrect facility type from your company records and delete and re-add the incorrect facility. Refer to the “Deleting a facility from an equipment” and “Adding a facility to an equipment” procedures in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.				
8	If the original alarm has Then <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">cleared</td> <td style="width: 70%;">the procedure is complete</td> </tr> <tr> <td>not cleared</td> <td>go to step 9</td> </tr> </table>	cleared	the procedure is complete	not cleared	go to step 9
cleared	the procedure is complete				
not cleared	go to step 9				
9	Ensure that no fibers are crossed. The OTU/ODU trail trace can be used to identify crossed fibers. If the OTU/ODU trail trace is provisioned, the “ ODU/OTU Trace Identifier Mismatch ” alarm is raised to indicate crossed fibers. Refer to the “Retrieving and editing trail trace messages” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.				
10	If the alarm does not clear, contact your next level of support or your Ciena support group.				

—end—

Procedure 5-100 OSC Loss Of Signal

Alarm ID: 556

Probable cause

This alarm is raised against an OSC facility when the optical signal for the facility falls below a fixed threshold. One or more of the following conditions can raise this alarm:

- a defective or dirty fiber linking the OSC ports
- a misconnected or disconnected fiber at the OSC port of the upstream neighbor
- a disabled or out-of-service OSC link on the upstream neighbor
- a powered down upstream neighbor

A cold restart and power cycles of the SRA, SAM, ESAM, 2xOSC or SPAP-2 w/2xOSC or shelf will cause a Loss Of Signal condition and this alarm will be raised. This alarm should clear when the cold restart or power cycle completes. In rare cases, this alarm does not clear even after the Loss Of Signal condition clears. Performing [step 7](#) and [step 24](#) of this procedure should clear this alarm.

Impact

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

Prerequisites

To perform this procedure, you must:

- use an account with at least a level 3 UPC
- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0
- have an antistatic wrist strap to dissipate electrostatic charges
- have a fiber cleaning kit
- obtain a replacement pluggable, circuit pack, or fiber patchcord, if required

Procedure 5-100 (continued)

OSC Loss Of Signal

Step	Action
1	Attempt to log into the network element at the upstream (source) end of the alarmed OSC link. If the NE does not respond, ask on-site personnel to confirm the NE is powered up and operational.
	If the far-end network element is Then
	powered down the OSC Loss Of Signal alarm is a result of this condition and will clear when this condition no longer exists.
	not powered down go to step 2
2	On the shelf with the alarmed facility, check port 4 OPTMON of the LIM, SRA, SAM, or ESAM that is associated with the alarmed OSC facility. If there is significant power on port 4 but there is no power at the OSC Rx port, then the fault is local to the site with the alarmed OSC. Power levels can be checked using the Performance->Performance Monitoring->New screen in Site Manager.
3	Using Site Manager Configuration->Equipment and Facility Provisioning screen check that the upstream OSC facility is provisioned. Refer to the "Retrieving equipment and facility details" procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310. If the OSC facility is out of service, restore it to service. Refer to the "Changing the primary state of a facility" procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310. If equipment alarms are active against it, clear those alarms before returning to this procedure.
4	If the original alarm has Then
	cleared the procedure is complete
	not cleared go to step 5
5	Perform a warm restart on the local and upstream SRA, SAM, ESAM, 2xOSC or SPAP-2 w/2xOSC circuit packs using the Fault->Restart menu of Site Manager. Refer to the "Restarting a circuit pack or shelf processor" procedure in Part 1 of this document.
6	If the original alarm has Then
	cleared the procedure is complete
	not cleared go to step 7
7	Using Site Manager Configuration->Equipment and Facility Provisioning screen provision the primary state of the OSC facility at the upstream NE to OOS and then back to IS.

Procedure 5-100 (continued)

OSC Loss Of Signal

Step	Action								
8	If the original alarm has cleared Then the procedure is complete not cleared go to step 9								
9	<p>CAUTION</p>  <p>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.</p>								
	<p>Have on-site personnel disconnect the Rx fiber from the OSC SFP+ SRA, SAM, ESAM, or SPAP-2 w/2xOSC reporting the alarm and using a power meter, measure the Rx power to determine if light is being received.</p> <p>Clean and reconnect the fiber to the Rx of the. See the minimum Rx values as follows:</p> <ul style="list-style-type: none"> • -34 dBm for Short reach SFP (NTK592NPE6) • -34 dBm for Standard reach SFP (NTK592NBE6) • -37 dBm for Premium reach SFP (NTK592NHE6) • -44 dBm for Long reach SFP (NTK592NGE5) • -44 dBm for Long reach SFP (NTK592NVE5) 								
10	If a DWDM SFP (NTK592NR) is used in conjunction with the OSC Filter (1516.9 nm) module (NTK504BA), check the fibering of the OSC filters at each end of the link. Verify that the power going into the filter from the Tx of the SFP is between 3 dBm and 6 dBm and the power coming out of the filter going into the Rx of the SFP is above -43 dBm and below -7 dBm. See the "Technical specifications" chapter in Part 3 of <i>Planning</i> , NTRN10EG, for more information.								
11	<table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; width: 40%;">If</th> <th style="text-align: left; width: 60%;">Then</th> </tr> </thead> <tbody> <tr> <td>the original alarm has cleared</td> <td>the procedure is complete</td> </tr> <tr> <td>Rx power is below the minimum value</td> <td>go to step 18</td> </tr> <tr> <td>Rx power is above the minimum value</td> <td>go to step 12</td> </tr> </tbody> </table>	If	Then	the original alarm has cleared	the procedure is complete	Rx power is below the minimum value	go to step 18	Rx power is above the minimum value	go to step 12
If	Then								
the original alarm has cleared	the procedure is complete								
Rx power is below the minimum value	go to step 18								
Rx power is above the minimum value	go to step 12								
12	Reseat the SRA, SAM, ESAM, 2xOSC or SPAP-2 w/2xOSC. Refer to the "Reseating a circuit pack" procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.								

Procedure 5-100 (continued) OSC Loss Of Signal

Procedure 5-100 (continued)

OSC Loss Of Signal

Step	Action				
20	Check the fibers of the alarmed OSC facility (at the network element raising the alarm and at the upstream network element): <ul style="list-style-type: none"> • verify the fibers are connected, and not crossed, looped back, or misconnected • check and clean any dirty fibers. Refer to Cleaning connectors procedures in <i>Installation - General Information</i>, 323-1851-201.0. If no line channels yet exist, verify the line fiber connections.				
21	If the original alarm has Then <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">cleared</td> <td>the procedure is complete</td> </tr> <tr> <td>not cleared</td> <td>contact your next level of support or your Ciena support group</td> </tr> </table>	cleared	the procedure is complete	not cleared	contact your next level of support or your Ciena support group
cleared	the procedure is complete				
not cleared	contact your next level of support or your Ciena support group				
22	Reseat the SRA, SAM, ESAM, 2xOSC or SPAP-2 w/2xOSC at the upstream site (sourcing the signal). Refer to the “Reseating a circuit pack” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.				
23	If the original alarm has Then <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">cleared</td> <td>the procedure is complete</td> </tr> <tr> <td>not cleared</td> <td>go to step 24</td> </tr> </table>	cleared	the procedure is complete	not cleared	go to step 24
cleared	the procedure is complete				
not cleared	go to step 24				
24	Replace the Tx OSC pluggable at the upstream site. Refer to the “Replacing a Pluggable module” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.				
25	If the original alarm has Then <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">cleared</td> <td>the procedure is complete</td> </tr> <tr> <td>not cleared</td> <td>go to step 26</td> </tr> </table>	cleared	the procedure is complete	not cleared	go to step 26
cleared	the procedure is complete				
not cleared	go to step 26				
26	Replace the SRA, SAM, ESAM, 2xOSC or SPAP-2 w/2xOSC circuit pack at the upstream site. Refer to the “Replacing an RLA 5x1 module” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.				
27	If the original alarm has Then <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">cleared</td> <td>the procedure is complete</td> </tr> <tr> <td>not cleared</td> <td>contact your next level of support or your Ciena support group</td> </tr> </table>	cleared	the procedure is complete	not cleared	contact your next level of support or your Ciena support group
cleared	the procedure is complete				
not cleared	contact your next level of support or your Ciena support group				

—end—

Procedure 5-101 OSC RFI

Alarm ID: 1871

Probable cause

This alarm is raised when the Ethernet-over-SONET (EOS) on the far end of the OSC span detects Loss of Frame (LOF) and injects Line RDI towards the local EOS.

Impact

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

Step	Action
1	Check that there is no connectivity issues at the far end.
2	If the “Loss Of Frame” alarm is active at the far end of the OSC, clear the alarm. Refer to the “ Loss Of Frame, Loss Of Multiframe, or Signal Fail alarms ” alarm clearing procedure in this document. The alarm clears after the Line RDI is no longer being detected (far end stops injecting Line RDI signal).
3	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-102

OSC Signal Degrade

Alarm ID: 711

Probable cause

This alarm is raised against an OSC facility when the OSC bit error rate (BER) crosses the provisioned threshold. The alarm clears when the BER falls below the provisioned threshold by a factor of ten. For example, if the provisioned BER is 1E-5, the average BER must drop below 1E-6 for the alarm to clear. Conditions that can cause the OSC channel BER to exceed the provisioned threshold include:

- a dirty fiber connection
- a failed OSC SFP
- an span loss beyond the specifications of the OSC SFP
- an incorrect OSC SFPs installed

This alarm is masked by the OSC Loss Of Signal alarm.

Impact

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

Prerequisites

To perform this procedure, you must:

- use an account with at least a level 3 UPC
- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0
- have an antistatic wrist strap to dissipate electrostatic charges
- have a fiber cleaning kit
- obtain a replacement circuit pack or fiber patchcord, if required

Step	Action
1	Using the Site Manager PM screen, retrieve the system measured OSC power at the amplifier by retrieving the PMs for OPTMON-<shelf>-<slot>-4. Use the reading for OPR-OTS, untimed column. Refer to the “Retrieving performance monitoring data” in the <i>Fault Management - Performance Monitoring</i> , 323-1851-520.

- 1 Using the Site Manager PM screen, retrieve the system measured OSC power at the amplifier by retrieving the PMs for OPTMON-<shelf>-<slot>-4. Use the reading for OPR-OTS, untimed column. Refer to the “Retrieving performance monitoring data” in the *Fault Management - Performance Monitoring*, 323-1851-520.

Procedure 5-102 (continued)

OSC Signal Degrade

Step	Action
2	Retrieve the OSC facility that is in alarm. Refer to the “Retrieving equipment and facility details” in the Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310. Look in the equipment window to determine the PEC of the OSC SFP being used.
3	Look up the minimum Rx power rating for the PEC from step 2 . Refer to the “Technical specifications” chapter in Part 3 of <i>Planning</i> , NTRN10EG.
4	If the reported Rx power is greater than the Receiver Sensitivity Then go to step 5 less than or equal to the Rx Sensitivity step 9

**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.

5	Remove the Rx Fiber from the OSC SFP that is raising the alarm. Measure the Rx power. Clean and replace the fiber.
6	If the original alarm has cleared the procedure is complete the measured Rx power is greater than the Receiver Sensitivity go to step 7 the measured Rx power is less than or equal to the Rx Sensitivity go to step 9
7	Replace the OSC SFP. Refer to the “Replacing a Pluggable module” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.
8	If the original alarm has Then cleared the procedure is complete not cleared contact your next level of support or your Ciena support group
9	Disconnect the fiber from the LIM that is connected to the OSC SFP Rx. Using a known good fiber and power meter, measure the power from the OSC Tx port on the LIM. Clean and replace the original fiber.

Procedure 5-102 (continued)

OSC Signal Degrade

Step	Action	
10	<p>If</p> <p>the original alarm has cleared</p> <p>the measured Rx power is greater than the Receiver Sensitivity</p> <p>the measured Rx power is less than or equal to the Rx Sensitivity</p>	<p>Then</p> <p>the procedure is complete</p> <p>go to step 11</p> <p>go to step 13</p>
11	Install a new fiber between the LIM OSC Tx and the OSC Rx port. After installation, measure the Rx power at the Rx OSC end, clean and insert the connector.	
12	<p>If</p> <p>the original alarm has cleared</p> <p>the measured Rx power is greater than the Receiver Sensitivity</p> <p>the measured Rx power is less than or equal to the Rx Sensitivity</p>	<p>Then</p> <p>the procedure is complete</p> <p>go to step 7</p> <p>contact your next level of support or Ciena support group</p>
13	At this point, it has been determined that the OSC power out of the LIM is below specification. Retrieve the OSC facility for the source OSC SFP at the far-end of the link. Refer to the “Retrieving equipment and facility details” in the Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310. Look in the equipment window to determine the PEC of the OSC SFP being used.	
14	Confirm the same kind of SFP is being used on both ends of the span.	
15	<p>If the PECs</p> <p>are different</p> <p>are the same</p>	<p>Then go to</p> <p>step 16</p> <p>step 19</p>
16	An incorrect PEC is installed. Consult your company records to determine which PEC is correct. The PEC must match.	
17	Replace the OSC SFP with the proper SFP. Refer to the “Replacing a Pluggable module” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545 and “Changing the provisioned PEC” procedure in the Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.	
18	<p>If original alarm</p> <p>has cleared</p> <p>has not cleared</p>	<p>Then</p> <p>the procedure is complete</p> <p>restart this procedure</p>

Procedure 5-102 (continued)

OSC Signal Degrade

Step	Action								
19	At the source site for the OSC signal, remove the Rx OSC fiber from the associated LIM module and measure the Tx power into the LIM from the OSC SFP. Clean and replace the fiber.								
20	Look up the minimum Tx Output power for the SFP PEC in the “Technical specifications” chapter in Part 3 of <i>Planning</i> , NTRN10EG.								
21	<table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; width: 30%;">If</th> <th style="text-align: left;">Then</th> </tr> </thead> <tbody> <tr> <td>the original alarm has cleared</td> <td>the procedure is complete</td> </tr> <tr> <td>the measured Tx power is greater than the Min Tx Output Power</td> <td>go to step 28</td> </tr> <tr> <td>the measured Tx power is less than or equal to the Min Tx Output Power</td> <td>go to step 22</td> </tr> </tbody> </table>	If	Then	the original alarm has cleared	the procedure is complete	the measured Tx power is greater than the Min Tx Output Power	go to step 28	the measured Tx power is less than or equal to the Min Tx Output Power	go to step 22
If	Then								
the original alarm has cleared	the procedure is complete								
the measured Tx power is greater than the Min Tx Output Power	go to step 28								
the measured Tx power is less than or equal to the Min Tx Output Power	go to step 22								
22	Unplug the Tx fiber from the OSC SFP. Using a known good fiber and power meter, measure the power from the OSC SFP Tx port. Clean and replace the original fiber.								
23	<table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; width: 30%;">If</th> <th style="text-align: left;">Then</th> </tr> </thead> <tbody> <tr> <td>the original alarm has cleared</td> <td>the procedure is complete</td> </tr> <tr> <td>the measured Tx power is greater than the Min Tx Output Power</td> <td>go to step 26</td> </tr> <tr> <td>the measured Tx power is less than or equal to the Min Tx Output Power</td> <td>go to step 24</td> </tr> </tbody> </table>	If	Then	the original alarm has cleared	the procedure is complete	the measured Tx power is greater than the Min Tx Output Power	go to step 26	the measured Tx power is less than or equal to the Min Tx Output Power	go to step 24
If	Then								
the original alarm has cleared	the procedure is complete								
the measured Tx power is greater than the Min Tx Output Power	go to step 26								
the measured Tx power is less than or equal to the Min Tx Output Power	go to step 24								
24	Replace the OSC SFP. Refer to the “Replacing a Pluggable module” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.								
25	<table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; width: 30%;">If the original alarm has</th> <th style="text-align: left;">Then</th> </tr> </thead> <tbody> <tr> <td>cleared</td> <td>the procedure is complete</td> </tr> <tr> <td>not cleared</td> <td>contact your next level of support or your Ciena support group</td> </tr> </tbody> </table>	If the original alarm has	Then	cleared	the procedure is complete	not cleared	contact your next level of support or your Ciena support group		
If the original alarm has	Then								
cleared	the procedure is complete								
not cleared	contact your next level of support or your Ciena support group								
26	The fiber between the LIM and OSC is inducing extra loss. Install new fiber between the LIM OSC Rx and the OSC Tx port. After installation, measure the Rx power at the Rx OSC port of the LIM, clean and insert the connector.								
27	<table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; width: 30%;">If</th> <th style="text-align: left;">Then</th> </tr> </thead> <tbody> <tr> <td>the original alarm has cleared</td> <td>the procedure is complete</td> </tr> <tr> <td>the measured Rx power is greater than the Receiver Sensitivity</td> <td>go to step 7</td> </tr> <tr> <td>the measured Rx power is less than or equal to the Rx Sensitivity</td> <td>contact your next level of support or Ciena support group</td> </tr> </tbody> </table>	If	Then	the original alarm has cleared	the procedure is complete	the measured Rx power is greater than the Receiver Sensitivity	go to step 7	the measured Rx power is less than or equal to the Rx Sensitivity	contact your next level of support or Ciena support group
If	Then								
the original alarm has cleared	the procedure is complete								
the measured Rx power is greater than the Receiver Sensitivity	go to step 7								
the measured Rx power is less than or equal to the Rx Sensitivity	contact your next level of support or Ciena support group								

Procedure 5-102 (continued)

OSC Signal Degrade

Step	Action
28	At this point, the power into the link meets specifications, yet the power leaving the link does not. This can be caused by any of the following: <ul style="list-style-type: none">• a high span loss• a dirty connector on inside of the LIM module or line side of the LIM module• an OSC filter failure on the LIM module• an incorrect OSC SFP pair for the span loss.
29	Troubleshooting of these items may be traffic affecting. Contact your next level of support or Ciena support group.

—end—

Procedure 5-103

OSPF Adjacency Loss alarms

Use this procedure to clear the following alarms associated with OSPF circuits provisioned on COLAN-A/COLAN-X, DCC, GCC, ILAN-IN/LAN-OUT, or OSC interfaces.

Conditions that can prevent the establishment of an OSPF adjacency include:

- no OSPF circuit provisioned at the far-end of the link
- the OSPF circuit parameters provisioned at both ends of the link do not match

The OSPF Adjacency Loss alarms apply to IPv4/OSPFv2 comms only

COLAN-A OSPF Adjacency Loss

Alarm ID: 978

COLAN-X OSPF Adjacency Loss

Alarm ID: 979

Probable cause

This alarm is raised when there is an OSPF circuit provisioned on a COLAN-A/COLAN-X interface, and the adjacency cannot be established.

SECTION/RS DCC OSPF Adjacency Loss

Alarm ID: 1036, 1037, 1038, 1039, 1131, 1356, 1357, 1358, 1359, 1360, 1711, 2052

Probable cause

This alarm is raised when there is an OSPF circuit provisioned on a DCC interface, and the adjacency cannot be established.

LINE/MS DCC OSPF Adjacency Loss

Alarm ID: 1313, 1314, 1315, 1316, 1317, 1709, 2051

Probable cause

This alarm is raised when there is an OSPF circuit provisioned on a Line DCC interface, and the adjacency cannot be established.

GCC0/GCC1/GCC2 OSPF Adjacency Loss

Alarm ID: 1040, 1041, 1144, 1318, 1319, 1320, 1361, 1362, 1363, 1427, 1428, 1429, 1431, 1726, 1727, 1728

Probable cause

This alarm is raised when there is an OSPF circuit provisioned on a GCC0/GCC1/GCC2 interface, and the adjacency cannot be established.

Procedure 5-103 (continued)

OSPF Adjacency Loss alarms

ILAN-IN OSPF Adjacency Loss

Alarm ID: 976

ILAN-OUT OSPF Adjacency Loss

Alarm ID: 977

Probable cause

This alarm is raised when there is an OSPF circuit provisioned on an ILAN-IN/ILAN-OUT interface, and the adjacency cannot be established.

OSC OSPF Adjacency Loss

Alarm ID: 975

Probable cause

This alarm is raised when there is an OSPF circuit provisioned on an OSC interface, and the adjacency cannot be established.

This alarm is also raised when the OSC fibers between the OSC1 and OSC2 at the Line AMP NE are swapped (misconnected/crossed).

Impact

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

OSPFv2 Adjacency Loss

Alarm ID: 1873

Probable cause

This alarm is raised when there is an OSPFv2 circuit provisioned on an interface (COLAN, ILAN, OSC, GCC, DCC) but the adjacency cannot be established.

Impact

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

OSPFv3 Adjacency Loss

Alarm ID: 1929

Probable cause

This alarm is raised when there is an OSPFv3 circuit provisioned on an interface (COLAN, ILAN, OSC, GCC, DCC) but the adjacency cannot be established.

Note that the OPSFv3 circuits apply to IPv6 networks only. The OSPFv3 and OSPFv2 alarms may both get raised together if both are applied to the same facility (for example, COLAN-X) and a fault occurs on that affected facility.

Procedure 5-103 (continued)
OSPF Adjacency Loss alarms

ATTENTION

This alarm displays in the Additional Information column the interface AID the alarm is raised against. The Additional Information field is available for SP2 and SPAP-2.

Impact

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

Step	Action	
1	Verify that there is an OSPF circuit provisioned at the far-end of the link by retrieving the OSPF circuits at the far-end of the failed facility. Ensure there is an entry for the failed facility. Refer to the “Retrieving communications settings” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.	
	When troubleshooting the OSPF adjacency loss alarms, make sure to compare the similar protocols on each end of the link. For example, either OSPFv2 or OSPFv3. Each protocol has its own tab in Site Manager, make sure to select the correct tab.	
	Note: OSPFv2 and OSPFv3 are not compatible with each other. Therefore the settings in one protocol do not affect the other.	
2	If a far-end OSPF circuit exists	Then go to step 5
	does not exist	step 3
3	Provision the missing OSPF circuit. Refer to the “Adding a new entry in the communications settings” in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.	
4	If the original alarm has cleared	Then the procedure is complete
	not cleared	go to step 5

Procedure 5-103 (continued) **OSPF Adjacency Loss alarms**

--end--

Procedure 5-104

OSPF Max Capacity Reached

Alarm ID: 1676

Probable cause

This alarm is raised when a shelf reaches its maximal capacity of handling the number of OSPF network elements in the OSPF network. These OSPF network elements may include 6500 and CPL shelves as well as other OSPF-capable equipment.

This alarm provides an early warning indication to prevent the OSPF network from potential failure.

Impact

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

Prerequisites

To perform this procedure, you require an account with at least a level 3 UPC.

Step	Action
1	If the alarm is raised on all 6500 shelves, split the OSPF network. Refer to “Data communications planning” in Part 4 of <i>Planning</i> , NTRN10EG
2	If the alarm is only raised on a single 6500 shelf, it can indicate that the memory of this shelf is fragmented and the OSPF is not able to expand its memory partition. In this case, perform an SP warm restart to clear the alarm. Refer to the “Restarting a circuit pack or shelf processor” procedure in Part 1 of this document.
3	If the alarm does not clear, contact your next level of support or Ciena support group.

—end—

Procedure 5-105

OSRP CCI Session Down

Alarm ID: 1386

Probable cause

This alarm is raised when the OSRP communication session to the photonic or MSPP subsystem has gone down. For OSRP Types of Photonic and DERIVED with a SONET/SDH XC, this communications session is between the two CPUs of the SP-2. For OSRP of type PROV, this is within the OAMP processor of the SP-2.

This alarm is expected for Photonic and SONET/SDH Control Planes when performing any operation that causes the CPU2 to restart. The alarm should automatically clear within a minute.

Impact

Major, service-affecting (M, SA)

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

Step	Action
1	Check for “Member Shelf Unreachable” alarm. If the alarm is active, clear that alarm first. The “OSRP CCI Session Down” alarm must clear automatically.
2	If the alarm did not clear, restart CPU2 (if Photonic or SONET/SDH, else restart the SP). Refer to the “Restarting a circuit pack or shelf processor” procedure in Part 1 of this document.
3	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-106 OSRP CCI Session Out of Sync

Alarm ID: 1387

Probable cause

This alarm is raised when Optical Signaling and Routing Protocol (OSRP) Cross Connection Interface (CCI) session has lost synchronization with the network element.

This alarm is raised during OSRP enabling, CPU2 restart, or when synchronization is lost between the CPU2 and the OAM&P.

Impact

Major, service-affecting (M, SA)

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

Step	Action
------	--------

- 1 This alarm is cleared by the system when CCI has synchronized the Control Plane database with the NE and the OSRP. If this alarm persists, reset the CPU2, or perform a protection switch of the SP. Refer to the “Operating a protection switch” procedure in Part 2 of *Configuration - Provisioning and Operating*, 323-1851-310.
- 2 If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-107

OSRP Configuration in Progress

Alarm ID: 1745

Probable cause

This alarm is raised when an OTN OSRP instance is added/deleted. This alarm applies to OTN shelves with OTN XC provisioned.

Impact

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

Step	Action	
1	If	Then go to
	two XCs are present	step 2
	only one XC is present	step 3
2	Perform a protection switch on the active XC. Refer to the “Operating a protection switch” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310. Go to step 4 .	
3	Perform a warm restart on the XC. Refer to the “Restarting a circuit pack or shelf processor” procedure in Part 1 of this document.	
4	If the alarm does not clear, contact your next level of support or your Ciena support group.	

—end—

Procedure 5-108 OSRP Line Operationally Blocked

Alarm ID: 1764

Probable cause

This alarm is raised in the following scenarios:

- the High Received Span Loss alarm is raised (only when the “Span loss exceed action” parameter is provisioned to “Blocked” for the OSRP line)
- the Crossed Fibers Suspected alarm is raised against an OPM port
- communication failure with DGEs and AMP sites
- a Circuit Pack Failure alarm is raised for:
 - an MLA/MLA2/MLA3/MLA2v/SLA/XLA or cascaded LIM (SLA) amplifier circuit-packs at ROADM OTS, at the AMP, or DGE OTS
 - a WSS included in a ROADM or a DGE OTS
- a DOC facility is OOS-MA
- DOC Auto add channels and Auto delete channels are disabled
- the DOC Invalid Photonic Domain alarm is raised
- Optical System Topology indicates TOADM or GOADM OTSs in Photonic Control Plane domain
- the OSRP line is blocked resulting from a Bandwidth lockout or Maintenance mode on the associated OSRP line. For information on these parameters, refer to the “L0 and L1 OSRP provisioning” chapter in *Configuration - Control Plane*, 323-1851-330.
- Coherent Select Control parameter set to Off in the Node Information System, on a Coherent Select node. Refer to the “Displaying node information” procedure in the *Administration and Security*, 323-1851-301.

Impact

Warning

Procedure 5-108 (continued)
OSRP Line Operationally Blocked

Step	Action
1	If the line is manually blocked, un-block the line by disabling the OSRP bandwidth lockout. Refer to the “Retrieving OSRP provisioning information” and “Editing an OSRP line” procedures in <i>Configuration - Control Plane</i> , 323-1851-330.
2	Verify and correct any of the causes listed in the “ Probable cause ”.
3	If the alarm does not clear, contact your next level of support or Ciena support group.

—end—

Procedure 5-109

OSRP Node Operationally Blocked

Alarm ID: 1422

Probable cause

This alarm can be raised during any of the following SONET/SDH, Photonic, or OTN Control Plane scenarios:

- SONET/SDH and Photonic Control Plane;
 - node is administratively blocked by the user
 - software upgrade
 - database backup or restore
 - warm restart of active CPU2
 - SP switchover
 - restart of an active OAM&P
- OTN Control Plane:
 - node is administratively blocked by the user
 - database restore during commit
 - warm or cold restart of active XC
 - switchover
 - warm restart of an OTN Flex MOTR or 40G OTN XCIF circuit pack

This alarm is also raised by the Photonic Control Plane when a database auto-save is in progress. See the disabled alarms list for finding occurrences of the “Database Auto Save in Progress” alarm that correlate with instances of this alarm. Note that the “Database Auto Save in Progress” alarm is disabled by default.

Impact

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

Step	Action
1	If the node is manually blocked, un-block the node by changing the OSRP node “Admin state” to “Unlocked”. Refer to the “Retrieving OSRP provisioning information” and “Editing an OSRP node” procedures in <i>Configuration - Control Plane</i> , 323-1851-330.

Procedure 5-109 (continued)

OSRP Node Operationally Blocked

Step	Action
2	If any of the actions listed in the “Probable cause” are in progress, wait until the action is completed. Note: This alarm will not be cleared during the second invoke of the upgrade. The alarm is cleared at the end of the second invoke.
3	If the alarm does not clear, contact your next level of support or Ciena support group.

—end—

Procedure 5-110 OSRP Port Capability Mismatch

Alarm ID: 1412

Probable cause

This alarm is raised when there is a hierarchical level configuration mismatch.

Impact

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

Prerequisites

To perform this procedure, you require an account with at least a level 3 UPC.

Step	Action
1	Compare the hierarchical level of the OSRP lines in both the local and remote nodes. Refer to <i>Configuration - Control Plane</i> , 323-1851-330 for related procedures.
2	Adjust the hierarchical levels as required at the remote or local node.
3	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-111 OTDR Trace In Progress

Alarm ID: 1712, 1964

Probable cause

This alarm is raised when the OTDR trace is in progress.

All traffic-related alarms are masked when this alarm is raised.

Impact

Warning

Step	Action
1	No action is required. The alarm clears when the trace completes automatically.
2	You can also stop the current trace in progress by pressing the "Stop Trace(s)" button in the Site Manager OTDR window to clear the alarm. Refer to "Performing a manual OTDR trace" procedure in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
3	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-112

OTL Skew Out Of Range

Alarm ID: 1681, 1682, 1683

Probable cause

This alarm is raised against the OTM3/OTUTTP client facility of a 40G+ CFP OCI circuit pack, or OTM4/OTUTTP client facility of a 100G OCI (NTK529AA/AC), or 100G WL3e OTR circuit pack when the system detects that the virtual lane skew exceeds the specified skew range from G.798.

Impact

Critical, service-affecting (C, SA) alarm, unprotected
Minor, non-service-affecting (m, NSA) alarm, protected

Prerequisites

To perform this procedure, you must:

- observe all safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545
- have the fiber connection information (that is, how the optical modules on each network element connect to other network elements)
- if required, obtain the replacement fiber for connection between the subtending equipment and the CFP
- if required, obtain a replacement CFP module
- use an account with at least a level 3 UPC

Step	Action
1	Determine the type of the connection fiber between the subtending equipment and the CFP module based on CFP type (NTTA01FB, NTTA01BJ, NTTA03BJ, and NTTA02BJ are SMF, NTTA03AA is MMF).
2	If the fiber type is
	SMF step 3
	MMF step 8
3	Ensure the Integrated Test Feature (ITS) is available on the 40G+ CFP OCI, 100G WL3e OTR, or 100G OCI and operating in Test Set mode. Refer to the “Performing a test with the Integrated Test Set” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.

Procedure 5-112 (continued)

OTL Skew Out Of Range

Step	Action
4	Ensure the Rx/Tx port on the CFP is fiber loop backed using a patch cord fiber.
5	If the alarm does not clear, replace the CFP. Refer to the “Replacing a Pluggable module” in the <i>Fault Management - Module Replacement</i> , 323-1851-545.
6	If the original alarm has cleared, then restore the original configuration and the procedure is complete. Otherwise, go to step 7 .
7	If the original alarm does not clear, it indicates the problem is caused by subtending equipment. Troubleshoot the subtending equipment. Go to step 14 .
8	Ensure that all parallel fibers connected between the subtending equipment and CFP have the same length. If not, then replace them to make them comply with this requirement.
9	If the original alarm does not clear, ensure the Integrated Test Feature (ITS) is available on the 40G+ CFP OCI, 100G WL3e or 100G OCI circuit pack and operating in Test Set mode.
10	Ensure the Rx/Tx port on the CFP is fiber loop backed using a special MPO24 loopback fiber.
11	If the alarm does not clear, replace the CFP. Refer to the “Replacing a Pluggable module” in the <i>Fault Management - Module Replacement</i> , 323-1851-545.
12	If the original alarm has cleared, then restore the original configuration with the new CFP and the procedure is complete. Otherwise, go to step 13 .
13	If the original alarm does not clear, it indicates the problem is caused by subtending equipment. Troubleshoot the subtending equipment.
14	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-113

OTS Provisioning Error

Alarm ID: 974

Probable cause

This alarm is raised against the OTS entity when there is an OTS provisioning error detected. This includes either a discrepancy between an OTS and its associated OTS (that is, an intra-node OTS neighbor), or between an OTS and its OSC neighbor (that is, an inter-node OTS neighbor).

This alarm can be raised in the following scenarios for intra-node OTS neighbors:

- the provisioned associated OTS (**Provisioned OTS** parameter) of the OTS entity does not match the discovered associated OTS (**Actual Associated OTS**)
- the OTS and its discovered associated OTS are not in the same Optical System Identifier (OSID)
- the OTS and its discovered associated OTS have different Configuration Types (for example, one Channel Access and one Amplifier)
- the OTS and its discovered associated OTS have Tx Path Identifiers of the same parity (that is, either both are odd or both are even)
- the OTS and its discovered associated OTS do not have the same Site Identifier
- fibers at the Line AMP NE are swapped (misconnected/crossed)

This alarm is raised when the OTS is provisioned using the Photonic Configuration Management application and the OTS “OSC Required” parameter is set to **True** and the OTS OSC slot/port is set to None. To clear the alarm, you must either provision the OTS OSC slot/port or set the OTS “OSC Required” parameter to **False**. The following actions raise the alarm for the Photonic Control Plane:

- the initial provisioning of a Dynamic Gain Equalizer (DGE) OTS (where no WSS-to-WSS adjacency exists)
- the reconfiguration of an OTS from CHA to DGE

Procedure 5-113 (continued)

OTS Provisioning Error

This alarm can be raised in the following scenarios for inter-node OTS neighbors, when the OTS and its OSC neighbor:

- are at same site
 - are not in the same OSID
 - have Tx Path Identifiers of the same parity (that is, either both are odd or both are even)
 - OSC fibers are swapped or misconnected

Impact

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

Prerequisites

To perform this procedure, you require an account with at least a level 3 UPC.

Step	Action
<p>Note: The provisioning of the Provisioned OTS parameter value is optional; however, if it is provisioned, then it must match the discovered associated OTS. An associated OTS will only be present if there is a second OTS sharing the same OSID (Optical System ID) on the same NE.</p>	
1	Retrieve the OTS details for the alarmed OTS. Refer to the “Retrieving OTS Management, OTS Equipment, and Facility details” and “Editing an OTS instance in the Photonic Configuration Management application” procedures in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
2	Verify the Provisioned OTS parameter value of the alarmed OTS entity matches the Actual Associated OTS . If required, correct the Provisioned OTS value to match the Actual Associated OTS . Refer to the “Editing an OTS instance in the Photonic Configuration Management application” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
3	If the original alarm has Then
	cleared the procedure is complete
	not cleared go to step 4

Procedure 5-113 (continued)

OTS Provisioning Error

Procedure 5-113 (continued)

OTS Provisioning Error

Procedure 5-113 (continued) **OTS Provisioning Error**

Step	Action
14	If the original alarm has Then
	cleared
	not cleared

Procedure 5-113 (continued)

OTS Provisioning Error

Step	Action
22	Check the Actual Far End Address on the associated line-facing LIM, and compare it to the provisioned Expected Far End Address. If the Actual Far End Address on the associated line-facing LIM does not match its provisioned Expected Far End Address, verify proper OSC fiber connectivity to the LIMs.
23	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-114 OTU Signal Degrade

Alarm ID: 835, 1220, 1383, 1445

Probable cause

This alarm is raised when the Rx interface error rate detected by the Section Monitoring Error Detection Code (BIP-8) exceeds 8E-10. The alarm clears when the error rate is 1E-10 or better. This alarm applies to OTUTTP, OTMC2, OTM1, OTM2, OTM3, and OTM4 facilities.

The OTU Signal Degrade alarm is raised when the error threshold of 1E-9 is reached. This is done to ensure that the alarm is raised before the bit error rate reaches 1E-9.

For 8xOTN Flex MOTR and (1+8)x OTN Flex MOTR circuit packs, this alarm is raised when the Error detection Code (BIP-8) exceeds 1E-7. The alarm clears when BIP-8 errors are below 1E-7.

100G WL3e OTR and 100G OCI circuit packs support Post-FEC OTU4 Signal Degrade error calculation in Broadband mode. Post-FEC OTU4 Signal Degrade threshold is provisionable from 1E-6 to 1E-9 (default).

10x10G OCI circuit packs support Post-FEC OTU2 Signal Degrade on the OTM2 client port in Broadband mode. Post-FEC OTU2 Signal Degrade threshold is provisionable from 1E-6 to 1E-9 (default).

10x10G PKT/OTN I/F and 48xGE PKT I/F circuit packs support Post-FEC OTU4 Signal Degrade error calculation in POTS Mode.

ATTENTION

The 10G OTR OTU SD alarm remains active for 40 seconds after all faults (for example, Loss Of Signal and Loss of Frame) clear. This occurs for OTN client facilities and for OTN line facilities with the Rx FEC format set to Off. If the OTU SD alarm does not clear 40 seconds after all related faults clear, then follow the troubleshooting steps outlined in this procedure.

Impact

Major, service-affecting (M, SA) alarm, unprotected

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

Prerequisites

To perform this procedure, you must

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0
- have an antistatic wrist strap to dissipate electrostatic charges
- have the optical fiber connection information (that is, how the circuit packs on each network element connect to other networks)
- have an optical power meter with the same optical connectors as the network element
- have attenuation pads

Step	Action
1	Identify the circuit pack and facility raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document.
2	Check the corresponding subtending circuit pack for failures or alarms. Troubleshoot these alarms/failures before proceeding.
3	Make sure that the circuit pack type and SFP/XFP/CFP type is consistent with the subtending equipment (bit-rate and protocol and FEC settings). Refer to the “Retrieving equipment and facility details” in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.

Procedure 5-114 (continued)

OTU Signal Degrade

Step	Action
4	Using the Site Manager Equipment & Facility Provisioning application under the Configuration menu, retrieve the Rx Actual Power value for the facility reporting the alarm. Refer to the “Retrieving equipment and facility details” in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
5	Select the alarmed OTU facility in the Site Manager Equipment and Facility Screen, click on the Ranges button to display the specifications for that SFP/XFP/CFP. Compare the Rx Actual Power value for the facility with the Rx minimum power and Rx maximum power values displayed.
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	Make sure the signal optical power level into the Rx interface is within specification.
	If the signal level is
	Then go to
	greater than the Rx maximum value step 8
	less than the Rx minimum value step 10
	within specifications step 13
8	The signal may require padding, or an incorrect SFP/XFP/CFP type is used on the circuit pack reporting the alarm or on the subtending equipment. Confirm the proper SFP/XFP/CFPs are installed and add attenuation pads as needed until the Rx power is within the reported specification.
9	If the original alarm
	Then
	clears procedure is complete
	does not clear go to step 13
10	The fiber may be dirty, the fiber connectors may not be fully seated, or an incorrect SFP/XFP/CFP type is used on the circuit pack reporting the alarm or on the subtending equipment. Confirm the proper SFP/XFP/CFP are installed, clean all fiber connectors and ensure they are fully seated.
11	If
	Then
	the original alarm clears procedure is complete
	power is within specifications go to step 13
	power is still below specifications there is an issue with the link or source fault. Contact your next level of support or Ciena support group.
	Recheck the Rx power by retrieving the Rx Actual Power value for the facility reporting the alarm again. (Select the “Retrieve Facility” button to reset to current values.)

Step	Action
12	Replace the SFP/XFP/CFP that supports the facility raising the alarm. Refer to <i>Fault Management - Module Replacement</i> , 323-1851-545.
13	If the original alarm has
	cleared
	not cleared
	Then
	the procedure is complete
	go to step 14
14	Replace the upstream SFP/XFP/CFP or source module. Refer to <i>Fault Management - Module Replacement</i> , 323-1851-545.
15	If the original alarm has
	cleared
	not cleared
	Then
	the procedure is complete
	contact your next level of support or your Ciena support group

—end—

Procedure 5-115

OTU Signal Fail (OTM, OTM2, OTUTTP)

Alarm ID: 1763, 1783, 1788

Probable cause

This alarm is raised when the Post-FEC error is higher than the provisioned value. This alarm applies to 10x10G MUX, 100G OCI, 100G OCLD, and 10x10G PKT/OTNIF circuit packs.

10x10G MUX circuit packs support Post-FEC OTU2 Signal Fail on the OTM2 client port in Broadband and POTS mode. The Post-FEC OTU2 Signal Fail threshold is provisionable from 1E-6 (default) to 1E-9 and 0. Note that Post-FEC OTU2 Signal Fail is disabled if the OTU Signal Fail Threshold value is set to 0.

Impact

Critical, service-affecting (C, SA) alarm

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

Prerequisites

To perform this procedure, you must

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0
- have an antistatic wrist strap to dissipate electrostatic charges
- have the network connection information (that is, how the interface circuit packs on each network element connect to other network elements and how each OC-3 connects to the DSM)

Step	Action
1	Identify the circuit pack and facility raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document.
2	Check the corresponding subtending circuit pack for failures or alarms. Troubleshoot these alarms/failures before proceeding.
3	Make sure that the circuit pack type and SFP/XFP/CFP type is consistent with the subtending equipment (bit-rate and protocol and FEC settings). Refer to the “Retrieving equipment and facility details” in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.

Procedure 5-115 (continued)
OTU Signal Fail (OTM, OTM2, OTUTTP)

Step	Action	
4	Using the Site Manager Equipment & Facility Provisioning application under the Configuration menu, retrieve the Rx Actual Power value for the facility reporting the alarm. Refer to the “Retrieving equipment and facility details” in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.	
5	Select the alarmed OTU facility in the Site Manager Equipment and Facility Screen, click on the Ranges button to display the specifications for that SFP/XFP/CFP. Compare the Rx Actual Power value for the facility with the Rx minimum power and Rx maximum power values displayed.	
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	Make sure the signal optical power level into the Rx interface is within specification.	
	If the signal level is	
	greater than the Rx maximum value	Then go to
	less than the Rx minimum value	step 8
	within specifications	step 10
		step 13
8	The signal may require padding, or an incorrect SFP/XFP/CFP type is used on the circuit pack reporting the alarm or on the subtending equipment. Confirm the proper SFP/XFP/CFPs are installed and add attenuation pads as needed until the Rx power is within the reported specification.	
9	If the original alarm	Then
	clears	procedure is complete
	does not clear	go to step 13
10	The fiber may be dirty, the fiber connectors may not be fully seated, or an incorrect SFP/XFP/CFP type is used on the circuit pack reporting the alarm or on the subtending equipment. Confirm the proper SFP/XFP/CFP are installed, clean all fiber connectors and ensure they are fully seated.	
11	If	Then
	the original alarm clears	procedure is complete
	power is within specifications	go to step 13
	power is still below specifications	there is an issue with the link or source fault. Contact your next level of support or Ciena support group.
	Recheck the Rx power by retrieving the Rx Actual Power value for the facility reporting the alarm again. (Select the “Retrieve Facility” button to reset to current values.)	

Procedure 5-115 (continued)
OTU Signal Fail (OTM, OTM2, OTUTTP)

Step	Action	
12	Replace the SFP/XFP/CFP that supports the facility raising the alarm. Refer to <i>Fault Management - Module Replacement</i> , 323-1851-545.	
13	If the original alarm has	Then
	cleared	the procedure is complete
	not cleared	go to step 14
14	Replace the upstream SFP/XFP/CFP or source module. Refer to <i>Fault Management - Module Replacement</i> , 323-1851-545.	
15	If the original alarm has	Then
	cleared	the procedure is complete
	not cleared	contact your next level of support or your Ciena support group

—end—

Procedure 5-116 Output Loss Of Signal

Alarm ID: 572, 1797

Probable cause

This alarm is raised against an AMP or AMPMON facility when the total output optical power from the amplifier has fallen below the provisioned output LOS threshold value.

The conditions that can cause the output power level to fall below the threshold level include:

- a disconnected fiber
- a dirty optical fiber connector
- a defective fiber optic patchcord
- a defective module
- incorrect provisioning data
- a reflective event (indicated by 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.

The “Output Loss Of Signal” alarm suppresses the “VOA Output LOS” alarm.

This alarm is masked by “Input Loss Of Signal” alarm on the same amplifier facility.

Impact

Major, service-affecting (M, SA) alarm

Prerequisites

To perform this procedure, you must:

- use an account with at least a level 3 UPC
- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0
- have an antistatic wrist strap to dissipate electrostatic charges
- have a fiber cleaning kit

Procedure 5-116 (continued)

Output Loss Of Signal

- have a network and site diagram
- have the LOS threshold level value for this amplifier

Step	Action				
1	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.				
2	If the original alarm has Then <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">cleared</td> <td>the procedure is complete</td> </tr> <tr> <td>not cleared</td> <td>repeat step 1 for each booster amplifier or pre-amplifier farther upstream from the alarmed amplifier</td> </tr> </table>	cleared	the procedure is complete	not cleared	repeat step 1 for each booster amplifier or pre-amplifier farther upstream from the alarmed amplifier
cleared	the procedure is complete				
not cleared	repeat step 1 for each booster amplifier or pre-amplifier farther upstream from the alarmed amplifier				
3	If the original alarm has Then <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">cleared</td> <td>the procedure is complete</td> </tr> <tr> <td>not cleared</td> <td>go to step 4</td> </tr> </table>	cleared	the procedure is complete	not cleared	go to step 4
cleared	the procedure is complete				
not cleared	go to step 4				
4	Verify the AMP facility parameters are correctly provisioned. If required, correct any discrepancies. Refer to the “Retrieving equipment and facility details” and “Editing facility parameters” procedures in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.				
5	If the original alarm has Then <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">cleared</td> <td>the procedure is complete</td> </tr> <tr> <td>not cleared</td> <td>go to step 6</td> </tr> </table>	cleared	the procedure is complete	not cleared	go to step 6
cleared	the procedure is complete				
not cleared	go to step 6				
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	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, Circuit Pack Missing, and Loss Of Signal. If there are no upstream alarms, then verify the optical patchcord connected to the port reporting the alarm: <ul style="list-style-type: none"> • ensure it is connected at both ends and that there is no problem with the optical patchcord • clean the connectors. Refer to the cleaning connectors procedures in <i>Installation - General Information</i>, 323-1851-201.0. 				

Procedure 5-116 (continued)

Output Loss Of Signal

Step	Action	
8	If the original alarm has	Then
	cleared	the procedure is complete
	not cleared	go to step 9
9	Provision the Output LOS threshold value for the AMP facility reporting the alarm to be 5 dB less than the current value. For example, if the Output LOS threshold is -6 dB, change the value to -11 dB. Refer to the “Editing facility parameters” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.	
10	Wait at least one minute for the alarm to clear. Change the Output LOS threshold value back to the original value.	
11	If the original alarm has	Then
	cleared	the procedure is complete
	not cleared	go to step 12
12	Restart the LIM, RLA 5x1 or XLA supporting the alarmed AMP facility. Refer to the “Restarting a circuit pack or shelf processor” in part 1 of this document.	
13	If the original alarm has	Then
	cleared	the procedure is complete
	not cleared	go to step 14
14	Replace the LIM, RLA 5x1 or XLA supporting the alarmed AMP facility. Refer to the “Replacing the amplifier modules” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.	
15	If the alarm does not clear, contact your next level of support or your Ciena support group.	

—end—

Procedure 5-117

Packet Configuration Integrity Fail

Alarm ID: 1943

Probable cause

This alarm is raised when at least one PKT/OTN circuit pack configuration does not match the OTN XC configuration.

The mismatch can occur due to failure such as, faults detected during an OTN XC switchover or Primary OTN XC is restarted when it is not in a hot redundancy state.

This alarm is also raised when eMOTR equipment group configuration does not match the configured hardware. The mismatch can occur due to failures such as, LM fault resulting in restart of the sub-system or incomplete configuration pushed in stand-alone eMOTR restart.

This alarm can also be raised on eMOTR circuit pack after an upgrade. This alarm condition can get raised on eMOTR when configuration in hardware does not match configuration on software during warm restart/upgrade.

A cold restart of the circuit pack that raised the alarm can clear the alarm.

Impact

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

Critical, service-affecting (C, SA) alarm

Step	Action	
1	If the alarm is raised against an eMOTR otherwise	Then go to step 2 step 5
2	If the alarm is raised against a specific Line Module Control Module	Then go to step 3 step 4

Procedure 5-117 (continued)

Packet Configuration Integrity Fail

Step	Action
3	<p>Perform a cold restart on that specific slot to recover the system as follows:</p> <ul style="list-style-type: none"> • Login to the eMOTR CLI using a user with superuser account privileges. • Use the CLI command “module show” to display the state of all modules. • For each module that shows OperState as “Faulted*”, perform a cold restart from TL1. Go to step 10. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p style="text-align: center;">ATTENTION</p> <p>Do not perform a warm restart to clear this alarm.</p> </div>
4	<p>Note: When the “Packet Configuration Integrity Fail” alarm is raised against eMOTR, the “config save” CLI command will be blocked.</p> <p>Perform a cold restart on all circuit packs in equipment group. Go to step 10.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p style="text-align: center;">ATTENTION</p> <p>Do not perform a warm restart to clear this alarm.</p> </div>
5	<p>Attempt another XC protection switch. If the alarm did not clear, continue to step 6.</p>
6	<p>Login to the packet CLI using a user with superuser account privileges.</p>
7	<p>Use the CLI command “module show” to display the state of all modules.</p> <p>No new configuration or existing configuration can be created or modified during this condition from CLI.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p style="text-align: center;">CAUTION</p> <p>Risk of interruption to service</p> <p>The following steps will cause a temporary traffic outage related to the specified Line Module (LM).</p> </div>
8	<p>For PKT/OTN circuit packs, each module with an “Oper State” of “Enabled*”:</p> <ul style="list-style-type: none"> • Issue the CLI command “module show slot <LM>”. • Issue the “module reload slot <LM>” command if “reload to restore config integrity” is indicated for the “OperState”. <p>Once the integrity of all LMs is restored, the alarm will be cleared.</p> <p>If the module reload fails, “module show slot <LM>” for that LM will continue to show “reload to restore config integrity”.</p>
9	<p>If the module reload fails multiple times, cold restart the Line Module to restore integrity. The command output will show “cold restart to restore config integrity” in this case.</p>

Procedure 5-117 (continued)
Packet Configuration Integrity Fail

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

—end—

Procedure 5-118 **Packet Rate Limit Exceeded**

Alarm ID: 591

Probable cause

This event is raised when the aggregate number of packets received by the shelf processor (SP) system during each time period crosses a pre-determined threshold. The event is raised to warn that the CPU can be locked up due to the high receiving packet rate. Network issues such as broadcast storms are the most common causes of this event.

Conditions that can trigger this alarm include:

- network issues such as broadcast storms
 - internal faults such as a babbling module
 - load delivery, particularly on gateway network element (GNE) shelves that use software forwarding, including NAT and Private-IP configurations

Impact

Warning

Step	Action						
1	In general, no action is required. The network element communications software clears this alarm automatically when the receiving packets rate is lower than the threshold or when load deliveries complete.						
2	<table border="1"><thead><tr><th data-bbox="533 1174 580 1184">If</th><th data-bbox="824 1174 868 1184">Then</th></tr></thead><tbody><tr><td data-bbox="533 1208 788 1216">this is a network issue</td><td data-bbox="824 1208 1317 1262">examine the network configuration, and identify and remove the trouble traffic source (for example, a broadcast storm)</td></tr><tr><td data-bbox="533 1275 788 1286">the alarm does not clear</td><td data-bbox="824 1275 1317 1330">it can be an internal fault. Contact your next level of support or your Ciena support group.</td></tr></tbody></table>	If	Then	this is a network issue	examine the network configuration, and identify and remove the trouble traffic source (for example, a broadcast storm)	the alarm does not clear	it can be an internal fault. Contact your next level of support or your Ciena support group.
If	Then						
this is a network issue	examine the network configuration, and identify and remove the trouble traffic source (for example, a broadcast storm)						
the alarm does not clear	it can be an internal fault. Contact your next level of support or your Ciena support group.						

—end—

Procedure 5-119

Packet Rate Limit Exceeded - CPU2

Alarm ID: 1267

Probable cause

This event is raised when the aggregate number of packets received by the shelf processor (SP) system during each time period crosses a pre-determined threshold. The event is raised to warn that the CPU2 can be locked up due to the high receiving packet rate. Network issues such as broadcast storms are the most common causes of this event.

Conditions that can trigger this alarm include:

- network issues such as broadcast storms
- internal faults such as a babbling module
- load delivery, particularly on gateway network element (GNE) shelves that use software forwarding, including NAT and Private-IP configurations

Impact

Warning

Step	Action						
1	In general, no action is required. The network element communications software clears this alarm automatically when the receiving packets rate is lower than the threshold or when load deliveries complete.						
2	<table border="1"> <thead> <tr> <th>If</th> <th>Then</th> </tr> </thead> <tbody> <tr> <td>this is a network issue</td> <td>examine the network configuration, and identify and remove the trouble traffic source (for example, a broadcast storm)</td> </tr> <tr> <td>the alarm does not clear</td> <td>it can be an internal fault. Contact your next level of support or your Ciena support group.</td> </tr> </tbody> </table>	If	Then	this is a network issue	examine the network configuration, and identify and remove the trouble traffic source (for example, a broadcast storm)	the alarm does not clear	it can be an internal fault. Contact your next level of support or your Ciena support group.
If	Then						
this is a network issue	examine the network configuration, and identify and remove the trouble traffic source (for example, a broadcast storm)						
the alarm does not clear	it can be an internal fault. Contact your next level of support or your Ciena support group.						

—end—

Procedure 5-120

Payload Extended Label Mismatch

Alarm IDs: 689, 690

Probable cause

This alarm is raised when the expected extended signal label does not match the received extended signal label of the VT/VC payload.

Impact

Major, service-affecting (M, SA) alarm, if on active path

Minor, non-service-affecting (m, NSA) alarm, if on inactive path

Prerequisites

To perform this procedure, you must

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545
- have an antistatic wrist strap to dissipate electrostatic charges
- have the network 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

Step	Action
1	Verify if there are alarms of higher order from the alarm hierarchy. Refer to the “Alarm hierarchies and alarm severities” chapter in Part 1 of this document.
2	Clear any alarms of higher order using the appropriate procedures.
3	If the original alarm has Then
	cleared the procedure is complete
	not cleared go to step 4
4	Identify the circuit pack raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document.
5	Use the network connection information to identify the transmit and receive ends of the alarmed signal.
6	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.

Procedure 5-120 (continued) **Payload Extended Label Mismatch**

Step	Action	
7	If the network element is not connected to a 6500 network element at the far-end part of a mid-span meet and the far-end network element is from another vendor connected to another 6500 network element	Then go to step 8 step 8 step 9
8	Use the alarm system of the other vendor to find and correct the problem. Go to step 15 .	
9	Log into each of the network elements on the STS/VT/VC path as required, and verify that all cross-connects are correctly provisioned. Make any required changes. Refer to the “Retrieving path connections” procedure in Part 1 of <i>Configuration - Bandwidth and Data Services</i> , 323-1851-320.	
10	If the original alarm has	Then
	cleared	the procedure is complete
	not cleared	go to step 11
11	Retrieve, record and compare the extended signal label messages at the transmit and the receive network elements. Refer to the “Retrieving and editing path provisioning” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.	
12	Ensure that the outgoing extended signal label message (Transmitted) at the transmit end matches the incoming expected extended signal label message (Expected Rx) at the receive end.	
13	Retrieve active alarms from the network element to determine if the original alarm has cleared.	
	If the original alarm has	Then
	cleared	the procedure is complete
	not cleared	go to step 14
14	Replace the circuit pack raising the alarm. Refer to the “Replacing an optical interface circuit pack” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.	
15	If the alarm does not clear, contact your next level of support or your Ciena support group.	

—end—

Procedure 5-121 **Payload Label Mismatch**

Alarm IDs: 12, 51, 59, 116, 191, 240, 275, 455, 456, 2088

Probable cause

This alarm is raised when the incoming signal label does not match the expected signal label. For example, when non-specific mapped STS-1/VC-4 is received and a VT/TUG structured STS-1/VC-4 is expected.

Impact

- Major, service-affecting (M, SA) alarm, if on active path
 - Minor, non-service-affecting (m, NSA) alarm, if on inactive path in a UPSR/SNCP configuration
 - Critical, service-affecting (C, SA) alarm

Prerequisites

To perform this procedure, you must

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545
 - have an antistatic wrist strap to dissipate electrostatic charges
 - have the network 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

Procedure 5-121 (continued)

Payload Label Mismatch

Step	Action	
4	Identify the circuit pack raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document.	
5	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.	
6	Use the network connection information to identify the transmit and receive ends of the alarmed signal.	
7	If the network element is	Then go to
	not connected to a 6500 network element at the far-end	step 8
	part of a mid-span meet and the far-end network element is from another vendor	step 8
	connected to another 6500 network element	step 9
8	Use the alarm system of the other vendor to find and correct the problem. Go to step 15 .	
9	Log into each of the network elements on the STS/VT/VC path as required, and verify that all cross-connects are correctly provisioned. Make any required changes. Refer to the “Retrieving path connections” procedure in Part 1 of <i>Configuration - Bandwidth and Data Services</i> , 323-1851-320.	
10	If the original alarm has	Then
	cleared	the procedure is complete
	not cleared	go to step 11
11	Retrieve and record the signal label messages at the transmit and the receive network. Refer to the “Retrieving and editing path provisioning” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.	
12	Ensure that the outgoing signal label message (Transmitted) at the transmit end matches the incoming expected signal label message (Expected Rx) at the receive end.	
13	If the original alarm has	Then
	cleared	the procedure is complete
	not cleared	go to step 14
14	Replace the circuit pack raising the alarm. Refer to the “Replacing an optical interface circuit pack” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545, and select the proper procedure for the module raising the alarm.	
15	If the alarm does not clear, contact your next level of support or your Ciena support group.	

—end—

Procedure 5-122

PHY Map Mismatch

Alarm IDs: 2021

Probable cause

This alarm is raised on PTP facility of the WLAI circuit pack when received Physical Identification (PID) does not match expected PID. Each OTSi in a Group Identifier (GID) must have a unique PID.

Impact

Critical, service-affecting (C, SA) alarm if not protected
Minor, non-service-affecting (m, NSA) alarm if protected

Prerequisites

To perform this procedure, you must

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0
- use an account with at least a level 3 UPC

Step	Action	
1	Identify the circuit pack or circuit packs raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document.	
2	From the Site Manager Configuration menu, select Equipment & Facility Provisioning . Select the alarmed facility, and record the values from the Rx PID , Trace Tx , and Associated Far End Rx PID columns. Refer to the “Retrieving equipment and facility details” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.	
3	If the Rx PID and Trace Tx values are	Then go to
	not equal	step 4
	equal	step 5
4	There is a likely a misconnected fiber. Verify that the optical fiber connections are correct on the circuit pack raising the alarm and on the upstream circuit pack. The Associated Far End Rx PID value from step 2 indicates where the misconnection exists.	
5	If the alarm does not clear, contact your next level of support or your Ciena support group.	

—end—

Procedure 5-123

Pluggable I/O Carrier 1/2 Fail

Alarm IDs: 1054, 1055

Probable cause

This alarm is raised when a port card (such as 20G L2SS) is provisioned with an associated pluggable I/O carrier 1/2, and the pluggable I/O carrier 1/2 fails, or when the port card detects that the power for the SFPs is not available or under voltage on the pluggable I/O carrier 1/2 after the card has enabled it.

Impact

Major, service-affecting (M,SA) alarm for a pluggable I/O carrier associated with an in-service circuit pack with in-service facilities with cross-connects, unprotected

Minor, non-service-affecting (m, NSA) alarm for a pluggable I/O carrier associated with an out-of-service circuit pack or an in-service circuit pack without cross-connects or protected

Prerequisites

To perform this procedure, you must:

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545
- have an antistatic wrist strap to dissipate electrostatic charges
- obtain a replacement pluggable I/O carrier

Step	Action
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	Replace the failed pluggable I/O carrier with a new one. Refer to the “Replacing the Front I/O Panel (Multi-Service)” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545, for instructions.
3	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-124

Pluggable I/O Carrier 1/2 Missing

Alarm IDs: 1052, 1053

Probable cause

This alarm is raised when a port card (such as a 20G L2SS) is provisioned with an associated pluggable I/O carrier 1/2, and the pluggable I/O carrier 1/2 is missing, or there is a problem with the presence lines to the I/O carrier 1/2 using the pluggable I/O panel or SP.

You may also see this alarm momentarily right after a shelf processor restart. If the alarm condition does not exist, this alarm will clear after a couple of seconds.

Impact

Major, service-affecting (M, SA) alarm for a pluggable I/O carrier associated with an in-service circuit pack with in-service facilities with cross-connects, unprotected

Minor, non-service-affecting (m, NSA) alarm for a pluggable I/O carrier associated with an out-of-service circuit pack or an in-service circuit pack without cross-connects or protected

Prerequisites

To perform this procedure, you must:

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545
- have an antistatic wrist strap to dissipate electrostatic charges
- obtain a supported pluggable I/O carrier

Step	Action
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	Install the required pluggable I/O carrier or replace the existing pluggable I/O carrier with the type that is required by the circuit pack. Refer to the “Replacing the Front I/O Panel (Multi-Service)” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545, for instructions.
3	If the alarm does not clear, contact your next level of support or your Ciena support group.

- | | |
| --- | --- |
| 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 | Install the required pluggable I/O carrier or replace the existing pluggable I/O carrier with the type that is required by the circuit pack. Refer to the “Replacing the Front I/O Panel (Multi-Service)” procedure in *Fault Management - Module Replacement*, 323-1851-545, for instructions. |
| 3 | If the alarm does not clear, contact your next level of support or your Ciena support group. |

—end—

Procedure 5-125

Pluggable I/O Carrier 1/2 Unknown

Alarm IDs: 1056, 1057

Probable cause

This alarm is raised when the port card (such as a 20G L2SS) is provisioned with an associated pluggable I/O carrier 1/2, and the physically present pluggable I/O carrier 1/2 has a PEC not supported by software, or when the SP has problems accessing the I/O carrier 1/2 1-wire EEPROM.

Impact

Major, service-affecting (M, SA) alarm for a pluggable I/O carrier associated with an in-service circuit pack with in-service facilities with cross-connects, unprotected

Minor, non-service-affecting (m, NSA) alarm for a pluggable I/O carrier associated with an out-of-service circuit pack or an in-service circuit pack without cross-connects or protected

Prerequisites

To perform this procedure, you must:

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545
- have an antistatic wrist strap to dissipate electrostatic charges
- obtain a supported pluggable I/O carrier

Step	Action
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	Replace the pluggable I/O carrier with the type that is required by the circuit pack. Refer to the “Replacing the Front I/O Panel (Multi-Service)” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545, for instructions.
3	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-126

Pluggable I/O Panel Mismatch

Alarm ID: 1050

Probable cause

This alarm is raised when a pluggable I/O panel is present but is not the correct type for the 20G L2SS circuit pack.

Impact

Major, service-affecting (M, SA) alarm for a pluggable I/O panel associated with an in-service circuit pack with cross-connects

Minor, non-service-affecting (m, NSA) alarm for a pluggable I/O panel associated with an out-of-service circuit pack or an in-service circuit pack without cross-connects

Prerequisites

To perform this procedure, you must:

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545
- have an antistatic wrist strap to dissipate electrostatic charges
- obtain a supported pluggable I/O panel

Step	Action
1	Identify the 20G L2SS circuit pack raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document. The Unit field in the Active Alarms application specifies the circuit pack and circuit pack slot using the following format: <circuit pack>-slot#
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	Replace the pluggable I/O panel associated with the circuit pack you identified in step 1 with a supported pluggable I/O panel. Refer to the “Replacing the Front I/O Panel (Multi-Service)” procedure in Part 1 of <i>Fault Management - Module Replacement</i> , 323-1851-545.
4	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-127

Pluggable I/O Panel Missing

Alarm ID: 1049

Probable cause

This alarm is raised when a pluggable I/O panel required by the 20G L2SS circuit pack is not present.

Impact

Major, service-affecting (M, SA) alarm for a pluggable I/O panel associated with an in-service circuit pack with cross-connects

Minor, non-service-affecting (m, NSA) alarm for a pluggable I/O panel associated with an out-of-service circuit pack or an in-service circuit pack without cross-connects

Prerequisites

To perform this procedure, you must:

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545
- have an antistatic wrist strap to dissipate electrostatic charges
- obtain a supported pluggable I/O panel for the 20G L2SS circuit pack (refer to the “I/O and protection hardware” section in Part 1 of *Planning*, NTRN10EG)

Step	Action
1	Identify the 20G L2SS circuit pack raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document. The Unit field in the Active Alarms application specifies the circuit pack and circuit pack slot using the following format: <code><circuit pack>-slot#</code>
2	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.

5-312 Alarm clearing procedures—I to Z

Procedure 5-127 (continued)

Pluggable I/O Panel Missing

Step	Action
3	Install a supported pluggable I/O panel associated with the 20G L2SS circuit pack you identified in step 1 . Refer to the “ <i>Replacing the Front I/O Panel (Multi-Service)</i> ” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.
4	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-128

Pluggable I/O Panel Unknown

Alarm ID: 1051

Probable cause

This alarm is raised when an unrecognized I/O panel is installed in a shelf provisioned with 20G L2SS circuit packs.

Impact

Major, service-affecting (M, SA) alarm for a pluggable I/O panel associated with an in-service circuit pack with cross-connects

Minor, non-service-affecting (m, NSA) alarm for a pluggable I/O panel associated with an out-of-service circuit pack or an in-service circuit pack without cross-connects

Prerequisites

To perform this procedure, you must:

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545
- have an antistatic wrist strap to dissipate electrostatic charges
- obtain a supported pluggable I/O panel for the 20G L2SS circuit pack (refer to the “I/O and protection hardware” section in Part 1 of *Planning*, NTRN10EG)

Step	Action
1	Identify the 20G L2SS circuit pack raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document. The Unit field in the Active Alarms application specifies the circuit pack and circuit pack slot using the following format: <code><circuit pack>-slot#</code>
2	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.

5-314 Alarm clearing procedures—I to Z

Procedure 5-128 (continued)

Pluggable I/O Panel Unknown

Step	Action
3	Replace the pluggable I/O panel for the circuit pack you identified in step 1 with a supported pluggable I/O panel. Refer to the “ <i>Replacing the Front I/O Panel (Multi-Service)</i> ” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.
4	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-129

Port Bandwidth Near Limit

Alarm IDs: 692, 693, 694

Probable cause

This alarm is raised when the cumulative CIR provisioned on the facility (as a percentage of the total bandwidth it has available) exceeds the bandwidth utilization threshold setting provisioned on that facility.

This alarm is raised on the L2SS or PDH gateway circuit pack against ETH, WAN or LAG facilities.

Impact

Warning

Prerequisites

To perform this procedure, you require an account with at least a level 3 UPC.

Step	Action	
1	Since this alarm is raised only as a result of a provisioning action, take note of which provisioning actions just occurred. If you are not sure what provisioning caused the alarm, retrieve the security log for the alarmed NE and determine the user and command that has a timestamp within a few seconds of the alarm being raised. Refer to the “Retrieving security logs” procedure in the <i>Administration and Security Technical Publication</i> , 323-1851-301. Contact the user shown to determine the change that was implemented.	
2	If you want to	Then go to
	change the bandwidth threshold	step 3
	reduce the number of Layer-2 connections	step 4
	increase the bandwidth (WAN or LAG ports only)	step 5
3	Increase the bandwidth threshold setting on the facility beyond the percentage of bandwidth currently being used. Refer to the “Editing facility parameters” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.	
	Note: Increasing the bandwidth utilization threshold to 100% will disable the AO entirely.	
	Go to step 6 .	

Procedure 5-129 (continued)

Port Bandwidth Near Limit

Step	Action
4	<p>Reduce the amount of bandwidth on the facility by either removing VCEs or changing the Bandwidth Profiles of the VCEs on the port to use less bandwidth. Refer to the “Deleting virtual circuit endpoints” and “Editing a bandwidth profile” procedures in Part 2 of <i>Configuration - Bandwidth and Data Services</i>, 323-1851-320.</p> <p>Note: If you reduce the number of Layer 2 connections, these connections may need to be added to other ports in the network, which requires re-engineering of network traffic.</p> <p>Go to step 6.</p>
5	<p>In the case of WAN and LAG facilities only, allocate more physical bandwidth to the facility (for example, add cross-connections to a WAN, or add member ports to a LAG). You can only add more bandwidth to WAN if VCAT is enabled. Refer to the “Adding an ETH or ETH10G facility to a LAG in a 20G L2SS, L2SS, PDH gateway, or RPR circuit pack” and “Editing facility parameters” procedures in Part 1 of <i>Configuration - Provisioning and Operating</i>, 323-1851-310.</p> <p>For WAN facilities, refer to the “Adding a path connection” procedure in Part 1 of <i>Configuration - Bandwidth and Data Services</i>, 323-1851-320. For more information on bandwidth allocation, refer to the “Bandwidth and facility management” in <i>6500 Data Application Guide</i>, NTRN15BA.</p>
6	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-130

Power Failure

Alarm IDs:1686

Probable cause

This alarm is raised when the shelf processor detects that low or no voltage exists on the backplane power bus.

This alarm is only applicable to the 7-slot Type 2 shelf equipment with AC Power Input Cards (NTK505RA). This alarm can also be raised against a fused Power Input Card when the fuse cartridge has been removed, or if the indicator fuse is not present on the card and the main fuse has blown.

Impact

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

Critical, Service-affecting (C, SA) alarm

Prerequisites

To perform this procedure, you must

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545
- have an antistatic wrist strap to dissipate electrostatic charges
- have a standard multimeter
- have a spare Power Input Card to replace failed Power Input Card in the shelf

Step	Action
1	Open the Shelf Inventory Site Manager application and verify that the Power Input Card associated with the alarm is listed. Refer to the “Displaying shelf inventory information” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
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	At the shelf faceplate, identify the Power Input Card that is the source of the alarm. If power is not reaching the system through the Power Input Card (due to a tripped breaker or externally disconnected power feed), the “Power OK” LED on the faceplate of the Power Input Card is off.

5-318 Alarm clearing procedures—I to Z

Procedure 5-130 (continued)

Power Failure

Step	Action	
4	If the LED is	Then
	on	contact your next level of support or your Ciena support group.
	off	go to step 5
5	Replace the Power Input Card. Refer to the “Replacing the Power Input Card” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.	
6	If the original alarm is	Then
	cleared	the procedure is complete
	not cleared	go to step 7
7	Replace the shelf processor for the 7-slot Type 2 shelf. Refer to <i>Fault Management - Module Replacement</i> , 323-1851-545.	
8	If the alarm does not clear, contact your next level of support or your Ciena support group.	

—end—

Procedure 5-131

Power Failure - A or Power Failure - B

Alarm IDs: 78, 79

Probable cause

This alarm is raised against a power feed when the shelf processor detects that low or no voltage exists on the A or B 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 with multiple power zones (such as the 32-slot shelf or 14-slot packet-optical shelf when equipped with 2x50A Power Input Card, may affect service if both the A and B feed for a zone have failed.

For a shelf equipped with Fused Power Input Cards, the “Power Failure - Fuse Blown” (m, NSA) alarm is raised against a power feed when its alarm indicator fuse is blown and there is sufficient voltage present on the associated power input terminals. A “Power Failure - Fuse Blown” will mask the “Power Failure - A/B” alarm.

As long as a shelf processor is active, a Power Failure - Low Voltage alarm will be raised to indicate a power brownout when all the power feeds to the shelf have low/no voltage.

Impact

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

Critical, service-affecting (C, SA) alarm

Note that the service-affecting alarm is applicable to the 32-slot shelf and 14-slot packet-optical shelf when equipped with 2x50A power input cards only. More specifically, for the 32-slot shelf and a 2x50A 14-slot configuration, a critical, service-affecting alarm is raised if matching power feeds for Power Input Card A and B are faulty or if only one Power Input Card is present. For all other scenarios, a minor, non-service-affecting alarm is raised.

Prerequisites

To perform this procedure, you must:

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0
- have an antistatic wrist strap to dissipate electrostatic charges
- have a standard multimeter
- have a spare Power Input Card to replace each Power Input Card in the shelf

Procedure 5-131 (continued)

Power Failure - A or Power Failure - B

- have spare main and indicator fuses to replace (if alarm is raised against a fused Power Input Card)

You do not have to replace each Power Input Card with a new Power Input Card. Use a single spare Power Input Card of the correct type to replace each Power Input Card in turn.

Step	Action						
1	<p>Open the Shelf Inventory application and verify that the Power Input Card associated with the alarm is listed. Refer to the “Displaying shelf inventory information” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i>, 323-1851-310.</p> <p>The Power Failure - A alarm is associated with Power Input Card A in slot 17-1 for 14-slot shelf, slot 17 for 6500-7 packet-optical shelf or 7-slot shelf, slot 17 for a 2-slot shelf (NTK503LA shelf variant), and slot 43 for 32-slot shelf. The Power Failure - B alarm is associated with Power Input Card B in slot 17-3 for 14-slot shelf, slot 18 for 6500-7 packet-optical shelf or 7-slot shelf, slot 17 for a 2-slot shelf (NTK503LA shelf variant), and slot 44 for 32-slot shelf. For 2-slot shelf types with integrated AC or DC power inputs, the Power Failure - A and Power Failure - B alarms are raised against the shelf.</p> <p>Note: For 2-slot shelf types (NTK503MAE5 and NTK503NAE5 variants) with integrated AC or DC power inputs, the power supply modules cannot be replaced. If the source of the alarm is not external and an integrated power supply unit has failed, you must replace the shelf. The 2-slot optical Type 2 shelf (NTK503LA) has field replaceable power supplies. See the “2-slot shelf replacement” procedure in the <i>Fault Management - Module Replacement</i>, 323-1851-545.</p>						
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	At the shelf faceplate, identify the Power Input Card that is the source of the alarm. If power is not reaching the system through the Power Input Card (due to a tripped breaker or externally disconnected power feed), the “Power OK” LED on the faceplate of the Power Input Card is off.						
4	<p>If the LED is</p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">on</td> <td style="width: 70%; text-align: right;">step 8</td> </tr> <tr> <td>off</td> <td style="text-align: right;">step 5</td> </tr> </table>	on	step 8	off	step 5		
on	step 8						
off	step 5						
5	<p>If the associated Power Input Card is</p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">fused</td> <td style="width: 70%; text-align: right;">step 6</td> </tr> <tr> <td>breakerless</td> <td style="text-align: right;">step 7</td> </tr> <tr> <td>breakerless</td> <td style="text-align: right;">step 8</td> </tr> </table>	fused	step 6	breakerless	step 7	breakerless	step 8
fused	step 6						
breakerless	step 7						
breakerless	step 8						

Procedure 5-131 (continued)

Power Failure - A or Power Failure - B

Step	Action										
6	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 8 .										
7	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 8 .										
8	<p style="text-align: center;">DANGER</p>  <p>Risk of electrical shock and short circuit</p> <p>Ensure that there is no chance of coming in contact with the power cables of the Power Input Card. Electrical shock or short circuit can result.</p>										
	<p>For the DC power sources, using a multimeter, carefully measure the voltage of the power feed to the alarmed Power Input Card or at the power cable termination between the L- and L+/Return. Test points are available on some power modules for this test. For D-Sub terminated power inputs (such as those found used in 2-slot and 7-slot Type 2 shelves) you can measure the voltage at the shelf-end of the power cable termination. You must disconnect the cable and carefully measure the voltage. Ensure that the polarity as well as the voltage is correct. (-48 V dc or +24 V dc for NTK505TR Power Input Card). For the AC power source, you can measure the power using an AC power tester).</p>										
9	<table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 50%;">If the feed voltage is</th> <th style="width: 50%;">Then</th> </tr> </thead> <tbody> <tr> <td>within the normal input voltage operating range required by:</td> <td style="text-align: center;">go to step 10</td> </tr> <tr> <td> <ul style="list-style-type: none"> • -48/-60 Vdc Power Input Card • 24 Vdc Power Input Card • AC Power Input Card and the polarity is correct </td> <td></td> </tr> <tr> <td>the normal input voltage operating range required by:</td> <td style="text-align: center;">use your company procedure to investigate and correct the fault in the power distribution system. Go to step 3.</td> </tr> <tr> <td> <ul style="list-style-type: none"> • -48/-60 Vdc Power Input Card • 24 Vdc Power Input Card • AC Power Input Card or if the polarity is reversed </td> <td></td> </tr> </tbody> </table>	If the feed voltage is	Then	within the normal input voltage operating range required by:	go to step 10	<ul style="list-style-type: none"> • -48/-60 Vdc Power Input Card • 24 Vdc Power Input Card • AC Power Input Card and the polarity is correct		the normal input voltage operating range required by:	use your company procedure to investigate and correct the fault in the power distribution system. Go to step 3 .	<ul style="list-style-type: none"> • -48/-60 Vdc Power Input Card • 24 Vdc Power Input Card • AC Power Input Card or if the polarity is reversed	
If the feed voltage is	Then										
within the normal input voltage operating range required by:	go to step 10										
<ul style="list-style-type: none"> • -48/-60 Vdc Power Input Card • 24 Vdc Power Input Card • AC Power Input Card and the polarity is correct											
the normal input voltage operating range required by:	use your company procedure to investigate and correct the fault in the power distribution system. Go to step 3 .										
<ul style="list-style-type: none"> • -48/-60 Vdc Power Input Card • 24 Vdc Power Input Card • AC Power Input Card or if the polarity is reversed											
10	Replace the power I/O module. Refer to the “Replacing the Power Input Card A or B” in the <i>Fault Management - Module Replacement</i> , 323-1851-545.										

5-322 Alarm clearing procedures—I to Z

Procedure 5-131 (continued)

Power Failure - A or Power Failure - B

Step	Action	
11	If the original alarm is	Then
	cleared	the procedure is complete
	not cleared	go to step 12
12	Replace the 6500 shelf processor. Refer to the “Replacing the shelf processor” in the <i>Fault Management - Module Replacement</i> , 323-1851-545.	
13	If the original alarm is	Then
	cleared	the procedure is complete
	not cleared	contact your next level of support or Ciena support group

—end—

Procedure 5-132

Power Failure - A (DSM) or Power Failure - B (DSM)

Alarm IDs: 133, 134

Probable cause

This alarm is raised when the DS1 service module (DSM) detects that no voltage exists on the A or B backplane power bus for the DSM.

Impact

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

Prerequisites

To perform this procedure, you must

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545
- have an antistatic wrist strap to dissipate electrostatic charges
- have a multimeter

Step	Action
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	Use a voltmeter to measure the voltage available at the power input connectors. The power input connectors are on the power module accessible from the left side of the DSM.
3	Confirm that at least -44 V dc is on both power inputs and polarity is correct.
If the feed voltage is	
equal to or greater than 44 V dc and the polarity is correct	
less than 44 V dc or reverse polarity	
use your company procedure to investigate and correct the fault in the power distribution system. Go to step 4 .	
4	Check the status of the 5A breaker on the power input board. If the breaker indicates it is tripped, the red breaker button has popped up, press the breaker button back in to reset it. If the breaker will not remain set, go to step 6 . Otherwise, go to step 5 .

5-324 Alarm clearing procedures—I to Z

Procedure 5-132 (continued)

Power Failure - A (DSM) or Power Failure - B (DSM)

Step	Action
5	If the alarm does not clear, replace the OAM module. Refer to the “Replacing DSM-OAM adapter module” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.
6	Contact your next level of support or your Ciena support group.

—end—

Procedure 5-133

Power Failure - Fuse Blown

Alarm ID: 1077

Probable cause

This alarm is raised against a power feed on a fused Power Input Module with a blown alarm indicator fuse as long there is sufficient voltage present on the associated power input terminals.

If there is low or no voltage on the power input terminals, the “Power Failure - Fuse Blown” alarm will be automatically masked and a “Power Failure - A/B” alarm is raised against the feed.

If the blown alarm indicator fuse is physically removed but the fuse cartridge containing a blown main fuse left in place, the “Power Failure - Fuse Blown” alarm will clear and a “Power Failure - A/B” alarm will be raised.

If the blown alarm indicator fuse is physically removed but the fuse cartridge containing a working fuse left in place with sufficient voltage applied to the associated power input terminal, the “Power Failure - Fuse Blown” alarm will clear and no “Power Failure - A/B” alarm will be raised.

If the fuse cartridge containing both the alarm indicator fuse and the main fuse is removed, the “Power Failure - Fuse Blown” alarm will clear and a “Power Failure -A/B” alarm will be raised.

Impact

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

Critical, service-affecting (C, SA) alarm

Prerequisites

To perform this procedure, you must

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0.
- have an antistatic wrist strap to dissipate electrostatic charges
- have spare main and indicator fuses
- have a multimeter

You do not have to replace each fuse with a new fuse. Use a single spare fuse of the correct type to replace each fuse in turn.

Procedure 5-133 (continued)

Power Failure - Fuse Blown

Step	Action
1	Open the Shelf Inventory application and verify that the Power Input Module associated with the alarm is listed. Refer to the “Displaying shelf inventory information” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
2	Identify the Power Input Module that is the source of the alarm. Verify that the indicator fuse has blown by visually checking that the colored flag is visible through its viewing window.
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	If the Power OK LED is
	off Then go to
	step 5
	on Then go to
	step 6
5	Remove the fuse cartridge from the Power Input Module and replace the indicator fuse and main fuse with one of the same amperage rating (which should be greater or equal to the provisioned shelf current. Refer to the “Determining the provisioned shelf current value” procedure in the <i>Administration and Security</i> , 323-1851-301). For details on replacing the fuse, refer to the “Replacing the main fuse and indicator fuse on the Fused Power Input Module” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.
	Note: When the fuse cartridge is removed, the Power Failure - Fuse Blown alarm clears and the Power Failure - A or Power Failure - B alarm is raised. This is expected.
6	Replace the indicator fuse and reseat the fuse cartridge in the shelf, making sure it is properly seated. Refer to the “Replacing the main fuse and indicator fuse on the Fused Power Input Module” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.
7	If the "Power OK" LED is
	Then
	on go to step 11
	off and the indicator fuse does not blow go to step 8
	off and the indicator fuse blows there is a shelf power issue or failed power I/O module. Go to step 10 .
8	Using a multimeter, measure the power feed to the alarmed Power Input Module. Test points are available on some power modules for this test. Ensure that the polarity as well as the voltage are correct (-48 V dc).

Procedure 5-133 (continued)

Power Failure - Fuse Blown

Step	Action
9	If the feed voltage is equal to or greater than 44 V dc and the polarity is correct
	Then go to step 10
	less than 44 V dc or reverse polarity use your company procedure to investigate and correct the fault in the power distribution system. Go to step 4 .
10	Replace the power I/O module and all fuses. Refer to the “Replacing the Power Input Module A or B” and “Replacing the main fuse and indicator fuse on the Fused Power Input Module” in <i>Fault Management - Module Replacement</i> , 323-1851-545.
11	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-134

Power Failure - Low Voltage

Alarm ID: 77

Probable cause

This alarm is raised against the shelf when a power brownout occurs because the battery voltage to the shelf drops below a minimum level, approximately -40 V dc.

A brownout occurs at approximately -40 V dc. The shelf remains in brownout state until the voltage rises above -42 V dc. The shelf continues to carry traffic, but without alarm capacity as long as the battery voltage remains below -42 V dc. If the battery voltage drops below approximately -37 V dc, the shelf fails and stops carrying traffic.

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

Critical, service-affecting (C, SA) alarm

The alarm status is critical because it is service-affecting if the battery voltage drops below -37 V dc.

Prerequisites

To perform this procedure, you must

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0
- have an antistatic wrist strap to dissipate electrostatic charges
- have a multimeter

Procedure 5-134 (continued)
Power Failure - Low Voltage

Step	Action						
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	Using a multimeter, measure the power feed to the alarmed Power Input Card. Test points are available on some power modules for this test. Ensure that the polarity as well as the voltage is correct (-48 V dc).						
3	<p>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.</p>						
	<table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; width: 40%;">If the feed supply is</th> <th style="text-align: left; width: 60%;">Then</th> </tr> </thead> <tbody> <tr> <td>equal to or greater than 42 V dc and the polarity is correct</td> <td>go to step 4</td> </tr> <tr> <td>less than 42 V dc or reverse polarity</td> <td>use your company procedure to investigate and correct the fault in the power distribution system. Go to step 4.</td> </tr> </tbody> </table>	If the feed supply is	Then	equal to or greater than 42 V dc and the polarity is correct	go to step 4	less than 42 V dc or reverse polarity	use your company procedure to investigate and correct the fault in the power distribution system. Go to step 4 .
If the feed supply is	Then						
equal to or greater than 42 V dc and the polarity is correct	go to step 4						
less than 42 V dc or reverse polarity	use your company procedure to investigate and correct the fault in the power distribution system. Go to step 4 .						
4	<p>CAUTION Risk of provisioning data loss and traffic loss Ensure that the voltage is correct at the shelf and that all circuit packs are operating correctly before continuing. Replacing the shelf processor on a partially functioning network element can result in a loss of provisioning data and a loss of traffic.</p>						
	Replace the shelf processor. Refer to the procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.						
5	If the alarm does not clear, contact your next level of support or your Ciena support group.						

—end—

Procedure 5-135

Pre-FEC Signal degrade

Alarm IDs: 1174, 1183, 1184, 1444, 1954, 1984, 2019

Probable cause

This alarm is raised when the Rx performance is degrading.

Pre-FEC Signal Degrade threshold is user provisionable so the user can decide the pre-FEC BER threshold level.

Pre-FEC Signal Degrade condition is not an automatic protection switch trigger (unlike the Pre-FEC Signal Fail condition).

Pre-FEC Signal Degrade fault detection time depends on the dBQ setting. Once the fault is detected, there is a 2.5 seconds hold-off time before the Pre-FEC Signal Degrade alarm is raised. The Pre-FEC Signal Degrade fault clear time also depends on the dBQ setting. Once the fault is cleared, there is a 10 seconds hold-on time before the Pre-FEC Signal Degrade alarm is cleared. No signal conditioning is applied when the Pre-FEC Signal Degrade fault is declared. For more information on dBQ values and the corresponding Pre-FEC signal degrade detection/clearing times, refer to the “FEC corrections per second and pre-FEC BER values—PFEC (OTM2 NGM)” table in *Performance Monitoring*, 323-1851-520.

The **Equipment & Facility Provisioning** application of Site Manager allows users to provision/view the Pre-FEC signal degrade threshold level and to view the Pre-FEC BER for a given threshold setting in dBQ. For more information, refer to Part 1 of *Configuration - Provisioning and Operating*, 323-1851-310.

Impact

Major, service-affecting (M, SA) alarm on an active traffic path
Minor, non-service-affecting (m, NSA) alarm if no connections are provisioned or if on the non-active path in a protected configuration

Prerequisites

To perform this procedure, you must:

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0
- have an antistatic wrist strap to dissipate electrostatic charges

Procedure 5-135 (continued)

Pre-FEC Signal degrade

- have the optical fiber connection information (that is how the circuit packs on each network element connect to other network elements)
 - have an optical power meter with the same optical connectors as the network element

Procedure 5-135 (continued)

Pre-FEC Signal degrade

—end—

Procedure 5-136

Pre-FEC Signal Fail

Alarm IDs: 838, 1004, 1173, 1443, 1953, 1983, 2018

Probable cause

This alarm is raised when the Pre-FEC Signal Fail user provisionable threshold has been crossed.

For 8xOTN Flex MOTR and (1+8)xOTN Flex MOTR circuit packs, this alarm is raised when an uncorrectable block error is detected. This means that the FEC setting on the facilities are mismatched.

Impact

Critical, service-affecting (C, SA) alarm if connections are provisioned
Minor, non-service-affecting (m, NSA) alarm if no connections are provisioned

Prerequisites

To perform this procedure, you must:

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0
- have an antistatic wrist strap to dissipate electrostatic charges
- have the optical fiber connection information (that is, how the circuit packs on each network element connect to other network elements)
- have an optical power meter with the same optical connectors as the network element

Step	Action
1	Identify the circuit pack raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document.
2	Confirm that the FEC setting on the ETH100G, OTUTTP, ETTP, PTP, OTM1, OTM2, OTM3, or OTM4 facility is the same at both ends of the link (RS10 (IEEE 802.3bj RS-10), Off, SCFEC (ITU-T G.975 I.4), UFEC (ITU-T G.975 I.7), RS8 (ITU-T G.709 RS-8)). Refer to the “Retrieving equipment and facility details” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
3	Check that the Pre-FEC Signal Fail Threshold value is correctly set. Refer to the “Retrieving equipment and facility details” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.

Procedure 5-136 (continued)

Pre-FEC Signal Fail

Step	Action
4	If the original alarm has Then
	cleared the procedure is complete
	not cleared go to step 5
5	Check the corresponding upstream circuit pack and photonic layer for failures or alarms. Troubleshoot these alarms/failures before proceeding.
6	Using the Site Manager Equipment & Facility Provisioning application under the Configuration menu, retrieve the Rx Actual Power value for the facility reporting the alarm. Refer to the “Retrieving equipment and facility details” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
7	With the alarmed facility selected, click on the Ranges button in Site Manager and compare the Rx Actual Power value from the facility with the Rx minimum power and Rx maximum power values displayed.
8	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
9	Ensure the signal optical power level into the Rx interface is within the specification reported. If not, check the Photonic layer equipment, the fiber, and fiber cleanliness between the photonic layer equipment and the port reporting the alarm. If unable to get the Rx Actual value to a level that is within specifications, contact your next level of support or Ciena support group.
10	If the original alarm has Then
	cleared the procedure is complete
	not cleared replace the circuit pack reporting the alarm. Refer to the “Replacing an optical interface circuit pack” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.
11	If the original alarm has Then
	cleared the procedure is complete
	not cleared replace the upstream circuit pack. Refer to the “Replacing an optical interface circuit pack” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.
12	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-137

Primary License Server Unavailable

Alarm ID: 2011

Probable cause

This alarm is raised when the 6500 shelf cannot communicate with the primary license server/manager.

Impact

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

Step	Action
1	Verify the network connection between the 6500 shelf and the license server/manager.
2	If you are using HTTPS, the correct date and time must be set on the shelf (either manually or using TOD/NTP server provisioning and synchronization). Refer to “Provisioning Time of Day servers” and “Operating a time of day synchronization” procedure in <i>Administration and Security</i> , 323-1851-301.
3	If you set the time after provisioning licensing, then perform a manual audit after setting the shelf time to clear the license server comms error. Refer to “Operating a license audit on the 6500” procedure in <i>Administration and Security</i> , 323-1851-301.
4	Verify that the primary license server/manager is provisioned and is not down. Refer to “Provisioning License Manager/Server information on the 6500” procedure in <i>Administration and Security</i> , 323-1851-301.
5	It can take up to 12 hours for the alarm to clear as, in steady state, the heartbeat is run every 12 hours. Run a manual audit which will reset the heartbeat to two minutes after which the heartbeat interval will gradually increase in time to the steady state time of 12 hours. Refer to “Operating a license audit on the 6500” procedure in <i>Administration and Security</i> , 323-1851-301.
	Note: An audit cannot clear the alarm when there is no primary license server provisioned on an NE even if a license server is up, running and populated with licenses.
	The alarm will clear two minutes after the manual audit is run.
6	Verify that the primary license server/manager is provisioned and is not down. Refer to “Provisioning License Manager/Server information on the 6500” procedure in <i>Administration and Security</i> , 323-1851-301.
7	If the alarm does not clear, contact your next level of support or Ciena support group.

—end—

Procedure 5-138

Primary RADIUS Accounting Server Unavailable

Alarm ID: 1516

Probable cause

This alarm is raised when no response is received from the primary RADIUS accounting server during user-provisioned timeout.

This alarm is also raised when the RADIUS accounting server provisioning on the network element is incorrect.

This security alarm is raised against a SP, SP-2, SPAP, SPAP-2 w/2xOSC, or an integrated shelf processor on the 8xOTN Flex MOTR circuit pack.

This alarm is raised for an IPv4 and/or IPv6 provisioned server. IPv6 must be enabled if an IPv6 server is provisioned and IPv4 must be enabled if an IPv4 server is provisioned.

Impact

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

Prerequisites

To perform this procedure, you require an account with at least a level 4 UPC.

Step	Action
1	Disable the server on 6500.
2	Re-enable the server and log in or log out of the server.
3	If the alarm is raised again, disable the RADIUS accounting feature and log in or log out of the server.
4	If the alarm is raised, ensure the following RADIUS accounting server provisioning values on the network element are correct: <ul style="list-style-type: none">• server IP address• server port• shared secret• timeout - If this value is too small, the server may not be able to respond quickly enough.
	Refer to the “Provisioning the primary or secondary RADIUS server” procedure in <i>Administration and Security</i> , 323-1851-301.
5	Check the status of the RADIUS accounting server. Ensure the status is ON.

Procedure 5-138 (continued)**Primary RADIUS Accounting Server Unavailable**

Step	Action
6	Log in or log out of the network element. This will send a RADIUS accounting message to all provisioned RADIUS accounting servers. The alarm will clear if a response is received from the server(s) within the provisioned timeout.
7	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-139

Primary RADIUS Server Unavailable

Alarm ID: 583

Probable cause

This alarm is raised when all requests to the primary RADIUS server of a shelf processor times out and a secondary RADIUS server is provisioned. If only the primary RADIUS server is provisioned (no secondary RADIUS server provisioned) and all requests time out, the All Provisioned RADIUS servers Unavailable alarm is raised (refer to the “All Provisioned RADIUS Servers Unavailable” alarm clearing procedure in Part 1 of this document).

This alarm is raised for an IPv4 and/or IPv6 provisioned server. IPv6 must be enabled if an IPv6 server is provisioned and IPv4 must be enabled if an IPv4 server is provisioned.

The alarm is not raised due to a server time out.

Impact

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

Prerequisites

To perform this procedure, you require an account with at least a level 4 UPC.

Step	Action
1	Make sure the primary RADIUS server of the shelf processor is enabled and has a valid IP address. Refer to the “Retrieving the centralized security administration details” procedure in <i>Administration and Security</i> , 323-1851-301.
2	Use your company information and confirm the following provisioned information is correct: <ul style="list-style-type: none">• The primary RADIUS server of the shelf processor is enabled.• The proper primary RADIUS server IP address is provisioned.• The proper shared secret for the primary RADIUS server is provisioned.• The proper timeout value for the primary RADIUS server is provisioned.• For Private IP networks, ensure the proper RADIUS proxy server settings are provisioned.

Procedure 5-139 (continued)

Primary RADIUS Server Unavailable

Step	Action
	Refer to the following procedures under “Procedures and options for centralized security administration” in the <i>Administration and Security</i> , 323-1851-301. <ul style="list-style-type: none">• Provisioning the primary or secondary RADIUS Server• Changing the shared secret for the RADIUS server• Editing the RADIUS proxy server settings
3	Log into the network element again using the RADIUS authentication (centralized security administration).
4	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-140

Primary Shelf Unreachable

Alarm ID: 716

Probable cause

This alarm is raised on a member shelf of a consolidated node when the member shelf cannot communicate with its primary shelf.

Impact

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

Prerequisites

To perform this procedure, you must:

- use an account with at least a level 3 UPC
- have the IP address of all shelves within the consolidated node
- have a network plan, or other documentation identifying shelf provisioning within the consolidated node

Step	Action						
1	Using company records, locate the primary shelf associated with the member shelf raising the alarm. Log into the primary shelf with Site Manager to confirm the shelf is running correctly. Direct access using the SP LAN-15 port may be required to log in. Refer to the “Logging in to a network element using a remote network connection” or “Logging into a network element using a direct network connection to the LAN port on the shelf processor” procedures in <i>Administration and Security</i> , 323-1851-301.						
2	Connect to and log into the 6500 CLI interface of the primary shelf. Refer to the “Starting a 6500 CLI session” procedure in <i>Administration and Security</i> , 323-1851-301. At the 6500 CLI, issue a PING x.x.x.x command where x.x.x.x is the IP address of the remote shelf raising the alarm. Refer to the “Using the ping command” in <i>Administration and Security</i> , 323-1851-301.						
	<table><thead><tr><th>If the ping is</th><th>Then go to</th></tr></thead><tbody><tr><td>successful</td><td>step 7</td></tr><tr><td>unsuccessful</td><td>step 3</td></tr></tbody></table>	If the ping is	Then go to	successful	step 7	unsuccessful	step 3
If the ping is	Then go to						
successful	step 7						
unsuccessful	step 3						
3	There is a communications issue between the two shelves. At a consolidated node, all shelves should be connected using ILAN cables. The shelves can be connected in a linear chain with all router types and the OSPF router type may be connected in a ring. Locate and log into all the shelves that are part of the consolidated node.						

Procedure 5-140 (continued)

Primary Shelf Unreachable

Step	Action				
4	Physically check all ILAN cables and ports. The port connection LED should be on for all ports with a cable plugged in. If they are not, confirm that the cabled ILAN ports have been added on the Communications Interfaces LAN window and on the Communications Interfaces IP window. Confirm that Router circuits have been added for the cabled ports in Communications Routers (either OSPF or ISIS circuits, depending on router type). Refer to the “Retrieving communications settings” in Part 1 of the <i>Configuration - Provisioning and Operating</i> , 323-1851-310.				
5	Clear any communications alarms that are raised against the ILAN ports, such as Link Down or OSPF alarms.				
6	If the original alarm has Then <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 40%;">cleared</td> <td style="width: 60%;">the procedure is complete</td> </tr> <tr> <td>not cleared</td> <td>go to step 7</td> </tr> </table>	cleared	the procedure is complete	not cleared	go to step 7
cleared	the procedure is complete				
not cleared	go to step 7				
7	Log into the Primary shelf with Site Manager. Direct access using the SP LAN-15 port may be required to log in. Refer to the “Logging in to a network element using a remote network connection” or “Logging into a network element using a direct network connection to the LAN port on the shelf processor” in <i>Administration and Security</i> , 323-1851-301.				
8	Retrieve the Node Information table. Refer to the “Displaying node information” in the node information procedures in <i>Administration and Security</i> , 323-1851-301.				
9	Identify which shelf/shelves is/are causing the alarm. These are the shelves where the secondary state parameter for the unreachable shelf indicates “Unreachable”. The affected shelf may have '(?)' next to its shelf number and be highlighted in cyan.				
10	If within the consolidated node Then <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 40%;">only some member shelves displays a fault</td> <td style="width: 60%;">the issue is likely those member shelves. Go to step 11.</td> </tr> <tr> <td>all member shelves display the same fault</td> <td>the issue is likely with the primary shelf. Go to step 12.</td> </tr> </table>	only some member shelves displays a fault	the issue is likely those member shelves. Go to step 11 .	all member shelves display the same fault	the issue is likely with the primary shelf. Go to step 12 .
only some member shelves displays a fault	the issue is likely those member shelves. Go to step 11 .				
all member shelves display the same fault	the issue is likely with the primary shelf. Go to step 12 .				
11	Directly log into the affected member shelf (shelves), and ensure all provisioning required for the member shelf of a consolidated node to operate is correct and without issue. Direct shelf access may be required. Refer to the “Consolidated node (TIDc)” section and the “Logging into a network element using a direct network connection to the LAN port on the shelf processor” procedure in <i>Administration and Security</i> , 323-1851-301, for more information.				

Procedure 5-140 (continued)

Primary Shelf Unreachable

Step	Action				
	<p>For example, verify and if necessary correct:</p> <ul style="list-style-type: none"> • Confirm that the shelf has a unique logical shelf number. • Confirm that the shelf TID matches with primary shelf. • Confirm that the TID consolidation option is enabled. • Confirm that the primary shelf is disabled. <p>Go to step 13.</p>				
12	<p>Directly log into the primary shelf, and ensure all provisioning required for the primary shelf of a consolidated node to operate is correct and without issue. Direct shelf access may be required. For example, verify and if necessary correct:</p> <ul style="list-style-type: none"> • Confirm that the shelf has a unique logical shelf number. • Confirm that the shelf TID matches with member shelves. • Confirm that the TID consolidation option is enabled. • Confirm that the primary shelf is enabled. 				
13	<p>If the original alarm has Then</p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">cleared</td> <td>the procedure is complete</td> </tr> <tr> <td>not cleared</td> <td>go to step 14</td> </tr> </table>	cleared	the procedure is complete	not cleared	go to step 14
cleared	the procedure is complete				
not cleared	go to step 14				
14	<p>Perform a warm restart on the SP of the member shelf(ves). Refer to the “Restarting a circuit pack or shelf processor” in Part 1 of this document. Wait 10 minutes and log back in.</p>				
15	<p>If the original alarm has Then</p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">cleared</td> <td>the procedure is complete</td> </tr> <tr> <td>not cleared</td> <td>go to step 16</td> </tr> </table>	cleared	the procedure is complete	not cleared	go to step 16
cleared	the procedure is complete				
not cleared	go to step 16				
16	<p>Perform a warm restart on the SP of the primary shelf. Refer to the “Restarting a circuit pack or shelf processor” in Part 1 of this document. Wait 10 minutes and log back in.</p>				
17	<p>If the original alarm has Then</p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">cleared</td> <td>the procedure is complete</td> </tr> <tr> <td>not cleared</td> <td>contact your next level of support or Ciena support group</td> </tr> </table>	cleared	the procedure is complete	not cleared	contact your next level of support or Ciena support group
cleared	the procedure is complete				
not cleared	contact your next level of support or Ciena support group				

—end—

Procedure 5-141

Protection Default K-bytes

Alarm IDs: 322, 525, 1126

Probable cause

This alarm is raised when an OC-48/STM-16 or OC-192/STM-64 circuit pack receives a default K-bytes pattern.

This problem arises when a network element is:

- not setup for 2-Fiber/4-Fiber BLSR/MS-SPRing/HERS
- set up for 2-Fiber/4-Fiber BLSR/MS-SPRing/HERS but does not have a 2-Fiber/4-Fiber BLSR/MS-SPRing/HERS configuration

The default K-bytes pattern is detected when the APS bytes are transmitted with the source node ID equal to the destination node ID.

Impact

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

Prerequisites

To perform this procedure, you must

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545
- have an antistatic wrist strap to dissipate electrostatic charges
- use an account with at least a level 3 UPC

Step	Action
1	Identify the circuit pack raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document. The circuit pack raising the alarm is the receiving network element.
2	Verify the 2-Fiber/4-Fiber BLSR/MS-SPRing/HERS provisioning at each node facing the alarmed NE as well as the provisioning on the alarmed NE. Ensure a 2-Fiber/4-Fiber BLSR node map has been added on each node. Refer to the “Accessing the Ring APS Configuration Editor to add a BLSR/MS-SPRing/HERS ring map” and “Editing a BLSR/MS-SPRing configuration for a node” procedures in the BLSR/MS-SPRing/HERS APS provisioning procedures in Part 1 of <i>Configuration - Bandwidth and Data Services</i> , 323-1851-320.

- 1 Identify the circuit pack raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document. The circuit pack raising the alarm is the receiving network element.
- 2 Verify the 2-Fiber/4-Fiber BLSR/MS-SPRing/HERS provisioning at each node facing the alarmed NE as well as the provisioning on the alarmed NE. Ensure a 2-Fiber/4-Fiber BLSR node map has been added on each node. Refer to the “Accessing the Ring APS Configuration Editor to add a BLSR/MS-SPRing/HERS ring map” and “Editing a BLSR/MS-SPRing configuration for a node” procedures in the BLSR/MS-SPRing/HERS APS provisioning procedures in Part 1 of *Configuration - Bandwidth and Data Services*, 323-1851-320.

Procedure 5-141 (continued)

Protection Default K-bytes

—end—

Procedure 5-142 Protection Exerciser Failed

Alarm IDs: 325, 437, 611, 612, 651, 955, 1025, 1110, 1326, 1338, 1707

Probable cause

This alarm is raised when the protection exerciser has failed to complete the exercise routine on the selected facilities.

This alarm is caused by one of the following conditions:

- a faulty circuit pack
- the exerciser is running somewhere else in the 2-Fiber/4-Fiber BLSR/MS-SPRing/HERS or 1+1/MSP linear far-end network is unprotected

Note: The “Protection Exerciser Failed” alarm will not be raised in the following scenarios:

- A scheduled Protection Exerciser will not raise this alarm if an active protection switch is present in the ring (the scheduled protection exerciser will fail silently). The number of protection exerciser runs will still be decremented if the exerciser run count is not set to Indefinitely.
- A manual Protection Exerciser is denied if there is an active protection switch present in the ring. No alarm is raised.

Impact

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

Prerequisites

To perform this procedure, you require an account with at least a level 3 UPC.

Procedure 5-142 (continued)

Protection Exerciser Failed

Step	Action	
1	Ensure that there is no active protection switch on the 2-Fiber/4-Fiber BLSR/MS-SPRing/HERS or 1+1/MSP linear 1+1 TPT configuration. Refer to the “Retrieving protection status details” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.	
	If protection switches on the 2-Fiber/4-Fiber BLSR/MS-SPRing/HERS or 1+1/MSP linear are	Then go to
	idle	step 2
	not idle	step 7
2	Verify if any exerciser is scheduled to run on another network element in the 2-Fiber/4-Fiber BLSR/MS-SPRing/HERS or 1+1/MSP linear configuration at approximately the same time. Exercisers on the same protection entity should have staggered schedules. Refer to the “Retrieving the exerciser schedule” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.	
3	If the exerciser is running on another network element in the 2-Fiber/4-Fiber BLSR/MS-SPRing/HERS or 1+1/MSP linear configuration, inhibit the exerciser. Refer to the “Running/inhibiting the exerciser in the protection exerciser” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.	
4	If the Protection Channel Match Fail alarm is active (indicating a potential crossed fiber), follow the alarm clearing procedure in this document to clear the alarm.	
5	Initiate the exerciser on the selected equipment. Refer to the “Running/inhibiting the exerciser” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.	
6	If the alarm does not clear, contact your next level of support or your Ciena support group. The procedure is complete.	

Procedure 5-142 (continued)
Protection Exerciser Failed

Step	Action
7	<p>If an auto switch is active, find and clear any of the following alarms if active:</p> <ul style="list-style-type: none"> • OC/STM, STS/HO VC and VT/LO VC facility <ul style="list-style-type: none"> — AIS (OC/STM) — Loss of Frame (OC/STM) — Loss Of Signal (OC/STM) — Signal Fail (OC/STM) — Trace Identifier Mismatch (STS/HO VC and VT/LO VC) — Protection Switch Active — OTM0, OTM1, OTM2, OTM3, OTM4Loss of Frame — Loss Of Signal — ODU AIS — ODU LCK — ODU OCI — OPU AIS — OTU Loss of Multiframe — OTU Pre-FEC Signal Fail — OTU Trace Identifier Mismatch — Protection Switch Active <p>Ensure all line alarms and auto-switches are cleared before continuing.</p>
8	Release all user-initiated protection switches. Refer to the “Releasing a protection switch” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
9	If the wait-to-restore is active, a Wait-to-Restore event active is raised against the 2-Fiber/4-Fiber BLSR/MS-SPRing/HERS or 1+1/MSP linear configuration. Wait for the event to clear.
10	Initiate the exerciser on the selected equipment. Refer to the “Running/inhibiting the exerciser” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
11	If the alarm does not clear, go to step 2 .

—end—

Procedure 5-143 **Protection Exerciser Failed Protection**

Alarm ID: 626

Probable cause

This alarm is raised when the 1:N protection exerciser for the 63xE1, 24xDS3/EC-1, 24xDS3/E3 or 16xSTM-1e circuit packs has detected failure in one of the protection switching components. The alarm is raised against the working circuit pack, but refers to a problem with the traffic path to the protection circuit pack.

This alarm is caused by one of the following conditions:

- faulty protection circuit pack
 - faulty protection sub-module (63xE1)
 - faulty I/O panel (I/O module for the 14-slot metro front electrical shelf)
 - Active protection switch

Impact

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

Prerequisites

To perform this procedure, you must

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545
 - have an antistatic wrist strap to dissipate electrostatic charges
 - use an account with at least a level 3 UPC

Step	Action				
1	<p>Ensure that there is no active protection switch on the 1:N configuration. Refer to the “Retrieving protection status details” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i>, 323-1851-310.</p> <p>If protection switches on the 1:N configuration are</p> <table><tr><td data-bbox="530 1535 605 1543">not idle</td><td data-bbox="1108 1535 1196 1543">step 2</td></tr><tr><td data-bbox="530 1579 566 1588">idle</td><td data-bbox="1108 1579 1196 1588">step 6</td></tr></table>	not idle	step 2	idle	step 6
not idle	step 2				
idle	step 6				

Procedure 5-143 (continued)

Protection Exerciser Failed Protection

Procedure 5-143 (continued)

Protection Exerciser Failed Protection

Step	Action						
12	<p>Wait for the Protection Sub-module Missing alarm to clear, then:</p> <ul style="list-style-type: none"> a. Release the lockout of protection on the 63xE1 working circuit pack performed in step 7. b. Run the protection exerciser again on the 63xE1 working circuit pack identified in step 6. <p>The protection exerciser will not run if there is a protection switch active on any of the other 63xE1 working circuit packs in the working group.</p> <p>The alarm can clear autonomously if the exerciser is set to run autonomously.</p>						
13	<table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 30%;">If the original alarm has</th> <th style="width: 70%;">Then</th> </tr> </thead> <tbody> <tr> <td>cleared</td> <td>the original protection sub-module was faulty. The procedure is complete.</td> </tr> <tr> <td>not cleared</td> <td>go to step 14</td> </tr> </tbody> </table>	If the original alarm has	Then	cleared	the original protection sub-module was faulty. The procedure is complete.	not cleared	go to step 14
If the original alarm has	Then						
cleared	the original protection sub-module was faulty. The procedure is complete.						
not cleared	go to step 14						
14	<p>Replace the 63xE1, 24xDS3/EC-1, 24xDS3/E3 or 16xSTM-1e protection circuit pack associated with the 63xE1, 24xDS3/EC-1, 24xDS3/E3 or 16xSTM-1e working circuit pack identified in step 6. Refer to the “Replacing the 63xE1 or 16xSTM-1e working or protection circuit packs” or “Replacing the 24xDS3/EC1 or 24xDS3/E3 circuit pack” procedures in <i>Fault Management - Module Replacement</i>, 323-1851-545.</p>						
15	<p>Run the protection exerciser on the 63xE1, 24xDS3/EC-1, 24xDS3/E3 or 16xSTM-1e working circuit pack identified in step 6.</p> <p>The protection exerciser will not run if there is a protection switch active on any of the other 63xE1, 24xDS3/EC-1, 24xDS3/E3 or 16xSTM-1e working circuit packs in the working group.</p> <p>The alarm can clear autonomously if the exerciser is set to run autonomously.</p>						
16	<table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 30%;">If the original alarm has</th> <th style="width: 70%;">Then</th> </tr> </thead> <tbody> <tr> <td>cleared</td> <td>the procedure is complete</td> </tr> <tr> <td>not cleared</td> <td>go to step 17</td> </tr> </tbody> </table>	If the original alarm has	Then	cleared	the procedure is complete	not cleared	go to step 17
If the original alarm has	Then						
cleared	the procedure is complete						
not cleared	go to step 17						
17	<p>Replace the I/O panel/module associated with the 63xE1, 24xDS3/EC-1, 24xDS3/E3 or 16xSTM-1e working circuit pack identified in step 6. Refer to the “Replacing the DS3/E3/EC1 or 32xSTM-1e front I/O panel” procedure in <i>Fault Management - Module Replacement</i>, 323-1851-545.</p>						

**CAUTION****Risk of loss of traffic**

Replacing the I/O panel/module is traffic affecting. Take the necessary actions before replacing the I/O panel/module.

Procedure 5-143 (continued)

Protection Exerciser Failed Protection

Step	Action				
18	Run the protection exerciser on the 63xE1, 24xDS3/EC-1, 24xDS3/E3 or 16xSTM-1e working circuit pack identified in step 6 . The protection exerciser will not run if there is a protection switch active on any of the other 63xE1, 24xDS3/EC-1, 24xDS3/E3 or 16xSTM-1e working circuit packs in the working group. The alarm can clear autonomously if the exerciser is set to run autonomously.				
19	If the original alarm has Then <hr/> <table><tr><td>cleared</td><td>the procedure is complete</td></tr><tr><td>not cleared</td><td>go to step 20</td></tr></table>	cleared	the procedure is complete	not cleared	go to step 20
cleared	the procedure is complete				
not cleared	go to step 20				
20	Contact your next level of support or your Ciena support group.				

—end—

Procedure 5-144 Protection Exerciser Failed Working

Alarm ID: 567

Probable cause

This alarm is raised when the 1:N protection exerciser for the 63xE1, 24xDS3/EC-1, 24xDS3/E3 or 16xSTM-1e circuit packs has detected a failure in one of the protection switching components. The alarm is raised against the working circuit pack. The alarm indicates a problem with the signals going to the working circuit pack that is not observed with the same signals bridged to the protection circuit pack.

ATTENTION

If the protection exerciser is set to run autonomously, traffic is automatically switched to the protection circuit pack.

This alarm is caused by one of the following conditions:

- a faulty working circuit pack
- a faulty working sub-module (63xE1)
- a faulty I/O panel (I/O module for 14-slot metro front electrical shelf)

Impact

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

Prerequisites

To perform this procedure, you must

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545
- have an antistatic wrist strap to dissipate electrostatic charges
- use an account with at least a level 3 UPC

Procedure 5-144 (continued)

Protection Exerciser Failed Working

Step	Action
1	Ensure that there is no active protection switch on the 1:N configuration. Refer to the “Retrieving protection status details” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
	If protection switches on the 1:N configuration are
	not idle
	Then go to step 2
	idle
	Then go to step 6
2	Release all user-initiated protection switches. Refer to the “Releasing a protection switch” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
3	If the wait-to-restore is active, the 1:N configuration in the Protection Status application will show the wait to restore protection state is active. Wait for the wait to restore protection state to clear.
4	Initiate the exerciser on the selected equipment. Refer to the “Running/inhibiting the exerciser” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
5	If the original alarm has
	cleared
	Then the procedure is complete
	not cleared
	Then go to step 6
6	Identify the circuit pack raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document.
7	If the shelf is
	metro front electrical
	Then go to step 13
	otherwise
	Then go to step 8
8	If the working circuit pack is
	63xE1
	Then go to step 9
	otherwise
	Then go to step 13
9	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
10	Replace the protection sub-module associated with the 63xE1 working circuit pack identified in step 6. Refer to the “Replacing the 63xE1 or 16xSTM-1e working or protection circuit packs” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.

Procedure 5-144 (continued)

Protection Exerciser Failed Working

Step	Action				
11	<p>Wait for the Protection Sub-module Missing alarm to clear, then:</p> <p>Run the protection exerciser again on the 63xE1 working circuit pack identified in step 6. Refer to the “Running/inhibiting the exerciser” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i>, 323-1851-310.</p> <p>The protection exerciser will not run if there is a protection switch active on any other 63xE1 working circuit packs in the working group.</p> <p>The alarm can clear autonomously if the exerciser is set to run autonomously.</p>				
12	<p>If the original alarm has Then</p> <table> <tr> <td>cleared</td> <td>the original protection sub-module was faulty. The procedure is complete.</td> </tr> <tr> <td>not cleared</td> <td>go to step 13</td> </tr> </table>	cleared	the original protection sub-module was faulty. The procedure is complete.	not cleared	go to step 13
cleared	the original protection sub-module was faulty. The procedure is complete.				
not cleared	go to step 13				
13	<p>Replace the 63xE1, 24xDS3/EC-1, 24xDS3/E3 or 16xSTM-1e working circuit pack identified in step 6. Refer to the “Replacing the 63xE1 or 16xSTM-1e working or protection circuit packs” or “Replacing the 24xDS3/EC1 or 24xDS3/E3 circuit pack” procedures in <i>Fault Management - Module Replacement</i>, 323-1851-545.</p> <p>The Protection Exerciser Failed Working alarm will clear when the working circuit pack is removed.</p>				
14	<p>Run the protection exerciser on the 63xE1, 24xDS3/EC-1, 24xDS3/E3 or 16xSTM-1e working circuit pack identified in step 6. Refer to the “Running/inhibiting the exerciser” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i>, 323-1851-310.</p> <p>Note: The alarm can be raised autonomously after replacing the working circuit pack, if the exerciser is set to run autonomously.</p>				
15	<p>If the original alarm has Then</p> <table> <tr> <td>cleared</td> <td>the procedure is complete</td> </tr> <tr> <td>not cleared</td> <td>go to step 16</td> </tr> </table>	cleared	the procedure is complete	not cleared	go to step 16
cleared	the procedure is complete				
not cleared	go to step 16				
16	<p>Replace the I/O panel/module associated with the 63xE1, 24xDS3/EC-1, 24xDS3/E3 or 16xSTM-1e working circuit pack identified in step 6. Refer to the “Replacing the DS3/E3/EC1 or 32xSTM-1e front I/O panel” procedure in <i>Fault Management - Module Replacement</i>, 323-1851-545.</p>				
<div style="border: 1px solid black; padding: 10px; text-align: center;">  <p>CAUTION Risk of loss of traffic Replacing the I/O panel/module is traffic affecting. Take the necessary actions before replacing the I/O panel/module.</p> </div>					

Procedure 5-144 (continued)

Protection Exerciser Failed Working

Step	Action				
17	Run the protection exerciser on the 63xE1, 24xDS3/EC-1, 24xDS3/E3 or 16xSTM-1e working circuit pack identified in step 6 . Refer to the “Running/inhibiting the exerciser” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310. The protection exerciser will not run if there is a protection switch active on any other 63xE1, 24xDS3/EC-1, 24xDS3/E3 or 16xSTM-1e working circuit packs in the working group. The alarm can clear autonomously if the exerciser is set to run autonomously.				
18	If the original alarm has Then <hr/> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">cleared</td> <td style="width: 70%;">the procedure is complete</td> </tr> <tr> <td>not cleared</td> <td>go to step 19</td> </tr> </table>	cleared	the procedure is complete	not cleared	go to step 19
cleared	the procedure is complete				
not cleared	go to step 19				
19	Contact your next level of support or your Ciena support group.				
20	Ensure that there is no active protection switch on the 1:N configuration. Refer to the protection status procedures in <i>Provisioning and Operating Procedures</i> , 323-1851-310. If protection switches on the 1:N configuration are Then go to <hr/> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">not idle</td> <td style="width: 70;">step 21</td> </tr> <tr> <td>idle</td> <td>step 25</td> </tr> </table>	not idle	step 21	idle	step 25
not idle	step 21				
idle	step 25				
21	Check for user switches and auto switches on other working circuit packs. <ul style="list-style-type: none"> • Release all user-initiated protection switches. Refer to the protection status procedures in <i>Provisioning and Operating Procedures</i>, 323-1851-310. • Investigate and clear any auto switches associated with other working circuit packs. <p>Note: Do not attempt to clear an auto switch associated with the circuit pack raising the Protection Exerciser Failed Working alarm as this may have been initiated by the protection exerciser to protect traffic.</p>				
22	If the wait to restore is active, you will see the wait to restore protection state for the 1:N configuration in the Protection Status application. Wait for the wait to restore protection state to clear.				
23	Initiate the exerciser on the selected equipment. Refer to the protection exerciser procedures in <i>Provisioning and Operating Procedures</i> , 323-1851-310.				

Procedure 5-144 (continued)

Protection Exerciser Failed Working

Step	Action
24	Retrieve all alarms to determine if the original alarm has cleared. See “Retrieving active alarms for a network element” procedure in Part 1 of this document.
	If the original alarm Then
	has cleared you have completed the procedure
	has not cleared go to step 25
25	Identify the circuit pack raising the alarm. See “Identifying the circuit pack, XFP/SFP/DPO module/port, or facility that has raised an alarm” procedure in Part 1 of this document.
26	Replace the 63xE1, 24xDS3/EC1, 24xDS3/E3 or 16xSTM1e working circuit pack identified in step 25 . Refer to the equipment replacement procedures in <i>Module Replacement Procedures</i> , 323-1851-545. The Protection Exerciser Failed Working alarm will clear when the working circuit pack is removed.
27	Run the protection exerciser on the 63xE1, 24xDS3/EC1, 24xDS3/E3 or 16xSTM1e working circuit pack identified in step 25 . Note: The alarm may be raised autonomously after replacing the working circuit pack if the exerciser is set to run autonomously.
28	Retrieve all alarms to determine if the alarm has been raised again. See “Retrieving active alarms for a network element” procedure in Part 1 of this document.
	If the alarm Then
	has not been raised again you have completed the procedure
	has been raised again go to step 29
29	Replace the I/O panel (module) associated 63xE1, 24xDS3/EC1, 24xDS3/E3 or 16xSTM1e working circuit pack identified in step 25 . Refer to the equipment replacement procedures in <i>Module Replacement Procedures</i> , 323-1851-545.
	CAUTION  Risk of loss of traffic Replacing the I/O panel is traffic affecting. Take the necessary actions before replacing the I/O panel.

Procedure 5-144 (continued)

Protection Exerciser Failed Working

Step	Action						
30	<p>Run the protection exerciser on the 63xE1, 24xDS3/EC1, 24xDS3/E3 or 16xSTM1e working circuit pack identified in step 25.</p> <p>The protection exerciser will not run if there is a protection switch active on any of the other 63xE1, 24xDS3/EC1, 24xDS3/E3 or 16xSTM1e working circuit packs.</p> <p>The alarm may clear autonomously if the exerciser is set to run autonomously.</p>						
31	<p>Retrieve all alarms to determine if the original alarm has cleared. See “Retrieving active alarms for a network element” procedure in Part 1 of this document.</p> <table style="width: 100%; border-collapse: collapse;"> <tr> <th style="text-align: left; width: 30%;">If the original alarm</th> <th style="text-align: left; width: 70%;">Then</th> </tr> <tr> <td>has cleared</td> <td style="padding-left: 20px;">you have completed the procedure</td> </tr> <tr> <td>has not cleared</td> <td style="padding-left: 20px;">go to step 32</td> </tr> </table>	If the original alarm	Then	has cleared	you have completed the procedure	has not cleared	go to step 32
If the original alarm	Then						
has cleared	you have completed the procedure						
has not cleared	go to step 32						
32	Contact your next level of support or your Ciena support group.						
—end—							

Procedure 5-145 Protection Invalid K-bytes

Alarm IDs: 323, 526, 1127

Probable cause

This alarm is raised when the OC-48/STM-16 or OC-192/STM-64 circuit pack at the far-end ADM network element in the 2-Fiber/4-Fiber BLSR/MS-SPRing/HERS configuration detects a protection request with an invalid APS identifier or an invalid request.

This alarm tracks the following APS codes detected at the receive (Rx) K-bytes on the OC-48/STM-16 or OC-192/STM-64 circuit pack:

- Unused Protection Channel Status (all codes)
- Unsupported Request (all codes)
- Reverse Request (long path indication)

This alarm is caused by one of the following conditions:

- an incorrect provisioning of the ring APS identifiers at the far-end
- an equipment problem at the far-end
- an incorrect fiber-optic cable connections
- provisioning of protection is inconsistent between the alarmed network element and the far-end network element

Impact

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

Prerequisites

To perform this procedure, you must

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545
- have an antistatic wrist strap to dissipate electrostatic charges
- use an account with at least a level 3 UPC

Procedure 5-145 (continued)

Protection Invalid K-bytes

Step	Action	
11	If the original alarm has	Then
	cleared	the procedure is complete
	not cleared	go to step 12
12	At the local network element, reseat the OC-48/STM-16 or OC-192/STM-64 circuit pack raising the alarm. Refer to the “Reseating a circuit pack” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.	
13	If the original alarm has	Then
	cleared	the procedure is complete
	not cleared	go to step 14
14	Replace the local OC-48/STM-16 or OC-192/STM-64 circuit pack. Refer to the “Replacing an optical interface circuit pack” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.	
15	If the alarm does not clear, contact your next level of support or your Ciena support group.	

—end—

Procedure 5-146 Protection Locked

Alarm IDs: 657, 737, 1708

Probable cause

This alarm is raised when a lockout is issued on an SDH-J 1+1, 1+1 port TPT, or 1+1 TPT protected line.

Impact

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

Step	Action
1	Remove the lockout from the protection line. Refer to the “Releasing a protection switch” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
2	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-147

Protection Mode Mismatch

Alarm IDs: 255, 256, 257, 289, 951, 1020, 1106, 1322, 1334, 1393, 1699

Probable cause

This alarm is raised when the received channel protection switching control bytes (APS bytes) on the protection interface circuit pack of a 1+1 OTN, 1+1/MSP linear, or 1+1 TPT configuration show a different protection switch mode than is provisioned on the local network element.

When changing the protection switching mode from 1+1/MSP unidirectional to 1+1/MSP bidirectional, or from 1+1/MSP bidirectional to 1+1/MSP unidirectional, the Protection Mode Mismatch alarm is raised against the node that was changed to, or remained in bidirectional mode.

Impact

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

Prerequisites

To perform this procedure, you require an account with at least a level 3 UPC.

Step	Action
1	Identify the circuit pack raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document.
2	Retrieve the switch mode of the interface pair. Refer to the “Retrieving protection parameters” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
3	Determine the network element and interface modules that are on the remote end of the link.
4	Log into the remote terminal.
5	Retrieve the switch mode of the optical interface pair on the remote terminal. Refer to the “Retrieving protection parameters” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.

Procedure 5-147 (continued)

Protection Mode Mismatch

Step	Action
6	<p>Compare the switch modes reported with each other and with the company records.</p> <ul style="list-style-type: none">• If both optic pairs report the same switch mode, contact your next level of support or your Ciena support group.• If the two switch modes are different, determine from the company records which is correct and change the switch mode of the other optical interface pair. Refer to the “Changing the protection parameters for a pair of facilities or equipment” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i>, 323-1851-310.
7	<p>Note: Changing the protection switch mode for one of the optical interface circuit packs in a pair will automatically change the protection switch mode for the other circuit pack in the pair.</p> <p>If the alarm does not clear, contact your next level of support or your Ciena support group.</p>

—end—

Procedure 5-148

Protection Scheme Mismatch

Alarm IDs: 252, 253, 254, 288, 819, 950, 1021, 1121, 1351, 1374, 1394, 1698

Probable cause

This alarm is raised when the near-end is provisioned as 1+1 and the protection scheme in the received APS bytes indicates a different protection scheme is provisioned on the far-end. This alarm is not indicative of the near-end provisioned as 1+1 and the far-end having no protection scheme provisioned.

Impact

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

Step	Action
1	Identify the circuit pack raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” in Part 1 of this document.
2	Retrieve the protection scheme of the interface pair. Refer to the “Retrieving protection parameters” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
3	Determine the network element and interface modules that are on the remote end of the link.
4	Log into the remote terminal.
5	Retrieve the protection scheme of the optical interface pair on the remote terminal. Refer to the “Retrieving protection parameters” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
6	Compare the protection scheme reported with each other and with the company records. <ul style="list-style-type: none">• If both optic pairs report the same protection scheme, contact your next level of support or your Ciena support group.• If the two protection scheme are different, determine from the company records which is correct and change the protection scheme of the other optical interface pair. Refer to the “Changing the protection parameters for a pair of facilities or equipment” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i>, 323-1851-310.
7	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-149

Protection Sub-module Mismatch

Alarm ID: 607

Probable cause

This alarm is raised when the E1 protection scheme is 1:N and a protection sub-module is present but is not the correct type for the 63xE1 circuit pack.

This alarm does not apply to E1 1:N protection on a 14-slot metro front electrical shelf.

Impact

Major, service-affecting (M, SA) alarm if 1:N protection is provisioned and the 63xE1 protection circuit pack is active

Minor, non-service-affecting (m, NSA) alarm if 1:N protection is provisioned and the 63xE1 protection circuit pack is not active

Prerequisites

To perform this procedure, you must

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545
- have an antistatic wrist strap to dissipate electrostatic charges
- obtain a supported protection sub-module for the 63xE1 circuit pack (refer to the “I/O and protection hardware” section in Part 1 of *Planning*, NTRN10EG)

Step	Action
1	Identify the 63xE1 circuit pack raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document. The Unit field in the Active Alarms application specifies the circuit pack and circuit pack slot using the following format: <circuit pack>-slot#
2	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.

- 1 Identify the 63xE1 circuit pack raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document. The **Unit** field in the **Active Alarms** application specifies the circuit pack and circuit pack slot using the following format: <circuit pack>-slot#
- 2 Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.

Step	Action
3	Replace the protection sub-module for the 63xE1 circuit pack you identified in step 1 with a supported protection sub-module. Refer to the “Replacing I/O protection module” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.
4	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-150

Protection Sub-module Missing

Alarm ID: 608

Probable cause

This alarm is raised when the E1 protection scheme is 1:N and the protection sub-module required by the 63xE1 circuit pack is not present.

This alarm does not apply to E1 1:N protection on a 14-slot metro front electrical shelf.

Impact

Major, service-affecting (M, SA) alarm if 1:N protection is provisioned and the 63xE1 protection circuit pack is active

Minor, non-service-affecting (m, NSA) alarm if 1:N protection is provisioned and the 63xE1 protection circuit pack is not active

Prerequisites

To perform this procedure, you must

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545
- have an antistatic wrist strap to dissipate electrostatic charges
- obtain a supported protection sub-module for the 63xE1 circuit pack (refer to the “I/O and protection hardware” section in Part 1 of *Planning*, NTRN10EG)

Step	Action
1	Identify the 63xE1 circuit pack raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document. The Unit field in the Active Alarms application specifies the circuit pack and circuit pack slot using the following format: <circuit pack>-slot#
2	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.

- 1 Identify the 63xE1 circuit pack raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document. The **Unit** field in the **Active Alarms** application specifies the circuit pack and circuit pack slot using the following format:

<circuit pack>-slot#
- 2 Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.

Procedure 5-150 (continued)

Protection Sub-module Missing

Step	Action
3	Install a protection sub-module for the 63xE1 circuit pack you identified in step 1 . Refer to the “Replacing I/O protection module” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.
4	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-151

Protection Sub-module Unknown

Alarm ID: 609

Probable cause

This alarm is raised when an unrecognized protection sub-module is installed in the shelf. This alarm does not apply to E1 1:N protection on a 14-slot metro front electrical shelf.

Impact

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

The alarm is m, NSA as the module can be operating correctly, but its inventory cannot be read. Payload alarms will signal the degree of the fault.

Prerequisites

To perform this procedure, you must

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545
- have an antistatic wrist strap to dissipate electrostatic charges
- obtain a supported I/O panel for the 63xE1 circuit pack (refer to the “I/O and protection hardware” section in Part 1 of *Planning*, NTRN10EG)

Step	Action
1	Identify the circuit pack raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document. The Unit field in the Active Alarms application specifies the circuit pack using the following format: <circuit pack>-slot#
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	Replace the protection sub-module for the 63xE1 circuit pack you identified in step 1 with a supported protection sub-module. Refer to the “Replacing I/O protection module” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.
4	If the alarm does not clear, contact your next level of support or your Ciena support group.

- | | |
| --- | --- |
| 1 | Identify the circuit pack raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document. The **Unit** field in the **Active Alarms** application specifies the circuit pack using the following format: <circuit pack>-slot# |
- | | |
| --- | --- |
| 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 | Replace the protection sub-module for the 63xE1 circuit pack you identified in [step 1](#) with a supported protection sub-module. Refer to the “Replacing I/O protection module” procedure in *Fault Management - Module Replacement*, 323-1851-545. |
- | | |
| --- | --- |
| 4 | If the alarm does not clear, contact your next level of support or your Ciena support group. |

—end—

Procedure 5-152 Protection Switch Active alarms

Use this procedure to clear alarms associated with active protection switches.

Forced Ring Switch Active

Alarm ID: 473, 474, 808, 1114, 1309

Probable cause

This alarm is raised when a user successfully operates a forced ring switch along a span of a 2-Fiber/4-Fiber BLSR/MS-SPRing/HERS configuration or on a ringlet port RLE. The traffic switches to the protection channels around the ring away from the span. This alarm is cleared when the user releases the forced ring switch, or when a higher priority request overrides it.

For the 10G RPR, this alarm is raised when a forced ring switch is active on a span. This alarm is raised against the WAN facility associated to the span.

Impact

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

Forced Span Switch Active

Alarm ID: 1225, 1226

Probable cause

This alarm is raised when a user successfully operates a forced span switch along a span of a 4-Fiber BLSR/MS-SPRing/HERS configuration. The traffic switches to the protection port for this span only. This alarm is cleared when the user releases the forced span switch, or when a higher priority request overrides it.

Impact

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

Forced Switch Active

Alarm ID: 62, 499, 500, 501, 502, 503, 504, 505, 506, 507, 614, 615, 644, 739, 958, 1014, 1122, 1329, 1341, 1353, 1404, 1405, 1406, 1603, 1704, 1738, 2058, 2080

Probable cause

This alarm is raised when a user successfully operates a forced switch on a 1+1/MSP linear, 1+1 port TPT, 1+1 TPT, UPSR/SNCP, A-SNCP, or 1:N configuration. This alarm is cleared when the user releases the forced switch, or when a higher priority request overrides it.

Impact

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

Procedure 5-152 (continued)

Protection Switch Active alarms

Lockout Active

Alarm ID: 517, 518, 519, 520, 740, 960, 1015, 1124, 1331, 1343, 1355, 1407, 1408, 1409, 1605, 1705, 2059, 2082

Probable cause

This alarm is raised when a user successfully operates a lockout on a 1+1/MSP linear, 1+1 port TPT, or 1+1 TPT configuration. This alarm is cleared when the user releases the lockout request.

Impact

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

Lockout of Protection Active

Alarm ID: 569

Probable cause

This alarm is raised when a user successfully operates a lockout of protection on a 1:N configuration. The alarm is cleared when the user releases the lockout of protection.

The lockout of protection on a 1:N protection circuit pack prevents protection for any working circuit packs in the 1:N protection group.

Impact

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

Lockout of Working Active

Alarm ID: 565

Probable cause

This alarm is raised when a user successfully operates a lockout of working on a 1:N configuration. This alarm is cleared when the user releases the lockout working.

The lockout working prevents a working circuit pack from switching to the protection circuit pack.

Impact

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

Procedure 5-152 (continued)

Protection Switch Active alarms

Lockout Protection Ring Active

Alarm ID: 477, 478

Probable cause

This alarm is raised when a user successfully operates a lockout protection ring on a 2-Fiber BLSR/MS-SPRing configuration. The alarm is cleared when the user releases the lockout of a protection ring.

The lockout of a protection ring on a 2-Fiber BLSR/MS-SPRing prevents ring switching around the ring. The lockout protection ring request overrides any active switches. If traffic is on the protection channels, the switch is dropped and traffic is returned to the working channels (regardless of the condition of the working line). If traffic is on the working channels, no protection switch is performed.

Impact

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

Lockout Working Ring Active

Alarm ID: 479, 480, 1117

Probable cause

This alarm is raised when a user successfully operates a lockout working ring on a 2-Fiber/4-Fiber BLSR/MS-SPRing/HERS configuration. This alarm is cleared when the user releases the lockout working ring.

The lockout working ring prevents the span from switching. The lockout working ring overrides any ring switch along the span and returns traffic to the working channels (regardless of the condition of the working channels). Traffic already using the protection channels on the span due to a ring switch initiated elsewhere continue to use the locked-out span.

Impact

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

Lockout Working Span Active

Alarm ID: 1223, 1224

Probable cause

This alarm is raised when the Lockout Working Span switch is successfully activated against the 4-Fiber BLSR/MS-SPRing/HERS ring configuration.

This alarm is cleared when the user releases the lockout working span.

Procedure 5-152 (continued)

Protection Switch Active alarms

When you operate a lockout of working along a span, you prevent traffic on the working line along the span from using protection span for a span switch and no span switch can occur along the span (ring switches can still be operated). If a span switch is already active along the span, the lockout overrides the switch and the traffic from the protection line returns to the working line regardless of the condition of the working line. However, traffic already using the protection span because a ring switch initiated elsewhere, still uses the locked-out span.

Lockout Protection Span Active

Alarm ID: 1286, 1287

Probable cause

This alarm is raised when the Lockout Protection Span switch is successfully activated against the 4-Fiber BLSR/MS-SPRing/HERS configuration. The alarm is cleared when the user releases the lockout of protection span.

The lockout of protection span on a 4-Fiber BLSR/MS-SPRing/HERS prevents all working traffic around the ring from using this protection span for span or ring switches. Therefore, no span switch can occur along this span and no ring switch can occur around the ring. If any traffic is on the protection port for this span, the lockout overrides the switch and traffic returns to the working port regardless of the condition of the working port. Span switches for other spans along the ring are still valid. If traffic is on the working port, no protection switch is performed.

Impact

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

Manual Ring Switch Active

Alarm ID: 475, 476, 807, 1115, 1310

Probable cause

This alarm is raised when a user successfully operates a manual ring switch along a span of a 2-Fiber/4-Fiber BLSR/MS-SPRing/HERS configuration or on a ringlet port RLE. A manual ring switch command switches traffic from the working channels on the affected span to the protection channels around the ring away from the span. This alarm is cleared when the user releases the manual ring switch, or when a higher priority request overrides it.

For the 10G RPR circuit pack, this alarm is raised when a manual ring switch is active on a span, it is raised against the WAN facility associated to the span.

Impact

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

Procedure 5-152 (continued)

Protection Switch Active alarms

Manual Span Switch Active

Alarm ID: 1227, 1228

Probable cause

This alarm is raised when a user successfully operates a manual span switch along a span of a 4-Fiber BLSR/MS-SPRing/HERS configuration. The traffic switches to the protection port for this span only. This alarm is cleared when the user releases the manual span switch, or when a higher priority request overrides it.

Impact

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

Manual Switch Active

Alarm ID: 67, 508, 509, 510, 511, 512, 513, 514, 515, 516, 616, 617, 645, 738, 959, 1013, 1123, 1330, 1342, 1354, 1401, 1402, 1403, 1604, 1737, 2057, 2081

Probable cause

This alarm is raised when a user successfully operates a manual switch on a UPSR/SNCP, 1+1/MSP Linear, or 1+1 TPT configuration with revertive mode.

This alarm is cleared when the user releases the manual switch, or when a higher priority request overrides it.

Impact

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

Protection Switch Active

Alarm ID: 568

Probable cause

This alarm is raised when traffic is switched to the protection circuit pack in a 1:N configuration. This alarm is cleared when traffic is switched back to the working circuit pack.

For the eMOTR circuit packs, this alarm is raised on the SAOS CLI, when the ring state changes from OK to Recovery/Protecting. The alarm clears when the ring state transitions back to OK. When the alarm is raised and cleared, SNMP trap is sent.

Impact

Warning

Procedure 5-152 (continued)

Protection Switch Active alarms

Prerequisites

To perform this procedure, you require an account with at least a level 2 UPC.

Step	Action
------	--------

Note: 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.

- 1 Release the indicated protection switch. Refer to the “Releasing a protection switch” procedure in Part 2 of *Configuration - Provisioning and Operating*, 323-1851-310.
- 2 If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-153 Protection Switch Complete

Alarm IDs: 490-498, 619, 621, 643, 650, 741, 809, 957, 1023, 1135, 1328, 1340, 1352, 1396

Probable cause

This alarm is raised when a protection switch has completed. For the 10G RPR circuit pack, this alarm is raised against the WAN facility of a span upon which a protection switch has been completed.

For an G.8032 Ethernet Ring Protocol (G.8032 ERP), this alarm is raised when the Ringlet enters either protected state or pending state.

For G.8032 rings provisioned with an infinite wait-to-restore time, the clearing of this alarm is controlled by “G.8032 switch alarm mode” parameter found in the Site Manager Node Information application. Refer to the “Node Information - System parameters” table and “Editing the nodal system parameters” procedure in *Administration and Security*, 323-1851-301 for more information.

ATTENTION

The Protection Switch Complete event for UPSR/SNCP is only enabled for manual switches. If you want to see path switching events, you must set a Path Switch Event parameter to Automatic which will also generate the events for autonomous switches. Refer to the “Node Information - System parameters” table and “Editing the nodal system parameters” procedure in *Administration and Security*, 323-1851-301 for more information.

Impact

Warning

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

Enabled by default

Procedure 5-153 (continued)
Protection Switch Complete

Step	Action								
Note: 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.									
1	Select your first step.								
	<table> <thead> <tr> <th>If</th> <th>Then go to</th> </tr> </thead> <tbody> <tr> <td>the alarm is raised against an G.8032 ERP</td> <td>step 5</td> </tr> <tr> <td>otherwise</td> <td>step 2</td> </tr> </tbody> </table>	If	Then go to	the alarm is raised against an G.8032 ERP	step 5	otherwise	step 2		
If	Then go to								
the alarm is raised against an G.8032 ERP	step 5								
otherwise	step 2								
2	Retrieve the traffic protection status for the alarmed circuit pack. Refer to the “Retrieving protection status details” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310. Note that in an optical link provisioned for bidirectional switching, the switch source may be at the far-end of the link.								
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 alarms by following the appropriate trouble clearing procedure in this document.								
	<table> <thead> <tr> <th>If</th> <th>Then</th> </tr> </thead> <tbody> <tr> <td>no automatic switches are active</td> <td>go to step 4</td> </tr> <tr> <td>the original alarm has cleared</td> <td>this procedure is complete</td> </tr> <tr> <td>the original alarm has not cleared</td> <td>go to step 4</td> </tr> </tbody> </table>	If	Then	no automatic switches are active	go to step 4	the original alarm has cleared	this procedure is complete	the original alarm has not cleared	go to step 4
If	Then								
no automatic switches are active	go to step 4								
the original alarm has cleared	this procedure is complete								
the original alarm has not cleared	go to step 4								
4	Determine if any user request resulted in a dropped protection switch. Check for protection switching alarms. Refer to the “Releasing a protection switch” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.								
	<table> <thead> <tr> <th>If</th> <th>Then</th> </tr> </thead> <tbody> <tr> <td>no user switches are active</td> <td>go to step 5</td> </tr> <tr> <td>the original alarm has cleared</td> <td>this procedure is complete</td> </tr> <tr> <td>the original alarm has not cleared</td> <td>go to step 5</td> </tr> </tbody> </table>	If	Then	no user switches are active	go to step 5	the original alarm has cleared	this procedure is complete	the original alarm has not cleared	go to step 5
If	Then								
no user switches are active	go to step 5								
the original alarm has cleared	this procedure is complete								
the original alarm has not cleared	go to step 5								
5	Select your next step.								
	<table> <thead> <tr> <th>If the ringlet</th> <th>Then go to</th> </tr> </thead> <tbody> <tr> <td>is newly provisioned</td> <td>step 6</td> </tr> <tr> <td>has gone from Idle to Protected state</td> <td>step 11</td> </tr> </tbody> </table>	If the ringlet	Then go to	is newly provisioned	step 6	has gone from Idle to Protected state	step 11		
If the ringlet	Then go to								
is newly provisioned	step 6								
has gone from Idle to Protected state	step 11								

Procedure 5-153 (continued)

Protection Switch Complete

Step	Action
6	Launch the G.8032 ERP Management application under Configuration: Data Services. For each node in the ringlet, verify the provisioning. Refer to the “Retrieving rings and ring ports information in an G.8032 ERP” procedure in Part 3 of <i>Configuration - Bandwidth and Data Services</i> , 323-1851-320.
7	For a major ring, verify that two ringlet ports are provisioned on each node.
8	For a sub-ring, verify that a single Termination ringlet port is provisioned on each of the nodes with the shared segment. Verify that two Tandem ringlet ports are provisioned on all other nodes in the sub-ring.
9	Verify that the Ring ID, RAPS VID and RAPS Type are consistent for all nodes in the ringlet.
10	Verify that an RPL port is provisioned. Go to step 16 .
11	Launch the G.8032 ERP Management application under Configuration: Data Services. Refer to the “Retrieving rings and ring ports information in an G.8032 ERP” procedure in Part 3 of <i>Configuration - Bandwidth and Data Services</i> , 323-1851-320.
12	Select the Ringlet Port Provisioning tab.
13	Use the Ring and Group filter fields to limit the display to the ringlet for which the alarm was raised.
14	Click Retrieve .
15	Observe the Block status for the ringlet ports. A Blocked state on a ringlet port other than the RPL indicates a problem on the facility. Once the problem on the facility is resolved, the alarm should clear after the expiry of the Wait To Restore timer.
16	If the alarm remains active, ensure that no other alarm is active, then contact your next level of support or Ciena support group.

—end—

Procedure 5-154

Protection Switch Complete - Revertive

Alarm IDs: 485, 486, 487, 488, 489, 642, 956, 1022, 1327, 1339, 1397, 1601, 1735

Probable cause

This alarm is raised when the protection mode is provisioned as revertive, and a protection switch has completed.

Impact

Warning

The Protection Switch Complete - Revertive alarm is not enabled by default and must be enabled by the user. To enable the alarm, set the Path Switch Event parameter to User & Auto in the System tab under the Node Information section. see “Editing the nodal system parameters” procedure in *Administration and Security*, 323-1851-301.

Step	Action								
Note: No action is required if a user is performing a test or maintenance operation. This warning is a reminder not to leave a potentially service-affecting condition on the system.									
1	Check the traffic protection status. Refer to the “Retrieving protection status details” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.								
2	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.								
<table> <thead> <tr> <th>If</th> <th>Then</th> </tr> </thead> <tbody> <tr> <td>no automatic switches are active</td> <td>go to step 3</td> </tr> <tr> <td>the original alarm has cleared</td> <td>this procedure is complete</td> </tr> <tr> <td>the original alarm has not cleared</td> <td>go to step 3</td> </tr> </tbody> </table>		If	Then	no automatic switches are active	go to step 3	the original alarm has cleared	this procedure is complete	the original alarm has not cleared	go to step 3
If	Then								
no automatic switches are active	go to step 3								
the original alarm has cleared	this procedure is complete								
the original alarm has not cleared	go to step 3								
3	Determine if a user switch (manual, forced or lockout) is active, release the switch. Refer to the “Releasing a protection switch” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.								
<table> <thead> <tr> <th>If</th> <th>Then</th> </tr> </thead> <tbody> <tr> <td>no user switches are active</td> <td>go to step 4</td> </tr> <tr> <td>the original alarm has cleared</td> <td>this procedure is complete</td> </tr> <tr> <td>the original alarm has not cleared</td> <td>go to step 4</td> </tr> </tbody> </table>		If	Then	no user switches are active	go to step 4	the original alarm has cleared	this procedure is complete	the original alarm has not cleared	go to step 4
If	Then								
no user switches are active	go to step 4								
the original alarm has cleared	this procedure is complete								
the original alarm has not cleared	go to step 4								

Procedure 5-154 (continued)

Protection Switch Complete - Revertive

Step	Action
4	If the alarm remains active, ensure that no other alarm is active.
5	If the alarm does not clear, contact your next level of support or Ciena support group.

—end—

Procedure 5-155 Provisioning Database Freeze Enable

Alarm ID: 1046

Probable cause

This alarm is raised against the shelf after the OPR-DBFRZ command is invoked by the user. All further provisioning commands are blocked. Refer to *TL-1 Description*, 323-1851-190, for more information about the OPR-DBFRZ command.

Impact

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

Prerequisites

To perform this procedure, you require an account with at least a level 3 UPC.

Step	Action
1	Initiate a warm restart on the shelf processor. Refer to the “Restarting a circuit pack or shelf processor” procedure in Part 1 of this document. A warm restart is recommended, even though any type of restart would clear this alarm.
2	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-156

Provisioning Incompatible

Alarm ID: 82

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 for reasons such as the following:

- an MSPP circuit pack is placed in a shelf before a SONET/SDH XC circuit pack is provisioned
- an E1 is placed in a 14-slot optical/rear electrical shelf
- a 24xDS3/EC-1 or 24xDS3/E3 circuit pack is placed in a 14-slot optical shelf
- a 10G circuit pack in slots 1-4, 11-14 for a 14-slot shelf and slot 1 to 8, 11 to 18, 21 to 28, 31 to 38 for a 32-slot shelf is placed in a shelf with a non-160G XC
- a FE electrical circuit pack placed in a 14-slot optical shelf
- provisioning equipment that requires high-flow cooling equipped in a 14-slot shelf when the **Actual cooling capacity** (actual cooling capacity of the shelf) shelf attributes is set to “Low flow”. Refer to the “Equipment provisioning validation based on shelf cooling capacity” section in *Administration and Security*, 323-1851-301 for farther details.
- provisioning equipment with a power consumption value that will cause the **Calculated shelf power** (aggregate shelf power usage) and/or the Calculated shelf zone X power shelf attribute (where “X” is the zone number for a shelf with multiple power zones) to exceed the shelf/zone power threshold limit (calculated from the **Provisioned shelf current** shelf attribute). Refer to the “Equipment provisioning validation based on shelf power capacity” section in *Administration and Security*, 323-1851-301 for farther details.
- a PKT/OTN circuit pack is placed in a shelf before a PKT/OTN XC circuit pack is provisioned
- a PKTOTN is inserted and the SM is not provisioned.

Impact

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

Procedure 5-156 (continued)
Provisioning Incompatible

Prerequisites

To perform this procedure, you must

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0
- have an antistatic wrist strap to dissipate electrostatic charges

Step	Action
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	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 (for example, an electrical circuit pack in an optical shelf, a 40G module in a non-40G shelf). Refer to the “Engineering rules” section in <i>Planning - Ordering information</i> , 323-1851-151, for engineering information on the module.
4	If the circuit pack is not compatible Then 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. Refer to the “Displaying node information” in the <i>Administration and Security</i> , 323-1851-301.
6	Compare the Provisioned and Actual cooling capacity with the required cooling capacity value for the new module. Refer to <i>Planning - Ordering information</i> , 323-1851-151, for engineering information on the module.
7	Confirm the shelf provisioned cooling value is High flow for a circuit pack that requires High flow, or Low flow or High flow for a circuit pack that requires Low flow cooling.
8	If the module is not compatible with the shelf cooling Then replace the cooling module with one that is compatible with the shelf. The procedure is complete. compatible with the shelf cooling go to the next step

Procedure 5-156 (continued)

Provisioning Incompatible

Step	Action
9	If the module is MSPP module compatible with the shelf cooling
	Then go to step 11 step 10
10	Confirm that a Cross-Connect (XC) module is installed in the shelf and that the slot selected is compatible with the installed cross connect. (For example, 10G circuit packs cannot be used in slots 1-4 or 11-14 with a cross connect less than 160G.)
	If the module is compatible with the shelf XC not compatible with the shelf XC
	Then go to step 9 replace the XC with one that is compatible with the shelf. The procedure is complete.
11	Retrieve the shelf power budget and provisioned shelf current. Refer to the “Displaying node information” procedure in the <i>Administration and Security</i> , 323-1851-301.
12	Determine the power requirement of the alarmed module. Refer to the “Technical specifications” chapter in Part 3 of <i>Planning</i> , NTRN10EG.
13	Calculate the worst case shelf available power by multiplying the provisioned shelf current by 43 volts to get total watts available and subtracting the shelf power budget from the calculated available power to get the available power.
14	If the power requirements of the alarmed module are greater than the available power less than the available power
	Then shelf power overload is causing the alarm. Refer to the alarm clearing steps for “ Shelf Power Near Limit ” on page 5-492. contact your next level of support or Ciena support group

—end—

Procedure 5-157

Provisioning Incompatible - Pluggable

Alarm ID: 1136

Probable cause

This alarm is raised when a pluggable is inserted in a supported slot with auto-equip enabled, and the pluggable cannot be provisioned in that slot because the provisioning equipment with a power consumption value will cause the **Calculated shelf power usage** shelf attribute (aggregate shelf power usage) to exceed the shelf power threshold limit (calculated from the **Provisioned shelf current** shelf attribute) or there is other provisioning currently in place which prevents this pluggable from being supported as is.

On a 40G+ CFP OCI circuit pack, if the sum of CFP pluggable “maximum power value” and ACTUALPOWER exceed the shelf power limit threshold, the automatically provisioning of CFP pluggable shall be blocked and the ‘Provisioning Incompatible’ alarm is raised against that port.

Impact

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

Prerequisites

To perform this procedure, you must

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0
- have an antistatic wrist strap to dissipate electrostatic charges

Step	Action
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	Retrieve the shelf power budget and provisioned shelf current. Refer to the “Displaying node information” procedure in the <i>Administration and Security</i> , 323-1851-301.
3	Determine the power requirement of the alarmed pluggable. Refer to the “Technical specifications” chapter in Part 3 of <i>Planning</i> , NTRN10EG.
4	Calculate the worst case shelf available power by multiplying the provisioned shelf current by 43 volts to get total watts available and subtracting the shelf power budget from the calculated available power to get the available power.

- 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 Retrieve the shelf power budget and provisioned shelf current. Refer to the “Displaying node information” procedure in the *Administration and Security*, 323-1851-301.
- 3 Determine the power requirement of the alarmed pluggable. Refer to the “Technical specifications” chapter in Part 3 of *Planning*, NTRN10EG.
- 4 Calculate the worst case shelf available power by multiplying the provisioned shelf current by 43 volts to get total watts available and subtracting the shelf power budget from the calculated available power to get the available power.

5-386 Alarm clearing procedures—I to Z

Procedure 5-157 (continued)

Provisioning Incompatible - Pluggable

Step	Action	Then
5	If the power requirements of the alarmed module are greater than the available power	shelf power overload is causing the alarm. Refer to the alarm clearing steps for " Shelf Power Near Limit " on page 5-492.
	less than the available power	contact your next level of support or Ciena support group

—end—

Procedure 5-158

Provisioning Mismatch

Alarm ID: 1133

Probable cause

This alarm is raised when the G.8032 Ethernet Ring Protocol (G.8032 ERP) on a node is receiving R-APS(OK) messages from more than one node ID. This indicates that an RPL Port is provisioned on more than one node in the ringlet.

Impact

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

Prerequisites

To perform this procedure, you require an account with at least a level 3 UPC.

Step	Action
1	For each shelf that has a node in the ringlet, launch the G.8032 ERP Management application under Configuration: Data Services.
2	Select the Ringlet Provisioning tab.
3	Use the Ring and Group filter fields to limit the display to the ringlet for which the alarm was raised.
4	Click Retrieve .
5	Make sure there is one and only one ringlet object defined with the attribute RPL Port set among all ringlet objects for the ringlet in all nodes of the ringlet. Refer to the “Retrieving rings and ring ports information in an G.8032 ERP” procedure in Part 3 of <i>Configuration - Bandwidth and Data Services</i> , 323-1851-320.
6	The alarm is cleared if the condition is not present for 17.5 seconds (3.5 consecutive R-APS frame intervals).

—end—

Procedure 5-159 Reach Violation

Alarm IDs: 2024

Probable cause

This alarm is raised on PTP facility if the actual length of the link exceeds the provisioned reach class. Once the violation is detected customer traffic will be blocked by conditioning from the on-ramp direction of the link, but GCC0 and GCC1 comms will remain up.

WLAI line ports allow users to provision the reach class for “Planned” distance.

Impact

Critical, service-affecting (C, SA) alarm if not protected

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

Prerequisites

To perform this procedure, you require an account with at least a level 3 UPC.

Step	Action
1	Verify the reach class of the link. Refer to “Retrieving equipment and facility details” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
2	Re-provision the WLAI line port PTP to make sure the actual length of the link does not exceed the provisioned reach class. Refer to “Editing facility parameters” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.

—end—

Procedure 5-160 RAMAN Failed To Turn On

Alarm ID: 944

Probable cause

This alarm is raised against a RAMAN facility of an SRA circuit pack when the handshaking between the local circuit pack and the far-end circuit pack fails. Reasons for the failure include:

- the far-end circuit pack has failed
- the Telemetry Gain signal is not present
- a disconnected fiber
- a pinched fiber connection
- a dirty optical fiber connector
- a defective fiber optic patchcord
- a defective module
- an incorrectly provisioned value

Note: After a shelf power cycle, the SRA circuit pack could take up to 20 minutes to recover. The alarm is active during this time.

Prerequisites

To perform this procedure, you must:

- use an account with at least a level 3 UPC
- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545
- have a network and site diagram
- have a fiber cleaning kit

Impact

Major, service-affecting (M, SA) alarm

Procedure 5-160 (continued)

RAMAN Failed To Turn On

Step	Action
1	Ensure the provisioning values on the network element upstream of the SRA are correct.
2	Place the alarmed RAMAN amplifier facility out of service (OOS). Refer to the “Changing the primary state of a facility” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
3	Clean and then reconnect the input fibers and connectors at the RAMAN amplifier. Refer to the cleaning connectors procedures in <i>Installation - General Information</i> , 323-1851-201.0.
4	Place the RAMAN amplifier back in-service (IS). Refer to the “Changing the primary state of a facility” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
5	If the alarm still persists, check the upstream connection for mating or pinched fibers.
6	Restart the SRA circuit pack supporting the alarmed RAMAN amplifier facility. Refer to the “Restarting a circuit pack or shelf processor” procedure in Part 1 of this document.
7	Replace the SRA circuit pack supporting the alarmed RAMAN facility. Refer to the “Replacing the amplifier modules” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.
8	If the alarm does not clear, contact your next level of support or Ciena support group.

—end—

Procedure 5-161

Redundant Database Synch Failed

Alarm ID: 1028

Probable cause

This alarm is raised against the shelf to indicate that the shelf processor (SP) database synchronization between the two SPs failed.

This alarm is masked under the following conditions:

- SP equipment faults, indicated by alarms such as Autoprovisioning Mismatch, Circuit Pack Failed, Circuit Pack Mismatch, Circuit Pack Missing, and Circuit Pack Unknown
- communications problems between the two SPs, indicated by alarms such as Intercard Suspected and Internal Mgmt Comms Suspected
- a load mismatch between the two SPs or any SP upgrade failed, indicated by alarms such as Circuit Pack Upgrade Failed, Software Auto-Upgrade in Progress, Software Configuration Unknown, Software Delivery Incomplete, Software Mismatch, and Software Upgrade Failed
- any system fault, indicated by alarms such as Disk Full, Database Integrity failed, and Transport Data Recovery Failed
- SP redundancy is deleted

ATTENTION

In case of SP redundancy, this alarm can be raised after a warm or cold restart. The alarm will clear automatically.

Impact

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

Step	Action
1	Verify that none of the conditions listed in the “Probable cause” section exist on the network element. Clear any active SP alarms according the alarm clearing procedures in this document.
2	Confirm the secondary SP equipment is in service. Refer to the “Retrieving equipment and facility details” in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310. Change the secondary SP equipment to in-service if required. Refer to the “Changing the primary state of a circuit pack, module, or Pluggable” in Part 1 of the <i>Configuration - Provisioning and Operating</i> , 323-1851-310.

5-392 Alarm clearing procedures—I to Z

Procedure 5-161 (continued)

Redundant Database Synch Failed

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

—end—

Procedure 5-162

Redundant Database Synch Failed - CP

Alarm ID: 1185

Probable cause

This alarm is raised against the shelf in the SONET/SDH or Photonic Control Plane to indicate that the shelf processor (SP) database synchronization between the two SPs failed. This alarm can be raised against SPs with CPU-2, or can be raised against any SP type in a Coherent Select configuration.

This alarm is masked under the following conditions:

- SP equipment faults, indicated by alarms such as Autoprovisioning Mismatch, Circuit Pack Failed, Circuit Pack Mismatch, Circuit Pack Missing, and Circuit Pack Unknown
- communications problems between the two SPs, indicated by alarms such as Intercard Suspected and Internal Mgmt Comms Suspected
- a load mismatch between the two SPs or any SP upgrade failed, indicated by alarms such as Circuit Pack Upgrade Failed, Software Auto-Upgrade in Progress, Software Configuration Unknown, Software Delivery Incomplete, Software Mismatch, and Software Upgrade Failed
- any system fault, indicated by alarms such as Disk Full, Database Integrity failed, and Transport Data Recovery Failed
- SP redundancy is deleted

ATTENTION

In case of SP redundancy, this alarm can be raised after a warm or cold restart. The alarm will clear automatically.

Impact

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

Procedure 5-162 (continued)

Redundant Database Synch Failed - CP

Step	Action
1	Verify that none of the conditions listed in the “Probable cause” section exist on the network element. Clear any active SP alarms according to the alarm clearing procedures in this document.
2	Confirm the secondary SP equipment is in service. Refer to the “Retrieving equipment and facility details” in Part 1 of the <i>Configuration - Provisioning and Operating</i> , 323-1851-310. Change it to in-service if required. Refer to the “Changing the primary state of a circuit pack, module, or Pluggable” in Part 1 of the <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
3	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-163 Redundant Database Synch in Progress

Alarm ID: 1026

Probable cause

This alarm is raised against the shelf to indicate that there is a database synchronization in progress between two shelf processors.

Impact

Warning

Step	Action
1	No action is required. The alarm clears once the synchronization is complete.
2	If the alarm does not clear, or is unexpected, contact your next level of support or your Ciena support group.

—end—

Procedure 5-164

Redundant Release Synch Failed

Alarm ID: 1044

Probable cause

This alarm is raised against the shelf to indicate that the Shelf Processor release synchronization between the two SPs failed.

This alarm is masked under the following conditions:

- SP equipment faults, indicated by alarms such as Autoprovisioning Mismatch, Circuit Pack Failed, Circuit Pack Mismatch, Circuit Pack Missing, and Circuit Pack Unknown
- communications problems between the two SPs, indicated by alarms such as Intercard Suspected and Internal Mgmt Comms Suspected
- a load mismatch between the two SPs or any SP upgrade failed, indicated by alarms such as Circuit Pack Upgrade Failed, Software Auto-Upgrade in Progress, Software Configuration Unknown, Software Delivery Incomplete, Software Mismatch, and Software Upgrade Failed
- any system fault, indicated by alarms such as Disk Full, Database Integrity failed, and Transport Data Recovery Failed
- SP redundancy is deleted

Impact

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

Step	Action
1	Verify that none of the conditions listed in the “Probable cause” section exist on the network element. Clear any active SP alarms according the alarm clearing procedures in this document.
2	Confirm the secondary SP equipment is in service. Refer to the “Retrieving equipment and facility details” in Part 1 of the <i>Configuration - Provisioning and Operating</i> , 323-1851-310. Change it to in-service if required. Refer to the “Changing the primary state of a circuit pack, module, or pluggable” in Part 1 of the <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
3	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-165

Redundant Release Synch in Progress

Alarm ID: 1042

Probable cause

This alarm is raised against the shelf to indicate that there is a release synchronization in progress between the two shelf processors.

Impact

Warning

Step	Action
1	No action is required. The alarm clears once the synchronization is complete.
2	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-166

Release Server Mismatch

Alarm ID: 1240

Probable cause

This alarm is raised when the provisioned release server does not match the current release.

Impact

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

Step	Action
1	Retrieve the release server list to check the server. Refer to the “Retrieving a list of the software releases and release servers” procedure in <i>Administration and Security</i> , 323-1851-301.
2	Delete the invalid release server or enter the valid release that matches the current release. Refer to the “Setting a release server” procedure in <i>Administration and Security</i> , 323-1851-301.
3	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-167

Release Server URL Fail

Alarm ID: 1078

Probable cause

This alarm is raised against the shelf when the:

- release server FTP URL parameters entered are invalid (IP/location/User/Password)
- release server is down when the NE does a check
- proper load does not exist on the FTP server

This alarm is raised for an IPv4 and/or IPv6 provisioned server. IPv6 must be enabled if an IPv6 server is provisioned and IPv4 must be enabled if an IPv4 server is provisioned.

Impact

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

Step	Action
1	Retrieve the release server list to trigger a check of the server to see if it has become available. Refer to the “Retrieving a list of the software releases and release Servers” in the <i>Administration and Security</i> , 323-1851-301.
2	Delete the invalid release server URL (clear the URL to disable this feature) or enter the valid release server FTP URL parameters in the URL field and click the Set Server button. Ensure the server selected has the proper load on it at the location referred to by the URL. Refer to the “Setting a release server” procedure in the <i>Administration and Security</i> , 323-1851-301.
3	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-168

Remote Alarm Indication

Alarm ID: 2067

Probable cause

This alarm is raised when the remote network element detects a defective signal from the 6500 network element and returns a Remote Alarm Indication signal in the PDH overhead.

Impact

Warning

Prerequisites

To perform this procedure, you must

- use an account with at least a level 2 UPC
- observe all safety requirements described in the “Observing product and personnel safety guidelines” section in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545

Step	Action
1	Identify the PTS PDH I/F 2xDIM or PTS MRO I/F 2xSFP+/14xSFP circuit pack raising the alarm. Refer to the “ Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm ” procedure in this document.
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	Verify all cross-connects between the near-end and far-end network elements. Refer to the “ Retrieving path cross-connects ” procedure in Part 1 of <i>Configuration - Bandwidth and Data Services</i> , 323-1851-320.
4	Retrieve all alarms at the far-end network element. Refer to the “ Retrieving active alarms for one or more network elements ” procedure in this document. Clear any alarms by following the appropriate alarm clearing procedure.
5	Ensure that the far-end facility is in-service.
6	Verify the required frame format provisioning for the entire PDH traffic path (refer to your company records). Edit the frame format if necessary. If the local PDH facility frame format requires correction, refer to the “ Editing facility parameters ” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.

Procedure 5-168 (continued)

Remote Alarm Indication

Step	Action
7	If the alarm has not cleared, check if there is any signal degradation of the upstream traffic path, including any DS1, DS3 and/or optical facilities carrying the signal. Signal degradation can be indicated by alarms such as Signal Degrade, Signal Fail, Excessive Error Rate, or similar, or by performance monitoring Threshold Crossing Alerts (TCA). If applicable, resolve the signal degradation of the DS1 traffic path associated with these alarms and/or TCAs.
8	Use a test set to test the signal source. <ul style="list-style-type: none">• If there is a valid signal on the transmit side and there is RAI on the receive side, the problem is in the source system. Perform troubleshooting on the source system according to your company procedures. The procedure is complete.• If there are no such conditions, go to step 9.
9	Contact your next level of support or your Ciena support group.

—end—

Procedure 5-169

Remote CCM Error

Alarm ID: 1209

Probable cause

This alarm is raised against a Maintenance Association (MA) entity when the Maintenance End Point (MEP) fails to receive a valid Continuity Check Message (CCM) from a RMEP for 3.5 times of the CCM interval.

Impact

Major, Service-affecting (M, SA) alarm

Step	Action	
1	Verify the local facility is in-service. Refer to the “Retrieving equipment and facility details” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.	
2	If the alarm is raised against	Then go to
	Port MEP	step 3
	Down MEP	step 6
	Up MEP	step 11
3	Verify the RMEP is configured on the peer node. Refer to the “Data services Ethernet OAM provisioning” chapter in Part 3 of <i>Configuration - Bandwidth and Data Services</i> , 323-1851-320.	
4	Verify the far-end facility is operational. Refer to the “Retrieving equipment and facility details” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.	
5	If the alarm is	Then
	cleared	this procedure is completed
	otherwise	step 16
6	Verify the relevant local VCE is in-service. Refer to the “Performing service activation for virtual circuits” procedure in Part 2 of <i>Configuration - Bandwidth and Data Services</i> , 323-1851-320.	
7	Verify the RMEP is configured on the peer node. Refer to the “Data services Ethernet OAM provisioning” chapter in Part 3 of <i>Configuration - Bandwidth and Data Services</i> , 323-1851-320.	
8	Verify the far-end facility is operational.	

Procedure 5-169 (continued)

Remote CCM Error

Step	Action
9	Use linktrace to isolate the location of the problem. Refer to the “Viewing link trace information” procedure in Part 3 of <i>Configuration - Bandwidth and Data Services</i> , 323-1851-320. Note: If there are multiple RMEPs, use the “RTRV-MEP-DEFECTS2” TL1 command (or) the ‘Defects’ tab in Ethernet OAM provisioning window in Site Manager to isolate the alarm condition against a specific RMEP.
10	If the alarm is cleared otherwise
	Then this procedure is completed step 16
11	Verify the relevant local VCE is in-service. Refer to the “Performing service activation for virtual circuits” procedure in Part 2 of <i>Configuration - Bandwidth and Data Services</i> , 323-1851-320.
12	Verify the relevant local VCS is in-service.
13	Verify the RMEP is configured on the peer node. Refer to the “Data services Ethernet OAM provisioning” chapter in Part 3 of <i>Configuration - Bandwidth and Data Services</i> , 323-1851-320.
14	Verify the far-end facility is operational.
15	Use linktrace to verify the forwarding entities along the network are functional.
16	If the alarm does not clear, contact your next level of support or Ciena support group.

—end—

Procedure 5-170

Remote Client Circuit Pack Failed - Pluggable

Alarm ID: 1082

Probable cause

This alarm is raised when the remote OME1110 CPE module indicates a failed client pluggable. This alarm is only applicable to EFM on SuperMux and L2 MOTR. For more information on interworking, see the *Network Interworking Guide*, NTCA68CA. For more information about OME1110, refer to the *OME1110 Deployment Guide*, 323-1851-250. The *OME1110 Deployment Guide* is included in the 6500 technical publication libraries from Release 7.0 to Release 9.1.

Impact

Critical, service-affecting (C, SA) alarm if active

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

Prerequisites

To perform this procedure, you must

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545
- have an antistatic wrist strap to dissipate electrostatic charges

Step	Action
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	Replace the failed client pluggable at the remote OME1110 CPE module.
3	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-171

Remote Client Circuit Pack Missing - Pluggable

Alarm ID: 1081

Probable cause

This alarm is raised when the remote OME1110 CPE module indicates a missing client pluggable. This alarm is only applicable to EFM on SuperMux and L2 MOTR. For more information on interworking, see the *Network Interworking Guide*, NTCA68CA. For more information about OME1110, refer to the *OME1110 Deployment Guide*, 323-1851-250. The *OME1110 Deployment Guide* is included in the 6500 technical publication libraries from Release 7.0 to Release 9.1.

Impact

Critical, service-affecting (C, SA) alarm if active

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

Prerequisites

To perform this procedure, you must

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545
- have an antistatic wrist strap to dissipate electrostatic charges

Step	Action
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	Install a client pluggable at the remote OME1110 CPE module.
3	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-172

Remote Client Circuit Pack Unknown - Pluggable

Alarm ID: 1083

Probable cause

This alarm is raised when the remote OME1110 CPE module indicates an unknown client pluggable. This alarm is only applicable to EFM on SuperMux and L2 MOTR. For more information on interworking, see the *Network Interworking Guide*, NTCA68CA. For more information about OME1110, refer to the *OME1110 Deployment Guide*, 323-1851-250. The *OME1110 Deployment Guide* is included in the 6500 technical publication libraries from Release 7.0 to Release 9.1.

Impact

Critical, service-affecting (C, SA) alarm if active

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

Prerequisites

To perform this procedure, you must

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545
- have an antistatic wrist strap to dissipate electrostatic charges

Step	Action
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	Replace the unknown client pluggable at the remote OME1110 CPE module with the correct pluggable.
3	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-173

Remote Client High Received Optical Power

Alarm ID: 1084

Probable cause

This alarm is raised when the remote OME1110 CPE module client pluggable indicates high optical power. This alarm is only applicable to EFM on SuperMux and L2 MOTR. For more information on interworking, see the *Network Interworking Guide*, NTCA68CA. For more information about OME1110, refer to the *OME1110 Deployment Guide*, 323-1851-250. The *OME1110 Deployment Guide* is included in the 6500 technical publication libraries from Release 7.0 to Release 9.1.

Impact

Critical, service-affecting (C, SA) alarm if active

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

Prerequisites

To perform this procedure, you must

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545
- have an antistatic wrist strap to dissipate electrostatic charges
- have attenuator pads

Step	Action
	 CAUTION Risk of loss of traffic The following steps are traffic affecting.
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	Remove the Rx fiber from the OME1110 client SFP. Using a power meter, measure the received power from the client equipment. Clean and reseat the fiber in the SFP.
3	Look up the client SFP maximum Rx power in the “Technical specifications” chapter in Part 3 of <i>Planning</i> , NTRN10EG.

- 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 Remove the Rx fiber from the OME1110 client SFP. Using a power meter, measure the received power from the client equipment. Clean and reseat the fiber in the SFP.
- 3 Look up the client SFP maximum Rx power in the “Technical specifications” chapter in Part 3 of *Planning*, NTRN10EG.

Procedure 5-173 (continued)

Remote Client High Received Optical Power

Step	Action	
4	If the Rx power is	Then go to
	higher than the maximum power	step 5
	lower than the maximum power	step 6
5	Add attenuators to the link to bring the Rx power down to within specification. Go to step 7 .	
6	Replace the client SFP.	
7	If the original alarm Then	
	is cleared	the procedure is complete
	is not cleared	contact your next level of support or Ciena support group
	—end—	

Procedure 5-174

Remote Client Link Down

Alarm IDs: 698, 901

Probable cause

This alarm is raised when the OME1000 series CPE module indicates that it has detected a port down event on the client side of the network. The possible reason for this alarms are:

- Loss Of Signal at the OME1000 client side receiver
- AN failed between the OME1000 client side and subtending equipment
- problem with the OME1000 client side transmitter

Note that EFM on SuperMux and L2 MOTR supports interworking with OME1110 only. For more information on interworking, see the *Network Interworking Guide*, NTCA68CA. For more information about OME1110, refer to the *OME1110 Deployment Guide*, 323-1851-250. The *OME1110 Deployment Guide* is included in the 6500 technical publication libraries from Release 7.0 to Release 9.1.

When a 20G L2SS circuit pack equipped in a 6500 network element is interworking with an OME1000 series CPE module, this alarm is not raised if the OME1000 series CPE module detects a port down event on the client side of the network.

Impact

Major, service-affecting (M, SA) alarm

Prerequisites

To perform this procedure, you must

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545
- have an antistatic wrist strap to dissipate electrostatic charges
- have a standard multimeter

Procedure 5-174 (continued)

Remote Client Link Down

Step	Action	
1	Confirm with the owner of the far-end equipment that there are no additional faults on their equipment and that the Ethernet facilities are in-service. Auto-negotiation should be enabled on the client equipment.	
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	Remove the Rx fiber from the OME1110 client SFP. Using a power meter, measure the received power from the client equipment. Clean and reseat the fiber in the SFP. Look up the client SFP minimum Rx power in the “Technical specifications” chapter in Part 3 of <i>Planning</i> , NTRN10EG.	
4	If the Rx power is	Then go to
	under the minimum power	step 5
	above the minimum power	step 8
5	Determine the reason for the low Rx power from the client equipment. These can include:	
	<ul style="list-style-type: none">• an SFP mismatch between the 6500 and OME1000 series equipment (including reach or wavelength)• fiber damage between SFPs• fiber connectors that are not fully seated	
6	If the Rx power is	Then
	still lower than specification	contact your next level of support
	within specification	go to step 7
7	If the original alarm has	Then
	cleared	the procedure is complete
	not cleared	go to step 8
8	Using a known good fiber, remove the fiber from the Tx side of the OME1110 client SFP and measure the Tx power of the SFP. Clean and replace the fiber. Look up the client SFP minimum Tx power in the “Technical specifications” chapter in Part 3 of <i>Planning</i> , NTRN10EG.	
9	If the Tx power is	Then go to
	lower than specification	step 10
	within specification	step 11

Procedure 5-174 (continued)

Remote Client Link Down

Step	Action				
10	Replace the client SFP. Refer to the “Replacing an SFP in an OME1110 service module” procedure in the <i>OME1110 Deployment Guide</i> , 323-1851-250. The <i>OME1110 Deployment Guide</i> is included in the 6500 technical publication libraries from Release 7.0 to Release 9.1.				
11	<p>If the original alarm has Then</p> <table> <tr> <td>cleared</td> <td>the procedure is complete</td> </tr> <tr> <td>not cleared</td> <td>go to step 12</td> </tr> </table>	cleared	the procedure is complete	not cleared	go to step 12
cleared	the procedure is complete				
not cleared	go to step 12				
12	<p>Have the client check the Rx power of the client equipment SFP. If it is lower than specifications, determine the reason for the low power and correct it. These can include:</p> <ul style="list-style-type: none"> • an SFP mismatch between the 6500 and OME1000 series or the 6500 and OME1110 equipment (including reach or wavelength) • fiber damage between SFPs • fiber connectors that are not fully seated 				
13	<p>If the original alarm has Then</p> <table> <tr> <td>cleared</td> <td>the procedure is complete</td> </tr> <tr> <td>not cleared</td> <td>there is a possible auto negotiation issue. Contact your next level of support or Ciena support group.</td> </tr> </table>	cleared	the procedure is complete	not cleared	there is a possible auto negotiation issue. Contact your next level of support or Ciena support group.
cleared	the procedure is complete				
not cleared	there is a possible auto negotiation issue. Contact your next level of support or Ciena support group.				

--end--

Procedure 5-175

Remote Client Low Received Optical Power

Alarm ID: 1085

Probable cause

This alarm is raised when the remote OME1110 CPE module client pluggable indicates low optical power. This alarm is only applicable to EFM on SuperMux and L2 MOTR. For more information on interworking, see the *Network Interworking Guide*, NTCA68CA. For more information about OME1110, refer to the *OME1110 Deployment Guide*, 323-1851-250. The *OME1110 Deployment Guide* is included in the 6500 technical publication libraries from Release 7.0 to Release 9.1.

Impact

Critical, service-affecting (C, SA) alarm if active

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

Prerequisites

To perform this procedure, you must

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545
- have an antistatic wrist strap to dissipate electrostatic charges

Step	Action	
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	Remove the Rx fiber from the OME1110 client SFP. Using a power meter, measure the received power from the client equipment. Clean and reseat the fiber in the SFP. Look up the client SFP minimum Rx power in the “Technical specifications” chapter in Part 3 of <i>Planning</i> , NTRN10EG.	
3	If the Rx power is under the minimum power above the minimum power	Then go to step 4 step 7

Procedure 5-175 (continued)

Remote Client Low Received Optical Power

Step	Action						
4	Determine the reason for the low Rx power from the client equipment. These can include: <ul style="list-style-type: none"> • an SFP mismatch between the 6500 and OME1110 equipment (including reach or wavelength) • fiber damage between SFPs • fiber connectors that are not fully seated 						
5	If the Rx power is <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;">still lower than specification</td> <td style="width: 50%; text-align: right;">Then</td> </tr> <tr> <td></td> <td style="text-align: right;">contact your next level of support</td> </tr> <tr> <td style="padding-left: 20px;">within specification</td> <td style="text-align: right;">go to step 6</td> </tr> </table>	still lower than specification	Then		contact your next level of support	within specification	go to step 6
still lower than specification	Then						
	contact your next level of support						
within specification	go to step 6						
6	If the original alarm has <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;">cleared</td> <td style="width: 50%; text-align: right;">Then</td> </tr> <tr> <td></td> <td style="text-align: right;">the procedure is complete</td> </tr> <tr> <td style="padding-left: 20px;">not cleared</td> <td style="text-align: right;">go to step 7</td> </tr> </table>	cleared	Then		the procedure is complete	not cleared	go to step 7
cleared	Then						
	the procedure is complete						
not cleared	go to step 7						
7	Replace the client SFP on the OME1110. Refer to the “Replacing an SFP in an OME1110 service module” procedure in the <i>OME1110 Deployment Guide</i> , 323-1851-250. The <i>OME1110 Deployment Guide</i> is included in the 6500 technical publication libraries from Release 7.0 to Release 9.1.						
8	If the original alarm is <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;">cleared</td> <td style="width: 50%; text-align: right;">Then</td> </tr> <tr> <td></td> <td style="text-align: right;">the procedure is complete</td> </tr> <tr> <td style="padding-left: 20px;">not cleared</td> <td style="text-align: right;">contact your next level of support or Ciena support group</td> </tr> </table>	cleared	Then		the procedure is complete	not cleared	contact your next level of support or Ciena support group
cleared	Then						
	the procedure is complete						
not cleared	contact your next level of support or Ciena support group						

—end—

Procedure 5-176

Remote Defect Indication

Alarm IDs: 858, 927, 1211, 1250, 2022

Probable cause

This alarm is raised against E1 and E3 facilities on 48 Channel Trans Mux (portless), 24xDS3/E3, and PDH gateway circuit packs when an E1 or E3 remote defect indication (RDI) is detected incoming from the far-end network element.

For the FLEX MOTR circuit pack this alarm is raised when a far-end receive failure has been detected.

For the WLAI circuit pack this alarm is raised against the PTP facilities when an incoming OTSi RDI from the far end network element is detected.

For the Ethernet OAM, this alarm is raised against a Maintenance Association (MA) entity when a Maintenance End Point (MEP) receives a valid Continuity Check Message (CCM) with the RDI bit set. The RDI bit is set if the MEP sending the CCM detects an XCON, ERR, TIMEOUT or STATUS defect.

Impact

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

Prerequisites

To perform this procedure, you must observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545.

Step	Action
1	Identify the circuit pack raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document.
2	If the alarm is raised against Ethernet OAM, verify that the transmit path local to the circuit pack and the receive path on the peer node is working correctly.
3	Use company traffic connection information to identify the source site of the signal.
4	If the network element is not connected to a 6500 network element at the far-end, or if the network element is part of a mid-span meet and the far-end network element is from another vendor, use the alarm system of the other vendor to find the problem.

Procedure 5-176 (continued)

Remote Defect Indication

Step	Action
5	Log into the source network element where the signal is generated. If you cannot log in remotely from the local network element, you must travel to the source site.
6	Retrieve all alarms from the remote network element at the transmit end. Refer to the alarms and events procedures in Part 1 of this document.
7	Look for any active alarms for the E3 channel that is alarmed on the far-end.
8	If there are Then no alarms for the source facility ensure that alarm reporting of related alarms (for example, VT2 and E1 alarms for troubleshooting E1 RDI, and STS1 and E3 alarms for troubleshooting E3 RDI) is enabled. Refer to the "Retrieving alarm profiles" in Part 1 of this document. Also ensure that the equipment and facility of the remote circuit pack are in-service. Refer to the "Retrieving equipment and facility details" procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310. If there are masked alarms on this facility, clear them and go to step 9 . alarms for the source facility refer to the appropriate alarm clearing procedures. The Remote Defect Indication alarm may be expected if other alarms are active.

5-416 Alarm clearing procedures—I to Z

Procedure 5-176 (continued)

Remote Defect Indication

Step	Action	
9	At the local network element, 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 10
10	If the alarm does not clear, contact your next level of support or your Ciena support group.	
	—end—	

Procedure 5-177

Remote Invalid Configuration

Alarm IDs: 806, 902

Probable cause

This alarm is raised when the remote OME1000 module has an invalid configuration such as invalid software version or invalid DIP switch settings.

ATTENTION

EFM on SuperMux and L2 MOTR supports interworking with OME1110 only. For the OME1110 the alarm is usually a transient alarm, present on initial fiber connection, or bringing the OME1110 in service. If the alarm persists for more than 5 minutes, it may indicate an incorrect software version or hardware issue with the OME1110. Contact your next level of support or Ciena support group.

For more information on interworking, see the *Network Interworking Guide*, NTCA68CA. For more information about OME1110, refer to the *OME1110 Deployment Guide*, 323-1851-250. The *OME1110 Deployment Guide* is included in the 6500 technical publication libraries from Release 7.0 to Release 9.1.

Impact

Critical, service-affecting (C, SA) alarm if active

Minor, non-service-affecting (m, NSA) alarm, if inactive (6500 GE circuit pack only)

Prerequisites

To perform this procedure, you must observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545.

Step Action

- 1 Retrieve alarms from the circuit pack reporting the alarm.
- 2 For the OME1000, verify the OME1000 DIP switch setting on the OME1000 GE or FE service module for 6500 interop configuration. For information on how to set the DIP switch settings on OME1000 service module, refer to the *OME1000 Installation and User Guide*, NTK972xx. (This step does not apply to the OME1110 module.)
- 3 Verify If the OME1000 GE or FE service module is running the correct software load (Release 2 for interoperability with 6500).

Procedure 5-177 (continued)

Remote Invalid Configuration

Step	Action
4	If the GE or FE service module is not running the correct software load, perform a software upgrade on the GE or FE service module.
5	If the alarm does not clear, perform a restart on the OME1000 module connected to the 6500 network element. Refer to the <i>OME1000 Installation and User Guide</i> , NTK972xx or the “Performing a remote restart of an OME1110” procedure in the <i>OME1110 Deployment Guide</i> , 323-1851-250. The <i>OME1110 Deployment Guide</i> is included in the 6500 technical publication libraries from Release 7.0 to Release 9.1.
6	If the alarm does not clear, replace the OME1000 module connected to the 6500 network element. Refer to the <i>OME1000 Installation and User Guide</i> , NTK972xx or “Replacing an OME1110 service module” procedure in the <i>OME1110 Deployment Guide</i> , 323-1851-250. The <i>OME1110 Deployment Guide</i> is included in the 6500 technical publication libraries from Release 7.0 to Release 9.1.
7	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-178

Remote Inventory Not Supported

Alarm ID: 1029

Probable cause

This alarm is raised when the access panel does not support external inventory slots (NTK505xA5) and an OMD4, OMX, CMD44, CMD64, CMD96, BMD2, UBMD2, MBDM2, GMD10, FIM, PPC6, TPT or DSCM module in provisioned in the access panel slots (83-90).

Impact

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

Prerequisites

To perform this procedure, you must

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545
- have an antistatic wrist strap to dissipate electrostatic charges

Step	Action
1	If the access panel PEC is NTK505MB Then the access panel may be faulty and requires replacement. Go to step 3 not NTK505MB go to step 2
2	If the equipment provisioned in external slots (83-90) is correct the access panel may be faulty and require replacement. Go to step 3 not correct go to step 4
3	Replace the access panel with an access panel that has connections for eight external slots (NTK505MB). Refer to the “Replacing the access panel” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545. Go to step 5.
4	Delete the equipment that is incorrectly provisioned in the external slots. Refer to the “Deleting a circuit pack, module or pluggable” procedure in the <i>Photonic Equipment</i> , 323-1851-102.6.

5-420 Alarm clearing procedures—I to Z

Procedure 5-178 (continued)

Remote Inventory Not Supported

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

—end—

Procedure 5-179

Remote Line High Received Optical Power

Alarm ID: 1088

Probable cause

This alarm is raised when the remote OME1110 CPE module line pluggable indicates high optical power. This alarm is only applicable to EFM on SuperMux and L2 MOTR. For more information on interworking, see the *Network Interworking Guide*, NTCA68CA. For more information about OME1110, refer to the *OME1110 Deployment Guide*, 323-1851-250. The *OME1110 Deployment Guide* is included in the 6500 technical publication libraries from Release 7.0 to Release 9.1.

Impact

Critical, service-affecting (C, SA) alarm if active

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

Prerequisites

To perform this procedure, you must

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545
- have an antistatic wrist strap to dissipate electrostatic charges
- have a standard multimeter

Step	Action
	 CAUTION Risk of loss of traffic The following steps are traffic affecting.
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	Remove the Rx fiber from the OME1110 line SFP. Using a power meter, measure the received power from the 6500 equipment. Clean and reseat the fiber in the SFP.
	Look up the client SFP maximum Rx power in the “Technical specifications” chapter in Part 3 of <i>Planning</i> , NTRN10EG.



CAUTION

Risk of loss of traffic

The following steps are traffic affecting.

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 Remove the Rx fiber from the OME1110 line SFP. Using a power meter, measure the received power from the 6500 equipment. Clean and reseat the fiber in the SFP.

Look up the client SFP maximum Rx power in the “Technical specifications” chapter in Part 3 of *Planning*, NTRN10EG.

Procedure 5-179 (continued)

Remote Line High Received Optical Power

Step	Action	
3	If the Rx power is	Then go to
	above the maximum power	step 4
	below the maximum power	step 6
4	Add an attenuator pad to lower the Rx line power to be within the minimum and maximum power specifications of the SFP.	
5	If the original alarm has	Then
	cleared	the procedure is complete
	not cleared	go to step 6
6	Replace the line SFP on OME1110. Refer to the “Replacing an SFP in an OME1110 service module” procedure in the <i>OME1110 Deployment Guide</i> , 323-1851-250. The <i>OME1110 Deployment Guide</i> is included in the 6500 technical publication libraries from Release 7.0 to Release 9.1.	
7	If the original alarm has	Then
	cleared	the procedure is complete
	not cleared	contact your next level of support or Ciena support group

—end—

Procedure 5-180 **Remote Line Low Received Optical Power**

Alarm ID: 1089

Probable cause

This alarm is raised when the remote OME1110 CPE module line pluggable indicates low optical power. This alarm is only applicable to EFM on SuperMux and L2 MOTR. For more information on interworking, see the *Network Interworking Guide*, NTCA68CA. For more information about OME1110, refer to the *OME1110 Deployment Guide*, 323-1851-250. The *OME1110 Deployment Guide* is included in the 6500 technical publication libraries from Release 7.0 to Release 9.1.

Impact

Critical, service-affecting (C, SA) alarm if active
Minor, non-service-affecting (m, NSA) alarm if inactive

Prerequisites

To perform this procedure, you must

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545
 - have an antistatic wrist strap to dissipate electrostatic charges
 - have a standard multimeter

Step	Action	
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	Remove the Rx fiber from the OME1110 line SFP. Using a power meter, measure the received power from the 6500 equipment. Clean and reseat the fiber in the SFP. Look up the client SFP minimum Rx power in the “Technical specifications” chapter in Part 3 of <i>Planning</i> , NTRN10EG.	
3	If the Rx power is	Then go to
	under the minimum power	step 4
	above the minimum power	step 7

Procedure 5-180 (continued)

Remote Line Low Received Optical Power

Step	Action
4	Determine the reason for the low Rx power from the 6500 equipment. These can include: <ul style="list-style-type: none"> • an SFP mismatch between the 6500 and OME1110 (including reach or wavelength) • fiber damage between SFPs • fiber connectors that are not fully seated • a failed SFP on the 6500 Confirm that the correct SFPs are installed, the fiber connectors are fully seated, there is no fiber damage, and the SFP in the 6500 is transmitting at the proper power level. Fix the issues as needed.
5	If the Rx power is Then
	still lower than specification contact your next level of support or Ciena support group
	within specification go to step 6
6	If the original alarm has Then
	cleared the procedure is complete
	not cleared go to step 7
7	Replace the line SFP on the OME1110. Refer to the “Replacing an SFP in an OME1110 service module” procedure in the <i>OME1110 Deployment Guide</i> , 323-1851-250. The <i>OME1110 Deployment Guide</i> is included in the 6500 technical publication libraries from Release 7.0 to Release 9.1.
8	If the original alarm has Then
	cleared the procedure is complete
	not cleared contact your next level of support or Ciena support group

—end—

Procedure 5-181

Remote Loopback Active

Alarm IDs: 700, 903

Probable cause

This alarm is raised against an ETH or ETH100 facility when the remote CPE port has been successfully put into remote loopback mode, using the Ethernet First Mile (EFM) protocol. The alarm stays active during the execution of the remote loopback.

Note that EFM on SuperMux and L2 MOTR supports interworking with OME1110 only.

For more information on interworking, see the *Network Interworking Guide*, NTCA68CA. For more information about OME1110, refer to the *OME1110 Deployment Guide*, 323-1851-250. The *OME1110 Deployment Guide* is included in the 6500 technical publication libraries from Release 7.0 to Release 9.1.

Impact

Minor, service-affecting (m, SA) alarm

Prerequisites

To perform this procedure, you must observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545.

Step	Action
1	Turn the Remote Loopback off. Once the remote loopback is turned off, remote loopback active alarms will clear. Refer to the “Operating/releasing a channelized loopback” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
2	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-182

Remote Loopback Fail

Alarm IDs: 701, 904

Probable cause

This alarm is raised against an ETH or ETH100 facility when the Ethernet First Mile (EFM) Remote Loopback protocol cannot be executed successfully with the far-end CPE module.

Note that EFM on SuperMux and L2 MOTR supports interworking with OME1110 only.

For more information on interworking, see the *Network Interworking Guide*, NTCA68CA. For more information about OME1110, refer to the *OME1110 Deployment Guide*, 323-1851-250. The *OME1110 Deployment Guide* is included in the 6500 technical publication libraries from Release 7.0 to Release 9.1.

Impact

Minor, service-affecting (m, SA) alarm

Prerequisites

To perform this procedure, you must observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545.

Step	Action
1	If one or more of the following alarms are raised against the ETH or ETH100 facility that raised the remote loopback fail alarm, follow the appropriate procedure(s) to clear the alarm(s): <ul style="list-style-type: none">• Loss Of Signal• Loss of Data Sync• Remote Receiver Fail (not applicable to EFM on SuperMux)• Remote Power Fail Indication• Remote Invalid Configuration• CPE Discovery Protocol Failure

- 1 If one or more of the following alarms are raised against the ETH or ETH100 facility that raised the remote loopback fail alarm, follow the appropriate procedure(s) to clear the alarm(s):
 - Loss Of Signal
 - Loss of Data Sync
 - Remote Receiver Fail (not applicable to EFM on SuperMux)
 - Remote Power Fail Indication
 - Remote Invalid Configuration
 - CPE Discovery Protocol Failure

Procedure 5-182 (continued)

Remote Loopback Fail

Step	Action
2	If the alarm does not clear, turn the remote loopback off. Once the remote loopback is turned off, the Remote Loopback Fail alarm will clear. Refer to the “ <i>Operating/releasing a channelized loopback</i> ” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
3	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-183

Remote Node Unreachable

Alarm IDs: 1413

Probable cause

This alarm is an indication that local end is unable to communicate with the remote side and is raised on expiry of OSRPLINE timers (inactivity timer or remote information response timer).

A MiniHello message (LIP) is generated every 15 seconds on/for each OSRP line (“on” when inband comms is used and “for” when out-of-band (OOB) communications are used). Therefore, a node expects to receive LIPs every 15 seconds on/for each OSRP line. However, each node also has a MiniHello Inactivity Timer set basically to 3xLIP generation timer (3x15 seconds=45 seconds). If a node does not see an LIP on/for an OSRP line within the Inactivity Timer period, then it raises the Remote Node Unreachable alarm.

For the Photonic Control Plane, if out-of-band (OOB) is disabled, the alarm can be raised under the following conditions:

- The OSC facility associated with the OSRP line or OSRP link is out-of-service.
- The circuit pack supporting the OSC facility (for example, 2xOSC on a 6500 shelf) is out-of-service, missing, or rebooting.
- A TID consolidated node (TIDc) member shelf supporting the OSC facility is down.
- Communication between the TIDc primary and member shelf is down.

When OOB is enabled on the OSRP link, the alarm can be raised in the following conditions:

- The OSRP line OOB Common Identifier provisioned at each node terminating the OSRP line does not match. (This parameter is provisioned on the OSRP line, not the OSRP link.)
- The OOB Remote Node ID is incorrect. For example, it does not match the node ID of the neighboring node.
- The OOB Remote IP address is incorrect. For example, it does not match the CONTROL-shelf#-GROUP0 of the neighboring node.

Procedure 5-183 (continued)

Remote Node Unreachable

- The OOB Remote UDP port is incorrect. For example, it does not match the UDP port provisioned in the neighboring node (see the “Retrieving OSRP provisioning information” and “Editing an OSRP instance” procedures in *Configuration - Control Plane*, 323-1851-330).
- OOB comms messages are routed using OSPF. Refer to the “Photonic Control Plane data communications” section in Part 4 of *6500 Planning*, NTRN10EG, for more information on how to setup and troubleshoot the various supported configurations.

This alarm is also raised when Interswitch Communication Channel Protocol (ISCC) communication fails on the Control Plane and the OSRP line goes down after the timeout).

Impact

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

Prerequisites

To perform this procedure, you require an account with at least a level 3 UPC.

Step	Action
1	Identify the port that raised the alarm. Refer to the procedure in Part 1 of this document.
2	Identify the neighbor node name, supporting Termination Point (TP), neighbor containing link ID.
3	If the alarm is raised against the Photonic Control Plane Then go to step 10 otherwise step 4
4	If a remote node OSRP Connection was deleted or not created, recreate the OSRP Connection.
5	If the original alarm has cleared the procedure is complete not cleared go to step 6

Procedure 5-183 (continued)

Remote Node Unreachable

Step	Action	
6	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. If using in-band communications, check the DCC/GCC/OSC datacomms settings (whichever is applicable based on the provisioned Control Plane). For out-of-band communications (supported by the Photonic Control Plane only) check the DCN/SCN datacomms settings or OSC datacomms settings, depending on which is being used. For details on in-band and out-of-band datacomms, refer to the “SONET/SDH, OTN, and Photonic Control Plane considerations” section in Part 4 of <i>6500 Packet-Optical Platform Planning</i> , NTRN10EG.	
7	If the ports are not configured correctly, change appropriate side to the correct setting.	
8	If the original alarm has	Then
	cleared	the procedure is complete
	not cleared	go to step 9
9	Verify if the Line Module is in a reboot state, wait five minutes for the Line Module to complete the boot cycle. Go to step 18 .	
10	Determine if OOB is used for an OSRP link or line by launching the OSRP Provisioning Site Manager application, selecting a link, and checking if OOB is enabled or disabled.	
11	If OOB is	Then go to
	disabled	step 12
	enabled	step 16
12	Determine the OSC facilities associated with the OSRP link or line by using the OSRP Provisioning and the OTS Management Site Manager applications:	
	<ul style="list-style-type: none"> In the OSRP Provisioning application, select the Lines tab and lookup the “Local TP” column to determine the AID of the amplifier circuit pack associated with the OSRP line (for example, ADJ-2-2-5, which means the amplifier port in shelf 2, slot 2, port 5). In the OTS Management application, select the ROADM OTS that contains the amplifier AID determined in the previous step, and lookup up the OSC port associated to the OTS. 	
13	Verify that the OSC facility is in-service using the Site Manager Equipment and Facility application. Place the facility in-service if it is out-of-service.	
14	Verify that there are no alarms related to the OSC facility. Refer to corresponding alarms clearing procedure if any OSC alarms are present.	

Procedure 5-183 (continued)

Remote Node Unreachable

Step	Action
15	If the OSC facility is on a TIDC member shelf, ensure that there are no alarms indicating communications issues between the TIDC primary shelf and that member shelf. For example, there should be no "ILAN Failure" and no "Member Shelf Unreachable" alarms. Go to step 18 .
16	Verify that the OSRP line OOB Common Identifier is correct. If it is incorrect, put the OSRP line out-of-service and edit the value to match the value provisioned at the neighboring node. Put the OSRP line back in-service.
17	Verify that the OSRP link Remote Node IP, Remote Node ID, and Remote Node UDP ports are correct. If they are incorrect, put the OSRP line associated to that OSRP link out-of-service and edit the values on the OSRP link. Put the OSRP line back in-service.
18	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-184 Remote Port OOS

Alarm IDs: 1069, 1070, 1248, 1365, 1366, 1847

Probable cause

This alarm is raised against a FLEX, LAG, ETH, ETH10G, ETTP, or ETH100 facility when there is a Tx conditioning failure due to the remote port being manually put OOS.

The alarm is raised on far end when NON-LAG UP MEP (maintenance end point) port administratively is declared OOS. However, if aggregated UP MEP port belonging all members moved to administratively OOS, then other end declares Far End client signal fail due to VLLI conditioning.

In case of LAG, the “Far End Client Signal Fail” alarm is raised instead of “Remote Port OOS”.

This alarm masks the “Far End Client Signal Fail” alarm on ETTP ports.

Impact

Major, service-affecting (M, SA) alarm if not protected

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

Prerequisites

To perform this procedure, you must observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545.

Step	Action
1	Make sure the remote port is put back in-service.
2	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-185

Remote Port Unreachable

Alarm IDs: 1246, 1367, 1368, 1369, 1370, 1846

Probable cause

This alarm is raised when the remote port on the far-end NE circuit pack is not transmitting heartbeat messages to the port on the near-end NE circuit pack which is alarming or the heartbeat messages are being impaired due to network interference. Alternatively, the port on the near-end NE circuit pack which is alarming, is not receiving the heartbeat messages from the remote port on the far-end NE circuit pack.

If the Virtual Link Loss Indicator (VLLI) is enabled, the alarm is raised on least numbered LAG/D-LAG member port when:

- Continuity Check Message (CCM) timeout occurs
- eMOTR receives bad MEPID or MAID from remote end
- there is a CCM interval error
- eMOTR receives a CCM MD level different than MEP MD level

This alarm masks the “Far End Client Signal Fail” and “Remote Port-Out of Service” alarms on ETTP ports.

Impact

Critical, service-affecting (C, SA) alarm if not protected
Minor, non-service-affecting (m, NSA) alarm if protected

Prerequisites

To perform this procedure, you must observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545.

Step	Action				
1	Verify the remote port fiber connections. Repair, clean, and reconnect the fibers as required.				
2	If the original alarm has Then <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">cleared</td> <td style="width: 70%;">the procedure is complete</td> </tr> <tr> <td style="width: 30%;">not cleared</td> <td style="width: 70%;">go to step 3</td> </tr> </table>	cleared	the procedure is complete	not cleared	go to step 3
cleared	the procedure is complete				
not cleared	go to step 3				

5-434 Alarm clearing procedures—I to Z

Procedure 5-185 (continued)

Remote Port Unreachable

Step	Action
3	Use the appropriate alarm clearing procedure to clear any alarms on the remote port including Loss Of Signal and AIS (STS Rx) alarms. If the alarms are against OC-n/STM-n circuit packs, clear these alarms first.
4	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-186

Remote Power Fail Indication

Alarm IDs: 697, 900

Probable cause

This alarm is raised when the far-end OME1110 CPE module indicates that there has been a power failure on one of the two power supplies.

This alarm is only applicable to EFM on SuperMux and L2 MOTR. For more information on interworking, see the *Network Interworking Guide*, NTCA68CA.

For more information about OME1110, refer to the *OME1110 Deployment Guide*, 323-1851-250. The *OME1110 Deployment Guide* is included in the 6500 technical publication libraries from Release 7.0 to Release 9.1.

Impact

Critical, service-affecting (C, SA) alarm, if active

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

Prerequisites

To perform this procedure, you must observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545.

Step	Action
1	Verify the power is supplied and connected to both power supplies on the OME1110. If the power is off, turn the power back on.
2	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-187

Remote Power Supply 1/2 Missing

Alarm IDs: 1090, 1091

Probable cause

This alarm is raised when the remote OME1110 CPE module indicates a missing power supply 1 or missing power supply 2. This alarm is only applicable to EFM on SuperMux and L2 MOTR. For more information on interworking, see the *Network Interworking Guide*, NTCA68CA.

For more information about OME1110, refer to the *OME1110 Deployment Guide*, 323-1851-250. The *OME1110 Deployment Guide* is included in the 6500 technical publication libraries from Release 7.0 to Release 9.1.

Impact

Major, non-service-affecting (m, NSA) alarm, if active

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

Prerequisites

To perform this procedure, you must

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545
- have an antistatic wrist strap to dissipate electrostatic charges

Step	Action
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	Verify the power supply 1 or 2 exists at the remote OME1110 module. If a power supply exists that corresponds to the missing power supply alarm, is likely the power supply is no longer functional. Replace it with a new power supply.
3	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-188

Remote Receiver Fail

Alarm IDs: 703, 906

Probable cause

This alarm is raised when the far-end OME1000 series CPE module indicates a trunk-side Rx failure to the 6500.

This alarm is not supported in the L2 MOTR and SuperMux EFM implementation. For more information on interworking, see the *Network Interworking Guide*, NTCA68CA.

Impact

Critical, service-affecting (C, SA) alarm, if active

Minor, non-service-affecting (m, NSA) alarm, if inactive (applies to 6500 GE circuit pack only)

Prerequisites

To perform this procedure, you must

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545
- have an antistatic wrist strap to dissipate electrostatic charges
- have a standard multimeter

Step	Action	
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	Remove the Rx fiber from the OME1000 module line SFP. Using a power meter, measure the received power from the 6500 equipment. Clean and reseat the fiber in the SFP. Look up the client SFP minimum Rx power in the “Technical specifications” chapter in Part 3 of <i>Planning</i> , NTRN10EG.	
3	If the Rx power is	Then go to
	under the minimum power	step 4
	above the minimum power	step 7

Procedure 5-188 (continued)

Remote Receiver Fail

Step	Action						
4	<p>Determine the reason for the low Rx power from the 6500 equipment. These can include:</p> <ul style="list-style-type: none"> • an SFP mismatch between the 6500 and OME1000 equipment (including reach or wavelength) • fiber damage between SFPs • fiber connectors that are not fully seated • a failed SFP on the 6500 <p>Confirm the correct SFPs are installed, the fiber connectors are fully seated, there is no fiber damage, and the SFP in the 6500 is transmitting at the proper power level. Fix the issues as needed.</p>						
5	<table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 30%; text-align: left; padding-bottom: 5px;">If the Rx power is</th><th style="width: 70%; text-align: left; padding-bottom: 5px;">Then</th></tr> </thead> <tbody> <tr> <td style="padding-top: 5px;">still lower than specification</td><td style="padding-top: 5px;">contact your next level of support or Ciena support group</td></tr> <tr> <td style="padding-top: 5px;">within specification</td><td style="padding-top: 5px;">go to step 6</td></tr> </tbody> </table>	If the Rx power is	Then	still lower than specification	contact your next level of support or Ciena support group	within specification	go to step 6
If the Rx power is	Then						
still lower than specification	contact your next level of support or Ciena support group						
within specification	go to step 6						
6	<table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 30%; text-align: left; padding-bottom: 5px;">If the original alarm has</th><th style="width: 70%; text-align: left; padding-bottom: 5px;">Then</th></tr> </thead> <tbody> <tr> <td style="padding-top: 5px;">cleared</td><td style="padding-top: 5px;">the procedure is complete</td></tr> <tr> <td style="padding-top: 5px;">not cleared</td><td style="padding-top: 5px;">go to step 7</td></tr> </tbody> </table>	If the original alarm has	Then	cleared	the procedure is complete	not cleared	go to step 7
If the original alarm has	Then						
cleared	the procedure is complete						
not cleared	go to step 7						
7	Replace the line SFP on the OME1000 equipment. Refer to the <i>OME1000 Installation and User Guide</i> , NTK972xx, or the “Replacing an SFP in an OME1110 service module” procedure in the <i>OME1110 Deployment Guide</i> , 323-1851-250. The <i>OME1110 Deployment Guide</i> is included in the 6500 technical publication libraries from Release 7.0 to Release 9.1.						
8	<table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 30%; text-align: left; padding-bottom: 5px;">If the original alarm has</th><th style="width: 70%; text-align: left; padding-bottom: 5px;">Then</th></tr> </thead> <tbody> <tr> <td style="padding-top: 5px;">cleared</td><td style="padding-top: 5px;">the procedure is complete</td></tr> <tr> <td style="padding-top: 5px;">not cleared</td><td style="padding-top: 5px;">contact your next level of support or Ciena support group</td></tr> </tbody> </table>	If the original alarm has	Then	cleared	the procedure is complete	not cleared	contact your next level of support or Ciena support group
If the original alarm has	Then						
cleared	the procedure is complete						
not cleared	contact your next level of support or Ciena support group						

—end—

Procedure 5-189 Resources Above Threshold

Alarm IDs:2125, 2152

Probable cause

This Warning is raised when internal resources on the circuit pack have exceeded its 90% threshold.

Impact

Warning

Prerequisites

To perform this procedure, you require an account with at least a level 3 UPC.

Step	Action
------	--------

- 1 if this Warning is raised during provisioning the PKTIWF facilities procedure, see the Historical Fault Browser in Site Manager to find an event that indicates which resource has hit has exceeded its 90% threshold.
- 2 If the jitter buffer memory is the resource which has exceeded its 90% threshold, delete the PKTIWF facilities which have a “Facility Provisioning Failure” alarm.
- 3 If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-190 Resources At Limit

Alarm IDs:2128, 2155

Probable cause

This Warning is raised when internal resources on the circuit pack have reached its 98% limit.

Impact

Warning

Prerequisites

To perform this procedure, you require an account with at least a level 3 UPC.

Step	Action
1	if this Warning is raised during provisioning the PKTIWF facilities procedure, see the Historical Fault Browser in Site Manager to find an event that indicates which resource has hit the 98% limit.
2	If the jitter buffer memory is the resource which is at its limit, delete the PKTIWF facilities which have a “Facility Provisioning Failure” alarm.
3	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-191

Ring Failure

Alarm ID: 810

Probable cause

This alarm is raised when the neighboring RPR station sends a different ring name than expected. This can result from:

- misprovisioning the RPR ring name on the given RPR station
- misconnecting the RPR station to the wrong RPR ring

This alarm is raised against the WAN facility of a RPR circuit pack.

ATTENTION

If the RPR ring name is mis-provisioned, traffic flowing through that RPR station is unaffected even if the severity of the alarm is Critical, service-affecting (C, SA).

Impact

Critical, service-affecting (C, SA) alarm

Prerequisites

To perform this procedure, you require an account with at least a level 3 UPC.

Step	Action
1	<p>Verify the received ring name of the WAN facility of the RPR that the alarm is raised against and compare it to the expected ring name. Refer to the “Loading ring data from a network element” procedure in the <i>Bandwidth and Data Services</i>, 323-1851-310, to retrieve the expected ring name and the “Retrieving equipment and facility details” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i>, 323-1851-310, to retrieve the WAN facility data.</p> <p>If the RPR station is supposed to be on this RPR ring but the RPR ring name is misprovisioned is not supposed to be on this RPR ring has correct RPR ring name</p> <p>Then go to step 2 step 3 step 4</p>
2	Change the RPR ring name of this station. Refer to the “Editing Ring Configurations” procedure in Part 1 of <i>Configuration - Bandwidth and Data Services</i> , 323-1851-320. Go to step 6 .

- 1 Verify the received ring name of the WAN facility of the RPR that the alarm is raised against and compare it to the expected ring name. Refer to the “Loading ring data from a network element” procedure in the *Bandwidth and Data Services*, 323-1851-310, to retrieve the expected ring name and the “Retrieving equipment and facility details” procedure in Part 1 of *Configuration - Provisioning and Operating*, 323-1851-310, to retrieve the WAN facility data.

If the RPR station is supposed to be on this RPR ring but the RPR ring name is misprovisioned is not supposed to be on this RPR ring has correct RPR ring name	Then go to step 2 step 3 step 4
--	---

- 2 Change the RPR ring name of this station. Refer to the “Editing Ring Configurations” procedure in Part 1 of *Configuration - Bandwidth and Data Services*, 323-1851-320. Go to [step 6](#).

Procedure 5-191 (continued)

Ring Failure

Step	Action
3	Remove this RPR station from this RPR ring. Delete the path connections between the WAN ports of this card and the optical paths and create passthrough connections in their place. Delete the passthrough connections (if they exist) and add new connections to connect this module's WAN ports to the correct ring. Refer to the "Retrieving path connections" procedure, "Adding a path connection" procedure, and "Deleting path connections" in Part 1 of the <i>Bandwidth and Data services</i> , 323-1851-320. Go to step 6 .
4	Find the neighboring RPR station the WAN is connected to. Refer to the "Retrieving path connections" procedure in Part 1 of <i>Configuration - Bandwidth and Data Services</i> , 323-1851-320 to trace the connections to the optics card. Use company records to determine the next RPR site on the ring in that direction.
5	Change the ring name on the RPR. Refer to the "Editing Ring Configurations" procedure in Part 1 of <i>Configuration - Bandwidth and Data Services</i> , 323-1851-320.
6	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-192 Ringlet Failure

Alarm ID: 811

Probable cause

This alarm is raised when the ingress ringlet ID number does not match the expected ringlet ID number on a ringlet. This alarm is raised against the WAN facility.

This can be caused by:

- misprovisioning the RPR span with east span to east span
 - misprovisioning the RPR span with west span to west span
 - miscabling of incorrect fiber-optic cable connections

Impact

Critical, service-affecting (C, SA) alarm

Prerequisites

To perform this procedure, you must

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545
 - have an antistatic wrist strap to dissipate electrostatic charges
 - use an account with at least a level 3 UPC

Step	Action
1	Verify the RPR span provisioning at each station. Correct any RPR span provisioning errors. Refer to the “Loading ring data from a network element” and “Editing Ring Configurations” procedures in Part 1 of the <i>Configuration - Bandwidth and Data Services</i> , 323-1851-320.
2	If the original alarm has
	cleared
	the procedure is complete
	not cleared
	go to step 3
3	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.

5-444 Alarm clearing procedures—I to Z

Procedure 5-192 (continued)

Ringlet Failure

Step	Action
4	Verify the fiber connections of the optic circuit pack associated with the RPR WAN.
5	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-193

Ring Protection Exerciser Failed

Alarm IDs: 1290, 1291

Probable cause

This alarm is raised when the protection exerciser has failed to complete the exercise routine on the selected facilities.

This alarm is caused by one of the following conditions:

- faulty circuit pack
- exerciser is running somewhere else in the 1+1 APS, 2-Fiber/4-Fiber BLSR/MS-SPRing/HERS or 1+1/MSP linear, 1+1 port TPT, or 1+1 TPT configuration
- crossed fibers
- incorrect node on a non-adjacent node
- LOW-R applied at the adjacent end of the span where the exerciser is run on the ring

Impact

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

Prerequisites

To perform this procedure, you require an account with at least a level 3 UPC.

Step	Action	
1	Ensure that there is no active protection switch on the 1+1 APS, 2-Fiber/4-Fiber BLSR/MS-SPRing/HERS or 1+1/MSP linear, 1+1 port TPT, or 1+1 TPT configuration. Refer to the “Retrieving protection status details” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310. If protection switches on the 2-Fiber/4-Fiber BLSR/MS-SPRing/HERS or 1+1/MSP linear, 1+1 port TPT, or 1+1 TPT configuration are	Then go to step 2
	idle	step 2
	not idle	step 7

Procedure 5-193 (continued)

Ring Protection Exerciser Failed

Step	Action
2	Check if any exerciser is scheduled to run on another network element in the 1+1 APS, 2-Fiber/4-Fiber BLSR/MS-SPRing/HERS or 1+1/MSP linear, 1+1 port TPT, or 1+1 TPT configuration at approximately the same time. Exercisers on the same protection entity should have staggered schedules. Refer to the “Retrieving the exerciser schedule” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
3	If the exerciser is running on another network element in the 1+1 APS, 2-Fiber/4-Fiber BLSR/MS-SPRing/HERS or 1+1/MSP linear, 1+1 port TPT, or 1+1 TPT configuration, inhibit the exerciser. Refer to the “Running/inhibiting the exerciser in the protection exerciser” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
4	If the Protection Channel Match Fail alarm is active (indicating a potential crossed fiber), follow the alarm clearing procedure in this document to clear the alarm.
5	Initiate the exerciser on the selected equipment. Refer to the “Running/inhibiting the exerciser” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
6	If the alarm does not clear, contact your next level of support or your Ciena support group. The procedure is complete.
7	If an auto switch is active, find and clear any of the following alarms if active: <ul style="list-style-type: none"> • OC/STM, STS/HO VC and VT/LO VC facility <ul style="list-style-type: none"> — AIS (OC/STM) — Loss of Frame (OC/STM) — Loss Of Signal (OC/STM) — Signal Fail (OC/STM) — Trace Identifier Mismatch (STS/HO VC and VT/LO VC) — Protection Switch Active • OTM0, OTM1, OTM2, OTM3, or OTM4 facility <ul style="list-style-type: none"> — Loss of Frame — Loss Of Signal — ODU AIS — ODU LCK — ODU OCI — OPU AIS — OTU Loss of Multiframe — OTU Pre-FEC Signal Fail — OTU Trace Identifier Mismatch — Protection Switch Active

Procedure 5-193 (continued)
Ring Protection Exerciser Failed

Step	Action
8	Ensure all line alarms and auto-switches are cleared before continuing.
9	Release all user-initiated protection switches. Refer to the “Releasing a protection switch” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
10	If the wait-to-restore is active, a Wait-to-Restore event active is raised against the 1+1 APS, 2-Fiber/4-Fiber BLSR/MS-SPRing/HERS or 1+1/MSP linear, 1+1 port TPT, or 1+1 TPT configuration. Wait for the event to clear.
11	Initiate the exerciser on the selected equipment. Refer to the “Running/inhibiting the exerciser” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
12	If the alarm does not clear, go to step 2 . If the alarm does not clear after repeating the procedure from step 2 , contact your next level of support or your Ciena support group.

—end—

Procedure 5-194

Ring Protection Switch Complete

Alarm IDs: 471, 472, 1113

Probable cause

This alarm is raised when a traffic switch occurs on a 2-Fiber/4-Fiber BLSR/MS-SPRing/HERS. The switch request was either automatic or user-initiated (manual or forced).

Impact

Warning

Prerequisites

To perform this procedure, you require an account with at least a level 2 UPC.

Step	Action
	<p>Note: No action is required if a user is performing a test or maintenance operation. This alarm is a reminder to not leave a potentially service-affecting condition on the system.</p>
1	Check the traffic protection status. Refer to the “Retrieving protection status details” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
2	If the switch was automatic, check for Signal Fail or Signal Degrade alarms related to this facility. Clear these alarms by following the appropriate trouble clearing procedure.
3	Determine if the switch was user-initiated by checking for any protection switch active alarms. Refer to “ Protection Switch Active alarms ” on page 5-370 .
4	If maintenance is complete, release the user-initiated switches. Refer to the “Releasing a protection switch” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
5	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-195 Ring Protection Switch Fail

Alarm IDs: 326, 528, 1129

Probable cause

This alarm is raised when the system attempts to switch traffic from the working to the protection channels in a 2-Fiber/4-Fiber BLSR/MS-SPRing/HERS configuration and fails.

This alarm is raised when one of the following conditions occurs on either the local or remote network element:

- a faulty circuit pack
 - a degraded signal
 - a higher priority switch status exists
 - an incorrect 2-Fiber/4-Fiber BLSR/MS-SPRing/HERS provisioning

Impact

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

Prerequisites

To perform this procedure, you require an account with at least a level 3 UPC.

Procedure 5-195 (continued)

Ring Protection Switch Fail

Step	Action
5	Verify the 2-Fiber/4-Fiber BLSR/MS-SPRing/HERS provisioning. Refer to the “Retrieving BLSR/MS-SPRing/HERS configuration information” procedure in Part 1 of <i>Configuration - Bandwidth and Data Services</i> , 323-1851-320.
6	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-196 Rollover in Progress

Alarm IDs: 10, 139, 140, 141, 142, 246, 272, 1066

Probable cause

This alarm is raised against the shelf to indicate there is one or more in-service traffic rollover operations in progress.

Impact

Warning

Step	Action						
1	Retrieve the rollovers in progress. Refer to the “Performing an in-service path connection rollover for all connections on a port” procedure in Part 1 of <i>Configuration - Bandwidth and Data Services</i> , 323-1851-320.						
2	The alarm remains against the shelf until all bridges have been deleted (rollover backed out), or all switches have been committed (rollover completed).						
	<table> <thead> <tr> <th>If you want to</th> <th>Then go to</th> </tr> </thead> <tbody> <tr> <td>back out of the rollover in progress</td> <td>step 3</td> </tr> <tr> <td>complete the rollover in progress</td> <td>step 4</td> </tr> </tbody> </table>	If you want to	Then go to	back out of the rollover in progress	step 3	complete the rollover in progress	step 4
If you want to	Then go to						
back out of the rollover in progress	step 3						
complete the rollover in progress	step 4						
3	<p>If the rollover is in the switched state, click Backout to back out to the bridged state. The state changes from switched to bridged.</p> <p>If the rollover is in the bridged state, click Backout to back out to the idle state. The state changes from bridged to idle.</p> <p>Go to step 6.</p>						
4	If the rollover is in the bridged state, click Switch to to roll the connection to the switched state. The state changes from bridged to switched.						
5	If the rollover is in the switched state, click Commit to complete the rollover.						
6	If the alarm does not clear, contact your next level of support or your Ciena support group.						

—end—

Procedure 5-197

Root Directory Has Reached Maximum File Entry Limit

Alarm ID: 1308

Probable cause

This alarm is raised when the root directory on the SP has reached its maximum file entry limit.

Impact

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

Step	Action
------	--------

- 1 Contact your next level of support or Ciena support group.

—end—

Procedure 5-198

Rx Channel Power Out of Range

Alarm IDs: 1312, 1571, 1597

Probable cause

This alarm is raised when the Rx Channel power is outside the Rx channel minimum power and Rx channel maximum power optical power range.

ATTENTION

The “Rx Channel Power Out Of Range” alarm may be raised on a valid setup as the thresholds for this alarm are in the acceptable operating range of the Rx interface. It is unlikely that this will occur as OnePlanner will typically set the Rx interface power in a range which will not raise this alarm. However, in some cases, when the Wavelength-Selective 40G OCLD, Flex2 WL3/WL3e OCLD, Flex3 WL3e OCLD, Flex4 WL3e OCLD, 100G WL3e OTR, or 100G WL3/WL3e OCLD circuit pack is deployed with an NGM circuit pack, the alarm may be raised. If necessary, an attenuator pad can be used to bring the power level within the alarm threshold level. For the alarm threshold levels, see the Ranges button within the Site Manager Equipment & Facility Provisioning application.

Impact

Major, service-affecting (M, SA) alarm, unprotected

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

Prerequisites

To perform this procedure, you must:

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0
- have an antistatic wrist strap to dissipate electrostatic charges
- have the optical fiber connection information (that is, how the optical modules on each network element connect to other network elements)
- have an optical power meter with the same optical connectors as the network element
- have attenuator pads

Step	Action
1	Identify the circuit pack and facility raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document.

- 1 Identify the circuit pack and facility raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document.

Procedure 5-198 (continued)

Rx Channel Power Out of Range

Procedure 5-198 (continued)
Rx Channel Power Out of Range

Step	Action
10	<p>If the original alarm has cleared the procedure is complete</p> <p>If the original alarm has not cleared reseat the circuit pack reporting the alarm. Refer to the “Reseating a circuit pack” procedure in <i>Fault Management - Module Replacement</i>, 323-1851-545.</p>
11	<p>If the alarm does not clear, contact your next level of support or your Ciena support group.</p>

—end—

Procedure 5-199

Rx Ethernet Idle

Alarm IDs: 820, 828

Probable cause

This alarm is raised against an Ethernet facility of a GE, 24x10/100BT, or SuperMux (in GFP-F mode) circuit pack when only idle frames are received for the duration of the provisioned Rx Ethernet idle period due to upstream equipment outage. If the outage is on the directly connected client port, the LAN Link Down alarm is raised.

Impact

Major, service-affecting (M, SA) alarm, if active

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

Step	Action
1	Ensure that the alarm is not caused by accidentally turning on the Rx idle parameter of the corresponding GE port (ETH facility), 10/100BT port (ETH100 facility), or SuperMux (in GFP-F mode) port (ETH facility). Refer to the “Editing facility parameters” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
2	Investigate if there is an outage or equipment malfunction on the upstream network element. Follow the upstream network element alarm clearing procedures to clear the alarms.
3	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-200

Rx Partial Loss of Capacity - LCAS

Alarm ID: 923

Probable cause

This alarm is raised against an LCAS-enabled WAN facility of an L2SS, 20G L2SS, PDH gateway, or SuperMux circuit pack. The alarm is raised when at least one (but not all) Rx LCAS group member is in a failed state and unable to receive data, resulting in a partial loss of capacity in the receive direction.

This alarm is not applicable when only one Rx LCAS group member is added.

Impact

Minor, non-service-affecting (m, NSA) alarm, protected
Minor, service-affecting (m, SA) alarm, unprotected

Prerequisites

To perform this procedure, you require an account with at least a level 3 UPC.

Step	Action	
1	Identify the WAN facility raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document.	
2	Look for any other alarms in the active alarm list that are against the WAN facility on the near-end and far-end. Use the appropriate alarm clearing procedure to clear the alarm.	
3	Verify the number of VCAT members provisioned at the near-end and far-end network elements match. Refer to the “Retrieving VCAT members of a virtual concatenation group (VCG)” in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.	
4	If the number of VCAT members	Then go to
	match	step 6
	do not match	step 5
5	Correct the mismatch by adding/restoring or removing VCAT members to the near or far-end WAN facility as required. Restore any incorrectly removed members at the far-end. Refer to the “Removing or restoring a VCAT member (LCAS-enabled) of a VCG” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.	
6	If the alarm does not clear, contact your next level of support or your Ciena support group.	

—end—

Procedure 5-201

Rx Power Out of Range

Alarm IDs: 671, 842, 844, 847, 969, 989, 1005, 1175, 1253, 1302, 1434

Probable cause

This alarm is raised when the Rx power is outside the minimum and maximum receive optical power range. For parallel optic CFPs, this is the logical OR of Power Out of Range of all optical channels.

Note: This alarm is also raised when the line facility loopback is active on the 10G OTR or 10G OTSC circuit packs and Rx fiber on the client port is disconnected.

Impact

Major, service-affecting (M, SA) alarm, unprotected

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

The alarm severity for the 10G AM1/AM2 circuit pack is always

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

Prerequisites

To perform this procedure, you must:

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0
- have an antistatic wrist strap to dissipate electrostatic charges
- have the optical fiber connection information (that is, how the optical modules on each network element connect to other network elements)
- have an optical power meter with the same optical connectors as the network element

Step	Action
1	Identify the circuit pack and facility raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” in Part 1 of this document.
2	Check the corresponding upstream circuit pack and photonic layer for failures or alarms. Troubleshoot these alarms/failures before proceeding.

Procedure 5-201 (continued)

Rx Power Out of Range

Step	Action								
3	<p>In the Site Manager Configuration menu, select the Equipment & Facility Provisioning application. Select the alarmed facility and retrieve the value from the Rx Actual Power (dBm) column of the facility table. (For 100G OCI or 40G OCI that use parallel optics CFPs, this parameter is Rx Actual High Power [dBm] or Rx Actual Low Power [dBm]). Refer to the “Retrieving optical power, wavelength, and dispersion ranges” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i>, 323-1851-310.</p> <p>If the received power is out of the power monitoring range for the facility, the Rx Actual Power (dBm) column will display “OOR-HI” or “OOR-LO” instead of a numerical value.</p>								
4	<p>Click on the Ranges button to compare the Rx Actual Power (dBm) value (Rx Actual High Power [dBm] or Rx Actual Low Power [dBm] value for 100G OCI) with the Rx minimum power (dBm) and Rx maximum power (dBm) values displayed. Record these values.</p>								
5	<p>Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.</p>								
6	<p>Use the optical power meter to measure the optical power level into the Rx interface.</p> <table style="width: 100%; border-collapse: collapse;"> <tr> <th style="text-align: left; width: 40%;">If the optical power is</th> <th style="text-align: right; width: 60%;">Then go to</th> </tr> <tr> <td style="padding-left: 10px;">less than the Rx minimum value in step 4</td> <td style="text-align: right; padding-right: 10px;">step 7</td> </tr> <tr> <td style="padding-left: 10px;">greater than the Rx maximum value in step 4</td> <td style="text-align: right; padding-right: 10px;">step 8</td> </tr> <tr> <td style="padding-left: 10px;">within the Rx minimum power to Rx maximum power range</td> <td style="text-align: right; padding-right: 10px;">step 11</td> </tr> </table>	If the optical power is	Then go to	less than the Rx minimum value in step 4	step 7	greater than the Rx maximum value in step 4	step 8	within the Rx minimum power to Rx maximum power range	step 11
If the optical power is	Then go to								
less than the Rx minimum value in step 4	step 7								
greater than the Rx maximum value in step 4	step 8								
within the Rx minimum power to Rx maximum power range	step 11								

Procedure 5-201 (continued)

Rx Power Out of Range

Step	Action				
7	Check the fibers for damage and ensure connections are mated properly and verify the fiber cleanliness between the subtending equipment and the port reporting the alarm. Go to step 11 .				
8	The signal may require padding, or you are using an incorrect pluggable type on the circuit pack reporting the alarm or an incorrect subtending pluggable type/circuit pack type. Contact your next level of support or your Ciena support group if you require more information.				
9	If the original alarm has Then <table> <tr> <td>cleared</td> <td>the procedure is complete</td> </tr> <tr> <td>not cleared</td> <td>restart the circuit pack reporting the alarm. Refer to the “Restarting a circuit pack or shelf processor” procedure in Part 1 of this document.</td> </tr> </table>	cleared	the procedure is complete	not cleared	restart the circuit pack reporting the alarm. Refer to the “Restarting a circuit pack or shelf processor” procedure in Part 1 of this document.
cleared	the procedure is complete				
not cleared	restart the circuit pack reporting the alarm. Refer to the “Restarting a circuit pack or shelf processor” procedure in Part 1 of this document.				
10	If the original alarm has Then <table> <tr> <td>cleared</td> <td>the procedure is complete</td> </tr> <tr> <td>not cleared</td> <td>reseat the circuit pack reporting the alarm. Refer to the “Reseating a circuit pack” procedure in <i>Fault Management - Module Replacement</i>, 323-1851-545.</td> </tr> </table>	cleared	the procedure is complete	not cleared	reseat the circuit pack reporting the alarm. Refer to the “Reseating a circuit pack” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.
cleared	the procedure is complete				
not cleared	reseat the circuit pack reporting the alarm. Refer to the “Reseating a circuit pack” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.				
11	If the original alarm has Then <table> <tr> <td>cleared</td> <td>the procedure is complete</td> </tr> <tr> <td>not cleared</td> <td>replace the pluggable module on the circuit pack reporting the alarm. Refer to the procedure in <i>Fault Management - Module Replacement</i>, 323-1851-545.</td> </tr> </table>	cleared	the procedure is complete	not cleared	replace the pluggable module on the circuit pack reporting the alarm. Refer to the procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.
cleared	the procedure is complete				
not cleared	replace the pluggable module on the circuit pack reporting the alarm. Refer to the procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.				
12	If the original alarm has Then <table> <tr> <td>cleared</td> <td>the procedure is complete</td> </tr> <tr> <td>not cleared</td> <td>replace the pluggable module on the subtending circuit pack or the subtending circuit pack. Refer to the procedure in <i>Fault Management - Module Replacement</i>, 323-1851-545.</td> </tr> </table>	cleared	the procedure is complete	not cleared	replace the pluggable module on the subtending circuit pack or the subtending circuit pack. Refer to the procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.
cleared	the procedure is complete				
not cleared	replace the pluggable module on the subtending circuit pack or the subtending circuit pack. Refer to the procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.				
13	If the alarm does not clear, contact your next level of support or your Ciena support group.				

—end—

Procedure 5-202

Rx Total Loss of Capacity - LCAS

Alarm ID: 924

Probable cause

This alarm is raised against an LCAS-enabled WAN facility of an L2SS, 20G L2SS, PDH gateway, or SuperMux circuit pack. The alarm is raised when all Rx LCAS group members are in a failed state and unable to receive data, resulting in a total loss of capacity in the receive direction.

ATTENTION

If the Rx Total Loss of Capacity - LCAS alarm raised, then the Tx Total Loss of Capacity - LCAS and Tx Partial Loss of Capacity - LCAS alarms cannot be raised. The LCAS-enabled WAN cannot receive the LCAS protocol from the far-end network element since there are no active Rx members.

Therefore, no Tx LCAS alarms can be raised at the same time. This is characteristic of the LCAS standard.

Impact

Minor, non-service-affecting (m, NSA) alarm, protected
Major, service-affecting (M, SA) alarm, unprotected

Prerequisites

To perform this procedure, you require an account with at least level 3 UPC.

Step	Action
1	Identify the circuit pack raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document.
2	Look for any other alarms in the active alarm list that are against the WAN facility on the near-end and far-end. Use the appropriate alarm clearing procedure to clear the alarm.
3	Verify that the number of VCAT members provisioned at the near-end and far-end network elements match. Refer to the “Retrieving VCAT members of a virtual concatenation group (VCG)” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
4	If the number of VCAT members Then go to
	match step 6
	do not match step 5

Procedure 5-202 (continued) **Rx Total Loss of Capacity - LCAS**

—end—

Procedure 5-203

Secondary alarms

Use this procedure to clear secondary alarms caused by higher order alarms (for example, Loss of Signal or Loss of Frame) at upstream/downstream locations or when a facility is put in the OOS state or a connection is deleted at upstream/downstream locations.

These alarms are only applicable to the OTN switching, MSPP and Broadband services. Unless otherwise indicated, an alarm applies to all three services.

AIS (OC/STM)

Alarm ID: (7, 34, 148, 892, 285, 1690)

Probable cause

This alarm is raised when the network element detects an OC-1, OC-3/STM-1/STM-1J/STM-1e, OC-12/STM-4/STM-4J, OC-48/STM-16, OC-192/STM-64 or OC-768/STM-256 AIS in the SONET/SDH line overhead

OC/STM AIS alarms are caused by one of the following conditions on the circuit pack that is the source of the alarmed signal:

- a facility is out-of-service
- a circuit pack has failed on the OC-1, OC-3/STM-1, OC-12/STM-4, OC-48/STM-16, OC-192/STM-64, OC-768/STM-256, or STM-1e circuit pack
- a circuit pack has failed on the DSM 84xDS1 termination module (TM)
- the site address for the DS1 service module (DSM) is not defined

This alarm is also raised when optics are provisioned as 2-Fiber/4-Fiber BLSR/MS-SPRing/HERS, but no ringmap has been entered. AIS is sent by the 2-Fiber/4-Fiber BLSR/MS-SPRing/HERS engine until it becomes active. A nodemap must be provisioned for the engine to become active.

Impact

Critical, service-affecting (C, SA) alarm for a UPSR/SNCP configuration with cross-connects

Critical, service-affecting (C, SA) alarm, if active 1+1/MSP linear or unprotected with cross-connects

Critical, service-affecting (C, SA) alarm for an unprotected 2-Fiber/4-Fiber BLSR/MS-SPRing/HERS

Minor, non-service-affecting (m, NSA) alarm if inactive 1+1/MSP linear, protected 1+1/MSP linear, or without cross-connects

Minor, non-service-affecting (m, NSA) alarm for a protected 2-Fiber/4-Fiber BLSR/MS-SPRing

AIS (STS/HO VC)

Alarm ID:(11, 48, 114, 189, 278, 460, 466)

Probable cause

This alarm is raised when the network element detects STS-1/VC-3, STS-3c/VC-4, STS-12c/VC-4-4c, STS-24c/VC-4-8c, STS-48c/VC-4-16c, or STS-192c/VC-4-64c AIS in the SONET/SDH path overhead.

STS/HO VC AIS alarms are caused by one of the following conditions at the far-end or passthrough network elements:

- an incoming signal is missing or errored at the far-end
- a circuit pack is failed at the far-end
- a loss of pointer alarm is raised at a passthrough connection to the optical interface
- the traffic is destined for an unreachable node in a 2-Fiber/4-Fiber BLSR/MS-SPRing/HERS configuration (traffic squelched)

This alarm can also be raised if an intrusive test access session is in progress. No action is required if this is the cause.

Impact

Minor, service-affecting (m, SA) alarm if on an active path

Minor, non-service-affecting (m, NSA) alarm if on an inactive path in a UPSR/SNCP configuration

The alarm status is minor because it is a secondary alarm that indicates a problem upstream of this network element.

AIS (VT/LO VC)

Alarm ID:(55, 238)

Probable cause

This alarm is raised when the network element detects VT1.5/VC11 or VT2/VC12 AIS in the SONET/SDH path overhead.

VT1.5/VC11 and VT2/VC12 AIS alarms are caused by one of the following conditions at the far-end or passthrough network elements:

- an incoming signal is missing or errored at the far-end
- a circuit pack is failed at the far-end
- STS/HO VC faults at a passthrough network element

Procedure 5-203 (continued)

Secondary alarms

Impact

Minor, service-affecting (m, SA) alarm if on an active path

Minor, non-service-affecting (m, NSA) alarm if on an inactive path in a UPSR/SNCP configuration

The alarm status is minor because it is a secondary alarm that indicates a problem upstream of this network element.

AIS (OC48/192/768/STM16/64/256 for converged Broadband and Photonic services)

Alarm ID: (7, 285, 987)

Probable cause

This alarm is raised when the client Rx interface or line interface (for SuperMux circuit pack) detects OC-48/OC-192/OC768 AIS in the SONET line overhead or STM-16/STM-64/STM256 AIS in the SDH MS overhead.

Impact

Critical, service-affecting (C, SA) alarm

AIS (OTUTTP, STTP, PATH, PDH)

Alarm ID:(1450, 1462, 2083, 2063)

Probable cause

This alarm is raised when the network detects SONET Line-AIS in the SONET/SDH line overhead. On OTN capable circuit packs (such as eMOTR), the alarm is raised at the OTU layer.

Impact

Critical, service-affecting (C, SA) alarm

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

Warning

Laser Off Far End Failure Triggered (OC48/STM16, OC192/STM64, OC768/STM256, ETH10G, ETH40G, ETH100G, OTM1, OTM2, OTM3, PTP, FC800, FC1200 for Broadband services)

Alarm ID: (676, 678, 839, 967, 988, 1219, 1243, 1285, 1301, 1375, 1438)

Probable cause

This alarm is raised to indicate the client Tx laser is shut down after detecting a remote failure or the upstream circuit pack client facility is in the OOS state.

Impact

Critical, service-affecting (C, SA) alarm if not protected

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

Local Fault (ETH10G, ETH40G, ETH100G, FC800, FC1200, ETTP)

Alarm ID: (674, 965, 1259, 1299, 1455)

Probable cause

This alarm is raised when the client Rx interface detects a 802.3ae local fault (LF).

Impact

Critical, service-affecting (C, SA) alarm if not protected

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

ODU AIS (OTMFLEX, OTM0, OTM1, OTM2, OTM3, OTM4 for Broadband services, ODUTTP, ODUCTP, ODU0, ODU1, ODUFLEX, TCMCTP, TCMTTP)

Alarm ID: (662, 992, 1160, 1468, 1477, 1478, 1495, 1496, 1608, 1729)

Probable cause

This alarm is raised when the Rx interface detects an ODU layer (path monitoring) AIS. The upstream Tx interface is sending ODU layer AIS. This can occur when the upstream OTMFLEX, ODUCTP, OTM0, OTM2, OTM3, or OTM4 facility is in the OOS state or when the upstream circuit pack is reporting a circuit pack fail.

This alarm is also raised on all of the 40G and 100G Line cards when ODU monitoring is Yes. ODU monitoring is Yes by default when 1+1 Line protection is provisioned on 40G Line cards.

This alarm can also be raised when proper payload index assignment is not used for circuit packs that interwork with the 2.5G MOTR circuit packs (NTK530NAE5 and NTK530NCE5). For more information about proper payload index assignment when interworking with these circuit packs, refer to the Part 1 of *Configuration - Bandwidth and Data Services*, 323-1851-320.

Procedure 5-203 (continued)

Secondary alarms

Impact

Critical, service-affecting (C, SA) alarm

Major, service-affecting (M, SA) alarm

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

ODU BDI (OTMFLEX, ODUTTP, ODUCTP, ODU0, ODU1, ODUFLEX, TCMCTP, TCMTTP)

Alarm ID: (664, 993, 1161, 1469, 1479, 1480, 1493, 1494, 1606, 1730)

Probable cause

This alarm is raised when the Rx interface detects an ODU layer (path monitoring) BDI (Backward Defect Indication). The upstream Tx interface sends ODU BDI when its Rx interface detects ODU failures.

This alarm is also raised on all of the 40G and 100G Line cards when ODU monitoring is Yes. ODU monitoring is Yes by default when 1+1 Line protection is provisioned on 40G Line cards.

When Alarm Correlation is enabled (see “Editing the nodal system parameters” procedure in *Administration and Security*, 323-1851-301), the behavior of this alarm is driven by the Conditioning Override parameter (see the “Editing the nodal system parameters” in *Administration and Security*, 323-1851-301) with the exception of OTMn/OTU client facilities with no Actual Far-End Address discovered by SPLI (see SPLI in *Administration and Security*, 323-1851-301) where this alarm is always enabled. This exception is to support interworking between the 6500 node and non-Ciena client equipment which does not support Alarm Correlation.

Impact

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

OPU AIS (OTM0, OTM1, OTM2, OTM3, or OTM4 for Broadband services, ODUCTP, ETTP, STTP, ODUTTP)

Alarm ID: (964, 1011, 1181, 1487, 1624, 1670, 1677)

Probable cause

This alarm is raised when the Rx interface detects an OPU layer (path monitoring) AIS. The upstream Tx interface is sending OPU layer AIS. This can occur when the upstream client signal cannot be provided for mapping into the OPU payload. A PN11 pattern is mapped into the OPU as a client payload generic AIS.

Impact

Critical, service-affecting (C, SA) alarm

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

OTU BDI (OTUTTP, OTM1, OTM2, OTM3, or OTM4 for Broadband services)

Alarm ID: (665, 1002, 1171, 1446)

Probable cause

This alarm is raised when the Rx interface detects an OTU layer (section monitoring) BDI (Backward Defect Indication). The upstream Tx interface sends OTU BDI when its Rx interface detects OTU failures.

When Alarm Correlation is enabled, (see the “Editing the nodal system parameters” procedure in *Administration and Security*, 323-1851-301) the behavior of this alarm is driven by the Conditioning Override parameter (see the “Editing the nodal system parameters” in *Administration and Security*, 323-1851-301) with the exception of OTMn/OTU client facilities with no Actual Far-End Address discovered by SPLI (see SPLI in *Administration and Security*, 323-1851-301) where this alarm is always enabled. This exception is to support interworking between the 6500 node and non-Ciena client equipment which does not support Alarm Correlation.

Impact

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

RFI (OC)

Alarm ID: (6, 37, 149, 284, 895, 986, 1693)

Probable cause

This alarm is raised when the network element detects a OC/STM remote fault indication (RFI) in the SONET line overhead because of a fault on another network element, or an optical fiber/cable has been cut.

Also, this alarm is raised if the site address for an attached DS1 service module (DSM) is not defined.

This alarm is also raised when optics are provisioned as 2-Fiber/4-Fiber BLSR/MS-SPRing/HERS, but no ringmap has been entered. AIS is sent by the 2-Fiber/4-Fiber BLSR/MS-SPRing/HERS engine until it becomes active. A nodemap must be provisioned for the engine to become active.

Impact

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

RFI (STS)

Alarm ID: (14, 52, 117, 192, 277, 462, 468)

Probable cause

This alarm is raised when the network element detects an STS remote fault/defect indication (RFI) in the SONET/SDH line overhead because of a fault on another network element, or an optical fiber/cable has been cut.

Procedure 5-203 (continued)

Secondary alarms

Impact

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

The alarm status is minor because it is a secondary alarm that indicates a problem upstream of this network element.

RFI (VT)

Alarm ID: (61, 241)

Probable cause

This alarm is raised when the network element detects an VT remote fault indication (RFI) in the SONET line overhead because of a fault on another network element, or an optical fiber/cable has been cut.

Impact

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

The alarm status is minor because it is a secondary alarm that indicates a problem upstream of this network element.

RFI (PATH)

Alarm ID: (2087)

Probable cause

This alarm is raised when the client Rx interface detects PATH RFI in the SONET line overhead.

Impact

Warning

RFI (STTP)

Alarm ID: (1463)

Probable cause

This alarm is raised when the client Rx interface detects STTP RFI in the SONET line overhead.

Impact

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

Remote Fault (ETTP)

Alarm ID: (675, 966, 1260, 1300, 1456)

Probable cause

This alarm is raised when the client Rx interface detects 802.3ae remote fault.

Impact

Critical, service-affecting (C, SA) alarm if not protected
Minor, non-service-affecting (m, NSA) alarm if protected

Prerequisites

To perform this procedure, you must

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0
- have an antistatic wrist strap to dissipate electrostatic charges
- have the network connection information (that is, how the interface circuit packs on each network element connect to other network elements and how each OC-3 connects to the DSM)

Step	Action	
1	If the alarm is	Then go to
	RFI, BDI or Remote Fault	step 8
	otherwise	step 2
2	If this is a 2-Fiber/4-Fiber BLSR/MS-SPRing/HERS configuration, verify if the 2-Fiber/4-Fiber BLSR/MS-SPRing/HERS ringmap has been provisioned. If not, provision the 2-Fiber/4-Fiber BLSR/MS-SPRing/HERS ringmap. Refer to the “Retrieving BLSR/MS-SPRing/HERS configuration information” procedure in Part 1 of <i>Configuration - Bandwidth and Data Services</i> , 323-1851-320.	
3	Verify if there are alarms of higher order from the alarm hierarchy. Refer to the “Alarm hierarchies and alarm severities” chapter in Part 1 of this document. First, clear any alarms of higher order in the hierarchy on the 6500 system or the subtending equipment using the appropriate procedures. You can also refer to the signal conditioning section in chapter 1 of this document to help troubleshoot secondary alarms.	
4	At the local network element, retrieve all alarms to determine if the original alarm has cleared.	

Procedure 5-203 (continued)

Secondary alarms

Step	Action
5	If the original alarm has cleared raised was STS/HO VC AIS, and the alarm has not cleared was another and has not cleared
	Then the procedure is complete verify if the Traffic Squelched alarm is raised. Refer to the alarm clearing procedure for “Traffic Squelched” on page 5-578. Then go to step 6 .
6	At the local network element, retrieve all alarms to determine if the original alarm has cleared.
7	If the original alarm has cleared not cleared
	Then the procedure is complete go to step 8
8	Identify the circuit pack raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document.
9	If a Local fault alarm is raised on an eMOTR SFP+ port, ensure the rate of the incoming traffic is matched with what the port is provisioned for. Refer to the “Retrieving equipment and facility details” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
10	If the shelf is equipped with a DSM not equipped with a DSM
	Then go to step 11 step 14
11	If a DSM is connected to the alarmed OC-3 circuit pack, retrieve the active alarms from the network element and verify if the Site Provisioning Required (DSM) alarm is also raised. If yes, use the appropriate procedure to clear the alarm.
12	Wait two to five minutes.
13	If the original alarm has cleared not cleared
	Then the procedure is complete go to step 14
14	Use the optical fiber/cable connection information to identify the transmit and receive sites of the alarmed signal.
15	If an RFI alarm is raised on a 2.5G MOTR SFP/XFP, ensure the SFP/XFP is fully inserted properly.

Procedure 5-203 (continued)

Secondary alarms

Step	Action						
16	If the network element is not connected to a 6500 network element at the remote end, or if the network element is part of a mid-span meet and the remote network element is from another vendor, use the alarm system of the other vendor to find the problem.						
17	Log into the remote network element at the transmit end. If you cannot log in remotely from the local network element, you must travel to the remote site.						
18	Retrieve all alarms from the remote network element at the transmit end.						
19	Look for an alarm message for the remote network element circuit pack connected to the original shelf.						
20	<table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 30%; text-align: left; padding-bottom: 5px;">If there are</th><th style="width: 70%; text-align: left; padding-bottom: 5px;">Then</th></tr> </thead> <tbody> <tr> <td style="width: 30%;">no alarms at the transmit end</td><td style="width: 70%;">ensure that the equipment and facility or the client and line facilities of the remote circuit pack are in-service and connected. Refer to the "Retrieving equipment and facility details" procedure in Part 1 of <i>Configuration - Provisioning and Operating</i>, 323-1851-310. Go to step 21.</td></tr> <tr> <td style="width: 30%;">additional alarms at the transmit end</td><td style="width: 70%;">refer to the appropriate alarm clearing procedures. The RFI alarm can be ignored if the local alarm is AIS, Loss of Pointer, or Network Trace Identifier Mismatch, or Unequipped. Go to step 21.</td></tr> </tbody> </table> <p>The setting of the RFI condition as a consequence of a Network Trace Identifier Mismatch, or Unequipped alarm is user provisionable.</p>	If there are	Then	no alarms at the transmit end	ensure that the equipment and facility or the client and line facilities of the remote circuit pack are in-service and connected. Refer to the "Retrieving equipment and facility details" procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310. Go to step 21 .	additional alarms at the transmit end	refer to the appropriate alarm clearing procedures. The RFI alarm can be ignored if the local alarm is AIS, Loss of Pointer, or Network Trace Identifier Mismatch, or Unequipped. Go to step 21 .
If there are	Then						
no alarms at the transmit end	ensure that the equipment and facility or the client and line facilities of the remote circuit pack are in-service and connected. Refer to the "Retrieving equipment and facility details" procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310. Go to step 21 .						
additional alarms at the transmit end	refer to the appropriate alarm clearing procedures. The RFI alarm can be ignored if the local alarm is AIS, Loss of Pointer, or Network Trace Identifier Mismatch, or Unequipped. Go to step 21 .						
21	At the local network element, retrieve all alarms to determine if the original alarm has cleared.						

Procedure 5-203 (continued)

Secondary alarms

Step	Action	Then
22	If the original alarm has cleared raised was STS/HO VC AIS or STS/LO VC AIS, and the alarm has not cleared raised was OC/STM AIS, and the alarm has not cleared raised was STS/HO VC RFI, and the alarm has not cleared raised was OC/STM or STS/LO VC RFI, and the alarm has not cleared raised was against OTUTTP, ODUTTP, STTP, or ETTP facility and the alarm has not cleared raised was otherwise, and the alarm has not cleared	the procedure is complete go to step 23 go to step 25 go to step 27 go to step 30 go to step 28 go to step 30
23	Log into each of the passthrough network elements and retrieve alarms.	
24	Verify if there are alarms of higher order from the alarm hierarchy. Refer to the “Alarm hierarchies and alarm severities” chapter in Part 1 of this document. Clear any alarms of higher order on the hierarchy first using the appropriate procedures. Go to step 29 .	
25	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.	
26	Replace the local circuit pack or DSM 84xDS1 TM reporting the original alarm. Refer to the “Replacing an optical interface circuit pack” or “Replacing the DSM 84xDS1 TM circuit pack” procedures in <i>Fault Management - Module Replacement</i> , 323-1851-545. Go to step 29 .	
27	Verify the fiber connection for the interface circuit pack that connects to the original shelf. Repair, clean, and reconnect the fiber as required. While this alarm is active, Section/RS DCC Link Failure or Line/MS DCC Link Failure alarms may be raised. These alarms clear automatically after the RFI alarm is cleared. Go to step 29 .	

Procedure 5-203 (continued)

Secondary alarms

Step	Action
28	Verify that the provisioned line rate on the upstream circuit pack matches the line rate on the local circuit pack. Correct any mismatches. Refer to the “Retrieving OTM info” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
29	If the original alarm has Then
	cleared the procedure is complete
	not cleared go to step 30
30	Contact your next level of support or your Ciena support group. and

Procedure 5-204

Secondary License Server Unavailable

Alarm ID: 2012

Probable cause

This alarm is raised when the 6500 shelf cannot communicate with the secondary license server/manager.

Impact

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

Step	Action
1	Verify the network connection between the 6500 shelf and the license server/manager.
2	If you are using HTTPS, the correct date and time must be set on the shelf (either manually or using TOD/NTP server provisioning and synchronization). Refer to “Provisioning Time of Day servers” and “Operating a time of day synchronization” procedures in <i>Administration and Security</i> , 323-1851-301.
3	If you set the time after provisioning licensing, then perform a manual audit after setting the shelf time to clear the license server comms error. Refer to “Operating a license audit on the 6500” procedure in <i>Administration and Security</i> , 323-1851-301.
4	Verify that the secondary license server/manager is provisioned and is not down. Refer to “Provisioning License Manager/Server information on the 6500” procedure in <i>Administration and Security</i> , 323-1851-301.
5	It can take up to 12 hours for the alarm to clear as, in steady state, the heartbeat is run every 12 hours. Run a manual audit which will reset the heartbeat to two minutes after which the heartbeat interval will gradually increase in time to the steady state time of 12 hours. Refer to “Operating a license audit on the 6500” procedure in <i>Administration and Security</i> , 323-1851-301. The alarm will clear two minutes after the manual audit is run.
6	If the alarm does not clear, contact your next level of support or Ciena support group.

—end—

Procedure 5-205

Secondary RADIUS Accounting Server Unavailable

Alarm ID: 1517

Probable cause

This alarm is raised when no response is received from the secondary RADIUS accounting server during user-provisioned timeout.

This alarm is also raised when the RADIUS accounting server provisioning on the network element is incorrect.

This security alarm is raised against an SP, SP-2, SPAP, SPAP-2 w/2xOSC, or an integrated shelf processor on a 8xOTN Flex MOTR circuit pack.

This alarm is raised for an IPv4 and/or IPv6 provisioned server. IPv6 must be enabled if an IPv6 server is provisioned and IPv4 must be enabled if an IPv4 server is provisioned.

Impact

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

Prerequisites

To perform this procedure, you require an account with at least a level 4 UPC.

Step	Action
1	Disable the server on 6500.
2	Re-enable the server and log in or log out of the server.
3	If the alarm is raised again, disable the RADIUS accounting feature and log in or log out of the server.
4	If the alarm is raised, ensure the following RADIUS accounting server provisioning values on the network element are correct: <ul style="list-style-type: none">• server IP address• server port• shared secret• timeout - If this value is too small, the server may not be able to respond quickly enough.
	Refer to the “Provisioning the primary or secondary RADIUS server” procedure in <i>Administration and Security</i> , 323-1851-301.
5	Check the status of the RADIUS accounting server. Ensure the status is ON.

Procedure 5-205 (continued)

Secondary RADIUS Accounting Server Unavailable

Step	Action
6	Log in or log out of the network element. This will send a RADIUS accounting message to all provisioned RADIUS accounting servers. The alarm will clear if a response is received from the server(s) within the provisioned timeout.
7	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-206

Secondary RADIUS Server Unavailable

Alarm ID: 584

Probable cause

This alarm is raised when all requests to the secondary RADIUS server of a SP times out and a primary RADIUS server is provisioned.

If only the secondary RADIUS server is provisioned (no primary RADIUS server provisioned) and all requests time out, the All Provisioned RADIUS servers Unavailable alarm is raised (refer to the “All Provisioned RADIUS Servers Unavailable” alarm clearing procedure in Part 1 of this document).

This alarm is raised for an IPv4 and/or IPv6 provisioned server. IPv6 must be enabled if an IPv6 server is provisioned and IPv4 must be enabled if an IPv4 server is provisioned.

The alarm is not raised due to server time out.

Impact

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

Prerequisites

To perform this procedure, you require an account with at least a level 4 UPC.

Step	Action
1	Make sure the secondary RADIUS server of the SP is enabled and has a valid IP address. Refer to the “Retrieving the centralized security administration details” procedure in <i>Administration and Security</i> , 323-1851-301.
2	Log into the network element again using the RADIUS authentication (centralized security administration).
3	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-207 Secondary Service Failed

Alarm ID: 1261

Probable cause

This alarm is raised when:

- the External Slot Inventory Interface Devices have failed
- the wrong LAN cable type is used to connect to passive modules. The I2C interface supports only straight LAN cables.
- the LAN cable connected to passive modules is too long.
- internal faults for non-essential services are detected between the SP and Access Panel.

Impact

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

Prerequisites

To perform this procedure, you require an account with at least a level 4 UPC.

Step	Action
1	Select Active Alarms from the Faults menu in Site Manager to retrieve alarms. Refer to the alarms and events procedures in Part 1 of <i>Fault Management - Alarm Clearing</i> , 323-1851-543. Record the current state of the system. Note: Perform the following actions until the alarm clears. After each step, if the alarm does not return after 10 minutes then the procedure is complete. Otherwise, go to the next step.
2	If there is a passive module connected to the Access Panel, then <ol style="list-style-type: none"> a. If a crossover LAN cable is being used, replace the cable with a straight LAN cable. b. If the LAN cable is more than 3m in length, replace the cable with a cable that is 3m or shorter.
3	Perform a warm restart on the active shelf processor. Refer to the “Restarting an interface module or the shelf processor” procedure in Part 1 of this document.

Secondary Service Failed

Step	Action
4	If there is a passive module connected to the Access Panel, reseat the LAN cable connecting it to the Access Panel, at both ends.
5	If 1+1 SP protection is provisioned, then perform a protection switch to the other shelf processor.
6	Reseat the original active SP. Refer to “Reseating a circuit pack” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.
7	Replace the original active SP if it has not been replaced within the past 48 hours. Refer to “Replacing a shelf processor” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.
8	Perform a protection switch back to the original active SP, and reseat the original standby SP.
9	Replace the original standby SP if it has not been replaced within the past 48 hours. Refer to “Replacing a shelf processor” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.
10	Reseat the Access Panel.
11	Replace the Access Panel if it has not been replaced within the past 48 hours. Refer to “Replacing an access panel” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.
12	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-208

Secondary SETS Locking to Primary

Alarm ID: 586

Probable cause

This alarm is raised while the synchronization equipment timing source (SETS) on the secondary cross-connect, or SuperMux circuit pack is locking to the SETS on the primary cross-connect, or SuperMux circuit pack.

On a (1+8)xOTN Flex MOTR circuit pack, this alarm is raised when the slave (even slot) tries to lock to the Master circuit pack (odd slot). This is done on the first mate cross-connection provisioning time.

This alarm is also raised when the mate cross-connect circuit pack is OOS.

ATTENTION

The “Secondary SETS Locking to Primary” alarm is raised after a cross-connect or SuperMux circuit pack is inserted into the shelf during a cross-connect or optical interface circuit pack reconfiguration. The alarm indicates that the newly inserted cross-connect circuit pack or SuperMux is locking to the SETS on the existing cross-connect or SuperMux circuit pack. Wait until the alarm clears before proceeding with the cross-connect or optical interface circuit pack reconfiguration/replacement procedure.

ATTENTION

This alarm is raised on the (1+8)x OTN Flex MOTR circuit pack in an even slot number when the first connection is made between adjacent (1+8)x OTN Flex MOTR circuit packs or when one of the 2 circuit packs is cold restarted or replaced. The alarm can stay active for up to two minutes and will clear once the card in the even slot number has synchronized to the card in the odd slot number. While the alarm is active, inter-card traffic between the cards is conditioned. If the even slot card fails to synchronize to the odd slot card, this alarm is replaced with an Intercard Suspect alarm.

The alarm clears when the secondary SETS has locked successfully.

Secondary SETS Locking to Primary

Equipment protection of the cross-connect circuit packs is unavailable while this alarm is raised.



CAUTION

Risk of service interruption

If you place a cross-connect circuit pack out-of-service or open the latch on a cross-connect circuit pack while this alarm is raised, you can cause loss of traffic.

Impact

Warning

Step Action

- 1** Log into the NE and verify the primary state of the mate cross-connect circuit pack. If the primary state is OOS-MA, change it to IS.
- 2** If the alarm does not automatically clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-209

Server Certificate About to Expire (6500)

Alarm ID: 1961

Probable cause

This alarm is raised when a server certificate on the SP is about to expire based on a provisioned number of days before the certificate expiry.

Impact

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

Step	Action
1	Connect to the NE using the Site Manager.
2	In the Security menu click on the Manage keys and choose SSL Keys .
3	On the SSL Keys screen, select the shelf whose certificate is about to expire.
4	Click on Regenerate button to regenerate the public and private keys.
5	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-210 Server Certificate Expired (6500)

Alarm ID: 1960

Probable cause

This alarm is raised when a server certificate on the SP is expired.

Impact

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

Step	Action
1	Connect to the NE using the Site Manager.
2	In the Security menu click on the Manage keys and choose SSL Keys .
3	On the SSL Keys screen, select the shelf whose certificate is about to expire.
4	Click on Regenerate button to regenerate the public or private keys or click on the Upload Certificate to upload the user certificate. The alarm will clear when the operation is successful.
5	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-211 Service Defect Indication

Alarm ID: 1741, 2060

Probable cause

This alarm is raised when the ETTP service on an eMOTR circuit pack has failed or is operationally disabled and conditioned because of VLLI/iVLLI (Inverse Virtual Link Loss Indicator).

This alarm is also raised on PKT/OTN when an ETTP is conditioned because of VLLI.

This alarm is an indication from the 6500 SNMP interface that there is a L2 service-impacting alarm against the ring protection or Connectivity Fault Management (CFM) associated with the eMOTR port. The alarm is raised when a G.8032 protection switch is active on the eMOTR circuit pack.

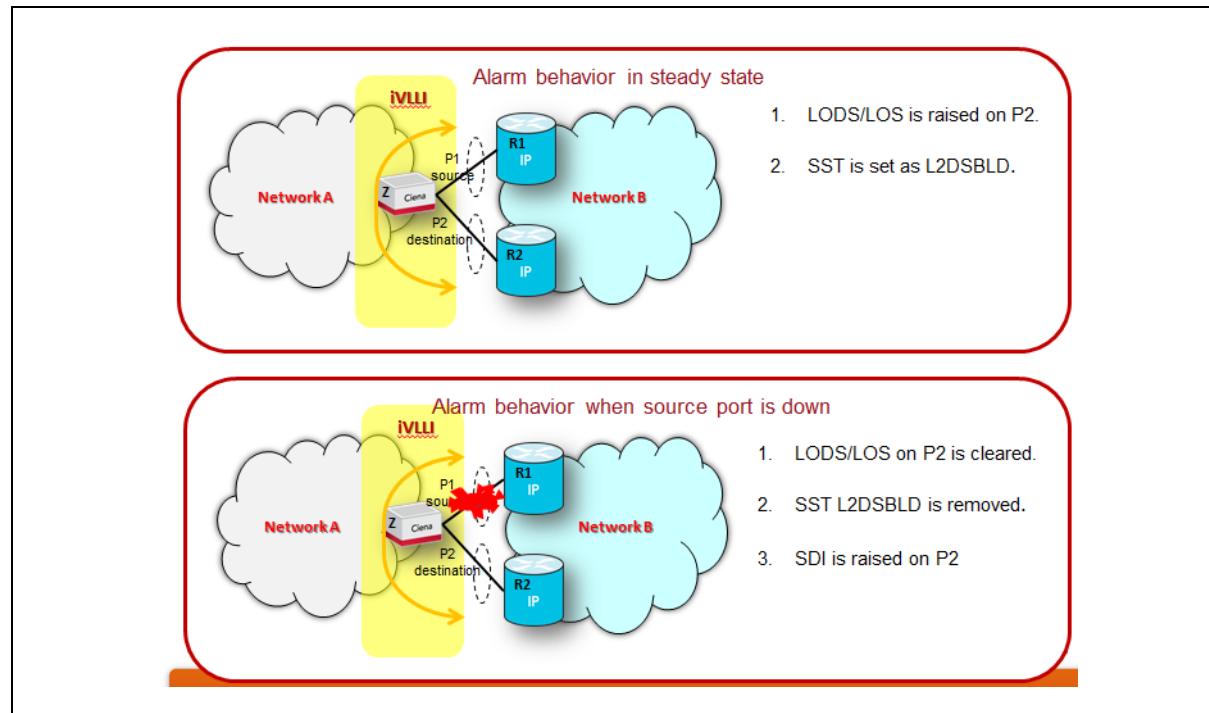
For eMOTR circuit packs, SDI alarm is also raised by iVLLI on backup port indicating that iVLLI is active on that port (when active port goes down and backup port comes up). See [Figure 5-2](#) and [Figure 5-3 on page 5-487](#).

This alarm is raised against a PKTIWF or ETTP facility of PTS MRO IF 2xSFP+/14xSFP, or PTS XC 800G, or PTS PDH I/F 2xDIM circuit pack when there is an alarmable condition detected in SAOS. For details refer to *SAOS-based Packet Services Fault and Performance*, 323-1851-650.

Procedure 5-211 (continued)

Service Defect Indication

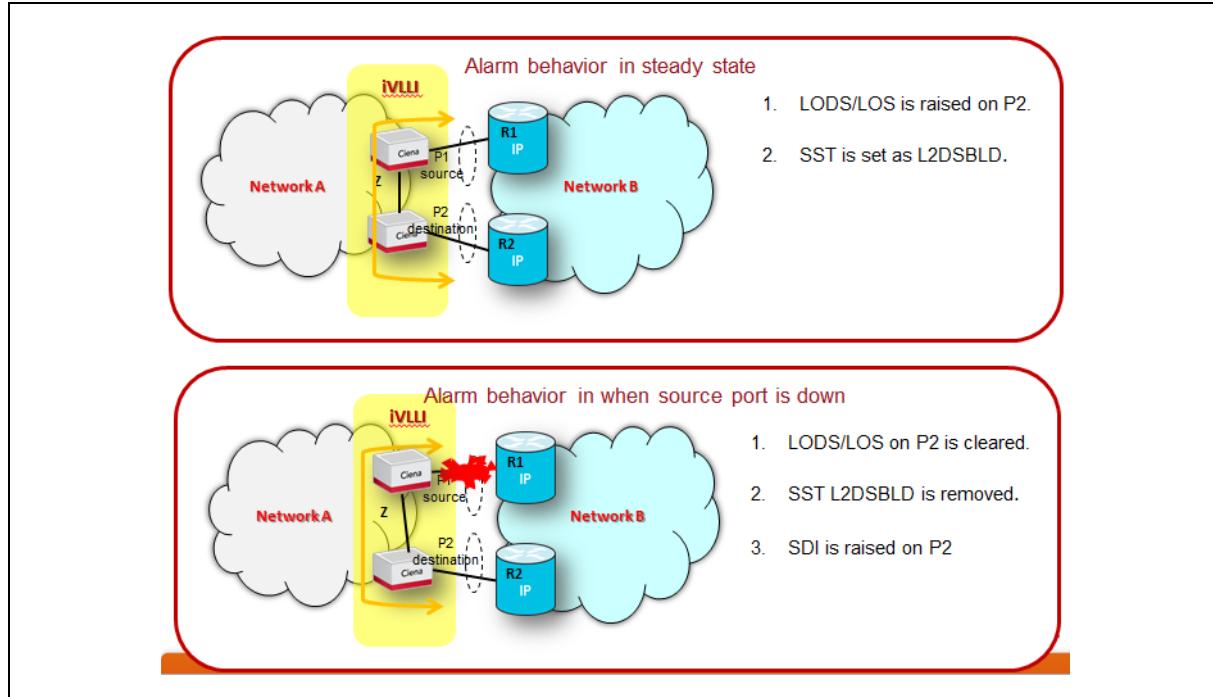
Figure 5-2
Single homed configuration



Note: The “Far End Client Signal Fail”, “Remote Port Unreachable” and “Remote Port OOS” alarms are not relevant in case of single-homed resilient handoff application.

Procedure 5-211 (continued)
Service Defect Indication

Figure 5-3
Dual homed configuration



Impact

Critical, service-affecting (C, SA) alarm
 Minor, non-service-affecting (m, NSA) alarm

Prerequisites

To perform this procedure, you require an account with at least a level 3 UPC.

Step	Action
1	Log into the SAOS CLI and examine the alarms and status of all the configured services. Refer to the <i>SAOS-based Packet Services Command Reference</i> , 323-1851-610, for information on retrieving alarm, port, Connectivity Fault Management (CFM), VLLI, and ring protection entities.

Procedure 5-211 (continued)

Service Defect Indication

Step	Action
2	Check and correct the L2 alarms and faults including: <ul style="list-style-type: none">• L2 port alarms• missing or mismatched L2 ring protection provisioning at the near-end or far-end• missing or mismatched L2 CFM provisioning at the near-end or far-end• CFM faults and/or VLLI faults
3	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-212 Service Mismatch

Alarm ID: 2027

Probable cause

This alarm is raised against an OTUTTP facility of a WLAI circuit pack.

This alarm indicates that the OTU rate is not aligned at either end of the link.

Impact

Critical, service-affecting (C, SA) alarm

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

Prerequisites

To perform this procedure, you require an account with at least a level 3 UPC.

Step	Action
1	Identify the port where this alarm is being raised and identify the OTUTTP port to which it is currently connected.
2	Verify the provisioned OTU rate at either end of the link. Refer to the “Retrieving equipment and facility details” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
3	If the provisioned OTU rates do not match, correct any mismatches. Refer to the “Editing facility parameters” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
4	If the alarm is not cleared, contact your next level of support or your Ciena support group.

—end—

Procedure 5-213

Shelf Bandwidth Near Limit

Alarm ID: 654

Probable cause

This alarm is raised against the shelf to indicate that the provisioned total network element/shelf bandwidth is approaching the maximum allowed for the shelf.

The alarm is raised when 90% of the total capacity is reached on any cross-connect circuit pack.

In a 7-slot shelf (NTK503RA), this alarm is raised on a system with X-Conn 240G+ STS-1/VC-3 (240/0) (NTK557ES) or X-Conn 240G+/80G VT1.5/VC-12 (240/80) (NTK557GS) circuit pack after using 108 Gb of XC capacity.

Impact

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

Prerequisites

To perform this procedure, you require an account with at least a level 3 UPC.

Step	Action
1	<p>Delete any cross-connects that are not required. Refer to the “Deleting path connections” procedure in Part 1 of <i>Configuration - Bandwidth and Data Services</i>, 323-1851-320.</p> <p>For information about how to calculate the number of cross-connects depending on the connection rate, refer to the “Connection and Bandwidth Management” section in Part 1 of the <i>6500 Planning</i>, NTRN10EG.</p>
2	If more low-order bandwidth is required, contact your network administrator to determine your course of action.

—end—

Procedure 5-214 Shelf Data Missing

Alarm ID: 570

Probable cause

This alarm is raised when the shelf does not have a shelf number provisioned.

Impact

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

Prerequisites

Before you perform this procedure, you must observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0.

Step	Action
1	This alarm clears when the commissioning of the shelf (specifically the shelf number) has been completed successfully. Complete the commissioning of the shelf. Refer to the “Commissioning a network element” procedures in <i>Commissioning and Testing</i> , 323-1851-221 for instructions.
2	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-215

Shelf Power Near Limit

Alarm ID: 981

Probable cause

This alarm is raised against the shelf when the aggregate shelf power usage (**Calculated shelf power**) exceeds the shelf, feeder, fuse, or zone power limit threshold (as provisioned using the **Provisioned shelf current** shelf attribute value).

Impact

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

Prerequisites

To perform this procedure, you require an account with at least a level 3 UPC.

Step	Action
1	Deprovision and remove all equipment from the shelf that is not required. Refer to the “Deleting a facility from an equipment” and “Deleting an ETH or ETH10G facility from a LAG in a 20G L2SS, L2SS, PDH gateway, or RPR circuit pack” procedures in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
2	If the original alarm has Then
	cleared the procedure is complete
	not cleared go to step 3
3	Retrieve the Provisioned shelf current and Shelf current capacity (shelf power available based on equipped Power Input Cards) shelf attribute values. Refer to the “Determining the provisioned shelf current value” procedure in <i>Administration and Security</i> , 323-1851-301.
4	If Provisioned shelf current is Then
	less than or equal to Shelf current capacity go to step 8
	greater than Shelf current capacity upgrade the Power Input Cards to match or exceed the Shelf current capacity value
5	If the original alarm has Then
	cleared the procedure is complete
	not cleared go to step 6

Procedure 5-215 (continued)

Shelf Power Near Limit

—end—

Procedure 5-216

Shutoff Threshold Crossed

Alarm ID: 540

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. For CDC configurations, this alarm is raised on the AMP facility of CCMD 8x16 or CCMD12 circuit packs. 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

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.

This alarm is raised on port 4 of the Fixed Gain Amplifier (FGA C-Band) (NTK552AB).

Prerequisites

To perform this procedure, you must:

- use an account with at least a level 3 UPC
- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0
- have a network and site diagram
- have a fiber cleaning kit
- have the Shutoff threshold level for this amplifier

Impact

Major, service-affecting (M, SA) alarm

Procedure 5-216 (continued)
Shutoff Threshold Crossed

Step	Action
1	Place the alarmed AMP facility out of service (OOS). Refer to the “Changing the primary state of a facility” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
2	Clean and then reconnect the input fibers and connectors at the amplifier. Refer to the cleaning connectors procedures in <i>Installation - General Information</i> , 323-1851-201.0.
3	Place the amplifier back in-service (IS). Refer to the “Changing the primary state of a facility” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
4	If the alarm still persists, check the upstream connection for mating or pinched fibers.
5	If the alarm is against port 8 of an SLA C-Band, MLA C-Band, MLA L-Band, MLA2 C-Band, MLA2 w/VOA, or MLA3 C-Band, check and clean the connection from the incoming line, including any patch panel connections. Refer to the “Cleaning Connectors” chapter in <i>Installation - General Information</i> , 323-1851-201.0.
6	If the alarm is against port 8 of an XLA circuit pack, check and clean the connection to port 7 of the SRA circuit pack and ensure the SRA circuit pack is in-service.
7	If the alarm is raised against port 6 of an MLA C-Band, MLA2 w/VOA, MLA3 C-Band, or XLA, check and clean the connection from the WSS common output as identified in the Table 5-1 .

Table 5-1
WSS common output ports

WSS 100 GHz w/OPM C-Band 2x1 (NTK553JAE5)	port 18
WSS 100 GHz w/OPM C-Band 2x1 (NTK553JB)	port 8
WSS 100 GHz w/OPM 5x1 (NTK553EAE5)	port 18
WSS 100 GHz w/OPM C-Band 4x1(NTK553HA)	port 12
WSS 50 GHz w/OPM 2x1 (NTK553KCE5, NTK553KAE5)	port 8
WSS 50 GHz w/OPM 9x1 (NTK553FAE5, NTK553FC)	port 22
WSS w/OPM Flex C-Band 9x1(NTK553LA)	port 22

Procedure 5-216 (continued)

Shutoff Threshold Crossed

Step	Action
8	If the alarm is against port 8 of the SLA, check and clean the connection from the relevant WSS switch port as follows: <ul style="list-style-type: none">• From the Configuration, Equipment & Facility screen, select the circuit pack identified by the alarm (the provisioned PEC field should equal NTK552AA or NTK552AB: SLA C-Band).• In the Facility Type dropdown box, select “ADJ”.• Locate the adjacency associated with port 5 (the Adjacency Type should equal “WSS”).• The “Expected Far End Address” gives the WSS switch port connected to the SLA in the format TID-SH-SL-PORT. Note the value after the last hyphen.• Locate the WSS port identified above. This is the connection from the SLA to the WSS switch input. Clean the fiber associated with the output of that switch (for example, if port 11 was identified above, clean port 12 of the WSS).
9	Use optical terminators on unused input faceplate connectors of installed WSS w/OPM circuit packs. If dust caps are used instead of optical terminators on “Switch In” ports, PMs can be reported against the ports and the ports may appear in-service. If the alarm is against port 4 of FGA, check and clean the connection from the incoming line.
10	Restart the LIM, RLA 5x1 supporting the alarmed AMP facility. Refer to the “Restarting a circuit pack or shelf processor” procedure in Part 1 of this document.
11	Replace the LIM, RLA 5x1 supporting the alarmed AMP facility. Refer to the “Replacing the amplifier modules” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.
12	If the alarm does not clear, contact your next level of support or Ciena support group.

—end—

Procedure 5-217

Site Provisioning Required (DSM)

Alarm ID: 131

Probable cause

This alarm is raised against the DS1 service module (DSM) when the address is not defined. The site address defines a shelf-wide unique identifier for each DSM connected to a 6500 shelf. The address must be manually provisioned and until it is provisioned the DSM 84xDS1 termination module (TM) in the DSM remains out of service.

It is possible to edit the site address but you cannot delete it.

Taking the DSM 84xDS1 TM out of service (OOS-MA or OOS-AUMA) masks the alarm.

Impact

Critical, service-affecting (C, SA) alarm if the DSM is provisioned with cross connections

Minor, non-service-affecting (m, NSA) alarm if the DSM is provisioned and has no cross connections

Prerequisites

To perform this procedure, you must

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545
- use an account with at least a level 3 UPC

Step	Action
1	Edit the DSM site address. Refer to the “Defining or editing a site address for a DSM” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310. You can define the DSM site address only by editing the properties of the working DSM 84xDS1TM in slot 1.
2	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-218

Skew Out Of Range

Alarm ID: 1680, 1777, 2031

Probable cause

This alarm is raised when the skew between the two carriers exceeds the skew range and is detected.

For the ETTP (ETH100G) clients that use parallel optics, this alarm is raised when the Virtual Lane (VL) Skew exceeds the IEEE 802.3ba VL Skew range 180ns. This is only applicable when FEC is disabled.

Impact

Major, service-affecting (M, SA) alarm

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

Prerequisites

To perform this procedure, you must;

- observe all the safety requirements described in “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545
- 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)
- if required, obtain replacement patchcord fiber pairs for the Tx/Rx to Mux/Demux connection
- if required, obtain a replacement Flex2 WL3 OCLD, Flex3 WL3e OCLD or a Flex4 WL3e OCLD circuit pack
- use an account with at least a level 3 UPC

Step	Action
1	Ensure that both prime and member Flex2 WL3 OCLD, Flex3 WL3e OCLD or a Flex4 WL3e OCLD equipment are working properly with error-free signal.

- | | |
| --- | --- |
| 1 | Ensure that both prime and member Flex2 WL3 OCLD, Flex3 WL3e OCLD or a Flex4 WL3e OCLD equipment are working properly with error-free signal. |

Procedure 5-218 (continued)

Skew Out Of Range

Step	Action	
2	Ensure that the transmitter wavelength separation between the prime and member is 200 GHz or less. If it is not, re-provision the transmitter wavelengths and rework the wavelength plan to make them comply to this rule.	
3	If the original alarm has	Then
	cleared	the procedure is complete
	not cleared	go to step 4
4	Ensure that the difference in estimated fiber length for each WL3 OCLD is less than 300 meters. If it is not, ensure that the wavelengths take the same photonic path and have similar sized patchcords at each end.	
5	If the original alarm has	Then
	cleared	the procedure is complete
	not cleared	go to step 6
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	Ensure that the Tx/Rx to Mux/Demux fiber pairs on the two carriers are correctly connected with exactly equal length duplex LC to LC fibers at both sites. If they are not, replace them with exactly equal length duplex LC to LC fibers.	
8	If the original alarm has	Then
	cleared	the procedure is complete
	not cleared	go to step 9
9	Replace the prime circuit pack. Refer to the “Replacing an optical interface circuit pack” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545. If the original alarm has cleared then the procedure is complete, otherwise go to next step.	
10	Replace the member circuit pack.	
11	If the alarm does not clear, contact your next level of support or your Ciena support group.	

—end—

Procedure 5-219

SLDD Adjacency Loss

Alarm ID: 1981, 1982

Probable cause

This alarm applies to the 6500 shelves that have SLDD enabled and an SLDD circuit provisioned on the alarmed interface. The alarm is raised when no SLDD adjacency can be established on the alarmed interface.

This alarm will clear on its own if it was due to missing or mis-matched provisioning at the far end, and this is resolved at the far end.

Impact

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

Step	Action
1	Ensure that the SLDD circuit is provisioned at the far end of the Link.
2	If the alarm does not clear, verify that the SLDD Scope ID at the two ends of the Link match.
3	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-220

Slot Empty

Alarm ID: 379

Probable cause

This alarm is raised when an unprovisioned or out-of-service slot is empty.

ATTENTION

You must install filler cards in all slots that do not contain a circuit pack 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) alarm

Prerequisites

To perform this procedure, you must:

- observe all safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0
- obtain a filler card or a module to install in the empty slot

Step	Action
1	Identify the slot raising the alarm.
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	Insert a filler card or a circuit pack into the slot raising the alarm. Refer to the “Installing circuit packs in the 6500 shelf” procedure in <i>Installation - General Information</i> , 323-1851-201.0.
4	Place the out of service slot back to In Service.
5	If the alarm does not clear, contact your next level of support or your Ciena support group.

- | Step | Action |
|------|--|
| 1 | Identify the slot raising the alarm. |
| 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 | Insert a filler card or a circuit pack into the slot raising the alarm. Refer to the “Installing circuit packs in the 6500 shelf” procedure in <i>Installation - General Information</i> , 323-1851-201.0. |
| 4 | Place the out of service slot back to In Service. |
| 5 | If the alarm does not clear, contact your next level of support or your Ciena support group. |

—end—

Procedure 5-221

Slot Sequence Provisioning Incomplete

Alarm ID: 1832, 1833

Probable cause

This warning is raised when the Intersecting Status field for the Slot Sequence is “UNRESOLVED”.

This warning is a reminder to the user to complete the provision of its intersecting Slot Sequence.

When a Slot Sequence is provisioned, its Intersecting Status field can be set to one of the following:

- “NOT APPLICABLE”, if the Slot Sequence does not require intersecting Slot Sequence provisioning
- “UNRESOLVED”, if the Slot Sequence requires intersecting Slot Sequence provisioning
- “RESOLVED”, if its intersecting Slot Sequence is provisioned

The condition clears when the Intersecting Status field of the Slot Sequence is changed from “UNRESOLVED” to “RESOLVED” or “NOT APPLICABLE”.

Impact

Warning

Prerequisites

To perform this procedure, you require an account with at least a level 3 UPC.

Step	Action	
1	If you want to Provision the intersecting Slot Sequence to RESOLVED	Then go to step 2
	NOT APPLICABLE	step 3
2	Provision the intersecting Slot Sequence so the Intersecting Status field for Slot Sequence is changed to “RESOLVED”. Refer to the “Editing OTS slot sequences” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310. Go to step 4 .	
3	Ensure that the Drop and Add Sequence fields for Slot Sequence are cleared and the Intersecting Status field is changed to “NOT APPLICABLE”.	
4	If the condition does not clear, contact your next level of support or your Ciena support group.	

—end—

Procedure 5-222

SNC Datapath Fault

Alarm ID: 1759

Probable cause

This alarm is raised when the datapath is down for an SNC because the underlying DOC channel has not achieved the end-to-end In-service/Optimized 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 DOC 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.

The alarm is raised for a given SNC with properly provisioned photonic cross-connections, when receive fault is detected (for example, Loss of Frame or Loss of Clock) or when one or more underlying DOC domains in the SNC path has indicated that the channel is not optimized.

Impact

Major, service-affecting (M, SA) alarm

Prerequisites

To perform this procedure, you must use an account with at least a level 3 UPC.

Step	Action
1	Identify the SNC that is raising the alarm. Select Sub-Network Connection from Configuration menu.
2	From the SNC list, select the SNC that raised the alarm.
3	In the Details area, click on the End to End diagnosis button to view the faults that raised the alarm.
4	If the alarm is raised due to a channel not being added properly along the path in the DOC, identify the node and view the DOC related alarms. Clear these alarms before continuing this procedure.

5-504 Alarm clearing procedures—I to Z

Procedure 5-222 (continued)

SNC Datapath Fault

Step	Action
5	If the end to end diagnostic information indicates Rx Fault for the SNC on the transponder link, Loss of Signal, Loss of Frame, or Loss of Clock, then clear these alarms.
6	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-223

SNCG Not On Home Path

Alarm ID: 2042

Probable cause

This alarm is raised when an SNCG is placed In-Service 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).

After a restoration event, once the SNCG (when GROUPED=YES), transitions to IS state on a path that is not its home path, a minor “SNCG Not on Home Path” alarm will be raised.

This alarm is not enabled by default.

Impact

Warning

Prerequisites

To perform this procedure, you must use an account with at least a level 3 UPC.

Step	Action
1	Clear the network fault that triggered the mesh restoration.
2	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 as follows:
a.	In Site Manager, under the Configuration drop-down menu, select Sub-Network connections window and select the Group SNC tab.

5-506 Alarm clearing procedures—I to Z

Procedure 5-223 (continued)

SNCG Not On Home Path

Step	Action
	<p>b. Select the alarmed SNCG and click on the Revert button.</p>
3	<p>If the alarm does not clear, contact your next level of support or your Ciena support group.</p>



CAUTION

Risk of traffic loss

Reverting the SNCG will cause the channel to go down for several minutes.

—end—

Procedure 5-224 **SNCG Unavailable**

Alarm ID: 1979

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.

For Permanent SNCGs, the alarm will be raised when the PSNCG using a dynamic DTL or DTL List runs out of available paths or if its home path is unavailable.

Impact

Critical, service-affecting (C, SA) alarm

Prerequisites

To perform this procedure, you must use an account with at least a level 3 UPC.

Procedure 5-224 (continued)

SNCG Unavailable

Step	Action
5	From the Site Manager Sub-Network Connection option, select the SNCG tab. Select the alarmed SNCG and verify whether a current route is available (listed) in the Route Information sub-tab (in the Details area). To do this, click on the SNCG Routes button to open the SNCG Routes dialog box. If the Current Route tab lists a route, then there is an available current route.
6	If the current route is available Then go to step 7 not available Then go to step 8
7	View the provisioning SNC screen, choose the Member SNC tab and note the member SNCs. From the SNC list in the Service Provisioning tab, note the nodes (Remote Node column) and ports (Remote EP column) of the home route.
8	Verify if any equipment alarm exist. If there are, then, clear these alarms. Go to step 11 .
9	From the Route Information tab, click on the SNC Status Diagnostic button to open the SNC Status Diagnostics box.
10	If the event detail column currently indicates failures or errors, stop the procedure and contact your network administrator.
11	For the remote end point, select the Configuration drop down and select the Subnetwork Connections tab. View the Provisioning SNC screen and verify there is a valid route going to the destinations node.
12	If a route is available Then go to step 13 not available Then establish a route
13	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-225

SNC Not On Home Path

Alarm ID: 2041

Probable cause

This alarm is raised when a Sub-Network Connection (SNC) is off its home path.

This alarm is a secondary alarm raised to identify services impacted by a network fault event. The alarm is raised when SNCs recover from a fault by mesh restoring to a protection path and cleared when the SNC is either put administratively out of service, or the SNC reverts back to its home path.

This alarm is also raised if the SNC 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).

After a restoration event, once the SNC (when GROUPED=NO) transitions to IS state on a path that is not its home path, a minor “SNC Not on Home Path” alarm will be raised.

This alarm is not enabled by default.

Impact

Warning

Prerequisites

To perform this procedure, you must use an account with at least a level 3 UPC.

Step	Action
1	Clear the network fault that triggered the mesh restoration.
2	If the SNC is provisioned to automatically revert to the home path, the alarm will clear when the SNC reverts itself. Otherwise, verify that the SNC home path is available, and revert the SNC back on home path as follows:
a.	In Site Manager, under the Configuration drop-down menu, select Sub-Network connections window.

5-510 Alarm clearing procedures—I to Z

Procedure 5-225 (continued)

SNC Not On Home Path

Step	Action
3	Select the alarmed SNC and click on the Revert button.
4	If the alarm does not clear, contact your next level of support or your Ciena support group.



CAUTION

Risk of traffic loss

Reverting the SNC will cause the channel to go down for several minutes.

—end—

Procedure 5-226

SNC Reservation Unavailable

Alarm ID: 1947

Probable cause

This alarm is raised when there is a failure to successfully negotiate a mesh restoration route for a packet SNC provisioned with reservation.

The alarm is a warning that if the current path of a packet SNC provisioned with reservation fails, then traffic recovery will be “slow” (can take minutes) rather than “fast” (sub-second).

Impact

Warning

Step	Action
------	--------

- 1 No action is necessary. This alarm will clear once the packet SNC successfully negotiates mesh restoration route later in time.
- 2 If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-227

SNC Takeover Failed

Alarm ID: 1507

Probable cause

This alarm is raised when the Subnetwork Connection (SNC) has failed to take over all cross-connections from end to end.

This alarm is supported for Photonic L0 and SONET/SDH Control Plane and Photonic SNC takeover.

This alarm can also be raised for SNC takeover limiting conditions. When an explicitly routed call is configured for the purpose of path takeover, the path of the OSS service is validated. If the validation fails, the SNC is created, its status diagnostic indicates the reason of the failure and the takeover attempted SNC remains OSS owned.

Impact

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

Prerequisites

To perform this procedure, you must use an account with at least a level 3 UPC.

Step	Action	
1	From the Site Manager Sub-Network Connection application, select the SNC tab.	
2	From the Route Information sub-tab (in the Details area), click on the “SNC Status Diagnostics” button next to the SNC state field to open the SNC Status Diagnostics dialog box.	
3	If the alarm is raised for	Then go to
	SONET/SDH Control Plane	step 4
	Photonic Control Plane	step 13
4	From within the SNC status diagnostic window, check if the Event Detail column indicates the SNC is stuck in the Starting or Down state.	

Procedure 5-227 (continued)

SNC Takeover Failed

Step	Action
5	If the SNC is in the Starting or Down state, a home route will not be available. If the SNC is in Starting state, the potential causes of the failure are a problem with the state of the Absolute Route Diversity (ARD), Max. Admin Weight (MAW), wrong routing, the regen timeslot (If the regen connection is taken over), or SNC protection class UNPROTECTED_HIGH (PRTT) provisioning, which is indicated in the Event Detail column. Follow the Procedure 5-228, "SNC Unavailable" alarm clearing procedure to clear this alarm.
6	Log in to each node along the takeover path of the non-OSRP connections. Using the required Cross Connections application ("Connection ID" column) determine how many (if any) of these connections have had their connection identifier changed to an OSRP NCCI connection identifier. Note: Timeslots are only provisioned for SONET/SDH SNCs. NCCI applies to both SONET/SDH and OTN.
7	If the SNC is in the Creating state, and the Event Detail column indicates an XCON validation failure, determine at which node the XCON validation has failed.
8	Using the Routing Profiles application, retrieve the routes and verify if the timeslots are provisioned correctly. Compare the timeslots with each non-OSRP connection from step 6 .
9	If the timeslots do not match, delete the SNC and re-provision the routing list and route. Refer to the "Deleting a sub-network connection", "Adding a route", and "Adding a routing list" procedures in Configuration - Control Plane , 323-1851-330.
10	After the timeslots are corrected, re-add the takeover SNC, specifying the newly provisioned routing list.
11	If this is not a timeslot issue, determine if the failure is due to an ARD, MAW or PRTT provisioning problem. Place the SNC OOS and re-provision the SNC parameters. Re-attempt the takeover by placing the SNC back to an IS state.
12	If the failure is seen during the connect phase, delete the SNC, delete any leftover non-OSRP connections on the takeover path (if any), and then create a non-takeover SNC on the same path. Refer to the "Deleting a sub-network connection" and "Adding a sub-network connection" procedures in Configuration - Control Plane , 323-1851-330 or Part 1 of Configuration - Bandwidth and Data Services , 323-1851-320.
13	Check the Event Detail column for indication of the problem that caused the SNC takeover to fail for the L0 Control Plane.
14	If the connection taken over is 1WAY or does not match the route specified in the Routing List, re-provision the connection to correct the problem.

Procedure 5-227 (continued)

SNC Takeover Failed

Step	Action
15	If the problem is fixed, the SNC will be taken over (there are automatic retries) and the alarm clears.
16	If the alarm did not clear, Place the SNC OOS, delete the SNC and create a new SNC with the parameters that may have been wrong on the first try. Refer to the “Deleting a sub-network connection” and “Adding a sub-network connection” procedures in <i>Configuration - Control Plane</i> , 323-1851-330 or Part 1 of <i>Configuration - Bandwidth and Data Services</i> , 323-1851-320.
17	If you are unable to fix the problem or if the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-228 SNC Unavailable

Alarm ID: 1423

Probable cause

This alarm is raised when the terminating Subnetwork Connection (SNC) or Permanent Sub-Network Connection (P-SNC) is in the creating or starting state. It is typically caused by a destination unreachable condition caused by insufficient bandwidth, lack of matching service classes, or lack of physical facility to the destination port.

This alarm clears when any of the following occur:

- The path defect on the OSRP line that created this condition is absent for 10 seconds.
 - The SNC is deleted.
 - The SNC Administrative State is set to Locked.

Note: For the OTN Control Plane, the SNC Name can be optionally included in all SNC related alarms. By default, SNC alarms do not include the SNC Name. Enabling of SNC Name in SNC alarms can be provisioned on a system level using the “Alarm Info” parameter. Refer to the “Editing the nodal system parameters” procedure in *Administration and Security*, 323-1851-301.

Impact

Critical, service-affecting (C, SA) alarm

Prerequisites

To perform this procedure, you must use an account with at least a level 3 UPC.

Step	Action
1	Identify the node raising the alarm and note any additional information. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document.
2	If the SNC raising the alarm is recently added, delete and re-create the SNC. Refer to the “Deleting a sub-network connection” and “Adding a sub-network connection” procedures in <i>Configuration - Control Plane</i> , 323-1851-330.
3	If the original alarm has Then
cleared	the procedure is complete
not cleared	go to step 4

Procedure 5-228 (continued)

SNC Unavailable

Step	Action
4	Verify if any equipment alarms are raised against circuit packs carrying the SNC. If there are, then clear these alarms before continuing this procedure.
5	From the Site Manager Sub-Network Connection application, select the SNC tab. Verify whether a current route is available in the Route Information sub-tab (in the Details area). To do this, click on the Routes button to open the SNC Routes dialog box. If the Current Route tab lists a route, then there is an available current route.
6	If the current route is Then go to
	available step 7
	not available step 9
7	View the provisioning SNC screen. From the SNC list, note the nodes (Remote Node column) and ports (Remote EP column) of the home route.
8	Verify if any equipment alarm exist. If there are, then, clear these alarms. Go to step 11 .
9	From the Route Information tab, click on the (...) button next to the SNC state field to open the SNC Status Diagnostics dialog box.
10	If the event detail column currently indicates failures or errors, stop the procedure and contact your network administrator.
11	Click Provisioning and select the SNC tab for each node. View the Provisioning SNC screen and verify there is a valid route (sufficient bandwidth that match the service class constraint) going to the destinations node.
12	If a route is Then
	available go to step 13
	not available establish a route
13	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-229

Software Auto-Upgrade in Progress

Alarm ID: 439

Probable cause

This alarm is raised if a newly inserted circuit pack is being auto-upgraded/downgraded to the active software release of the network element.

This alarm can also be raised when a shelf processor is replaced and the inserted SP is running a different software release than the active release on the network element.

For 40G OTN XCIF circuit packs, this alarm can be raised when the profile of the circuit pack is changed after a database restoration.

This alarm is also raised when the user cancels the upgrade operation.

Impact

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

Step	Action
------	--------

- 1 Wait for the auto-upgrade/downgrade of the circuit pack to complete.
The auto-upgrade/downgrade of the circuit pack can take up to five minutes.
For 40G OTN XCIF circuit packs, the circuit pack will go through a cold restart. It can take up to 20 minutes for the alarm to clear.
- 2 If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-230

Software Configuration Unknown

Alarm ID: 138

Probable cause

This alarm is raised when the SP software fails to install the software control information.

Impact

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

Step	Action
1	If a Software Mismatch and an Incomplete Software Lineup alarm are also both active Then perform the alarm clearing procedure for the “Incomplete Software Lineup” on page 5-22. If the Software Configuration Unknown alarm does not clear, go to step 2 .
	a Software Mismatch and an Incomplete Software Lineup alarm are not both active go to step 2
2	Contact your next level of support or your Ciena support group.

—end—

Procedure 5-231

Software Delivery Incomplete

Alarm ID: 453

Probable cause

This alarm is raised when a transfer of a new software release to the SP has failed.

Impact

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

Prerequisites

To perform this procedure, you must

- be able to connect to the SP
- use an account with at least a level 3 UPC

Step	Action
1	Click Cancel in the Release Management application. Refer to the “Upgrading a software load” procedure in <i>Administration and Security</i> , 323-1851-301. Canceling stops the action and cleans up any files left in invalid states.
2	This alarm can also clear if you try to deliver the software release again. Try to establish and resolve the cause of the failure then retry the delivery. Refer to the “Transferring a software load to a network element” procedure in <i>Administration and Security</i> , 323-1851-301. The alarm clears if the software release delivery is successful.
3	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-232

Software Delivery in Progress

Alarm ID: 454

Probable cause

This alarm is raised if a new release is being transferred to the SP.

Impact

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

Prerequisites

To perform this procedure, you require an account with at least a level 3 UPC.

Step	Action
1	<p>Wait for the transfer of the software release to the SP to complete. Refer to the “Transferring a software load to a network element” procedure in <i>Administration and Security</i>, 323-1851-301.</p> <p>The transfer of the software release to the SP can take up to an hour. Refer to the <i>Software Upgrade Procedures</i> for information on the length of upgrades. For a list of procedures, refer to the “Software Upgrade Procedures” section in <i>Planning - Ordering Information</i>, 323-1851-151.</p>
2	<p>If you want to abort the transfer, click Cancel in the Release Management application.</p> <p>Canceling stops the action and cleans up any files left in invalid states.</p>
3	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-233

Software Mismatch

Alarm ID: 75

Probable cause

This alarm is raised if a SP is inserted in the shelf and the SP is running a different software release than the active release on the network element.

Impact

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

Step	Action
1	Check the current release running on the network element. Refer to the “Checking the current software release” procedure in <i>Commissioning and Testing</i> , 323-1851-221.
2	If the SP is running a release that is lower than that of the shelf, the NE will have minimal functionality and display a shelf number of 0. A “Transport Data Recovery” alarm may also be present.
3	Perform an upgrade on the network element. For the upgrade “to release”, use the current release running on the network element. Refer to the <i>Software Upgrade Procedures</i> for this release listed in the “Software Upgrade Procedures” section in <i>Planning - Ordering Information</i> , 323-1851-151.
4	Ensure that the system is restored to its original state by retrieving all conditions and alarms. Clear all alarms using the appropriate alarm clearing procedure.
5	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-234

Software Subsystem Failed

Alarm ID: 1424

Probable cause

This alarm is raised when a circuit pack has a software failure that cannot be recovered on its own or when a circuit pack (except the eMOTR circuit pack) fails to boot up after few attempts.

This alarm can be raised on an eMOTR circuit pack with a Packet Configuration Integrity Fail condition when upgraded from Release 10.2x to Release 11.1 in a standalone or mate configurations. A warm restart will clear the alarm for all cases except when the failure is because of the SDK PRAM being out of sync. See the “Packet Configuration Integrity Fail” alarm procedure.

Impact

Critical, service-affecting (C, SA) alarm

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

Prerequisites

To perform this procedure, you require an account with at least a level 3 UPC.

Step	Action
1	If the alarm is raised against a WSS w/OPM (NTK553KA/HA/JB/LA/FC) or CCMD8x16 circuit pack, perform the DGN-EQPT command against the circuit pack raising the alarm. Refer to the DGN-EQPT command description in <i>TL-1 Description</i> , 323-1851-190.
2	If the alarm does not clear, perform a warm restart on the circuit pack that is raising the alarm. Refer to the “Restarting a circuit pack or shelf processor” procedure in Part 1 of this document.
3	CAUTION Risk of traffic loss  A cold restart on an unprotected circuit pack causes a traffic loss. A cold restart on an active protected circuit pack causes a protection switch that impacts traffic.

- 1 If the alarm is raised against a WSS w/OPM (NTK553KA/HA/JB/LA/FC) or CCMD8x16 circuit pack, perform the DGN-EQPT command against the circuit pack raising the alarm. Refer to the DGN-EQPT command description in *TL-1 Description*, 323-1851-190.
- 2 If the alarm does not clear, perform a warm restart on the circuit pack that is raising the alarm. Refer to the “Restarting a circuit pack or shelf processor” procedure in Part 1 of this document.

CAUTION

Risk of traffic loss

A cold restart on an unprotected circuit pack causes a traffic loss. A cold restart on an active protected circuit pack causes a protection switch that impacts traffic.

If the alarm does not clear, perform a cold restart on the alarmed circuit pack. Refer to the “Restarting a circuit pack or shelf processor” procedure in Part 1 of this document.

Procedure 5-234 (continued)
Software Subsystem Failed

Step	Action
4	If the alarm does not clear, reseat the circuit pack. Refer to the “Reseating a circuit pack” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.
5	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-235 **Software Subsystem Restart**

Alarm ID: 1627

Probable cause

This alarm is raised when a circuit pack has a software failure which cannot be recovered on its own.

Impact

Critical, service-affecting (C,SA) alarm

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

Prerequisites

To perform this procedure, you require an account with at least a level 3 UPC.

Step	Action		
1	Perform a warm restart on the interface circuit pack that is raising the alarm. Refer to the “Restarting a circuit pack or shelf processor” procedure in Part 1 of this document. Go to step 2 .		
2	If the original alarm has cleared not cleared	Then	the procedure is complete go to step 3
3	<p>CAUTION</p> <p>Risk of traffic loss</p> <p data-bbox="711 1214 1317 1288">Reseating an unprotected circuit pack causes a traffic loss. Reseating an active protected circuit pack causes a protection switch that impacts traffic.</p>		
4	Reseat the circuit pack. Refer to the “Reseating a circuit pack” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545. If the alarm does not clear, contact your next level of support or your Ciena support group.		

—end—

Procedure 5-236

Software Upgrade Failed

Alarm ID: 71

Probable cause

This alarm is raised when a failure occurs during a manual or automatic upgrade of circuit packs.

The alarm can also be raised when there is an unsaved SAOS-based CLI configuration.

Impact

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

Step	Action
------	--------

- 1 If the alarm is raised due to an unsaved SAOS-based CLI configuration, save the SAOS-based CLI configurations on the primary PKT/OTN cross-connect circuit packs and then re-issue the upgrade operation.
- 2 Contact your next level of support or your Ciena support group.

—end—

Procedure 5-237

Software Upgrade in Progress

Alarm ID: 74

Probable cause

This alarm is raised while a system upgrade is in progress after the initialization of the software upgrade. The alarm clears after the upgrade is complete.

This alarm is for information only. Do not perform any actions other than the upgrade activity while it is active. The alarm clears after the upgrade is complete.

Impact

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

Step	Action
------	--------

- 1 If the alarm does not clear after the upgrade is complete, contact your next level of support or your Ciena support group.

—end—

Procedure 5-238

Span protection Switch Complete

Alarm ID: 1229, 1230

Probable cause

This alarm is raised when a 2-Fiber LSR/MS-SPRing or 4-Fiber BLSR/MS-SPRing/HERS protection group switches activity on the span from working channel to protection channel due to either an automatic or user switch request. The standing condition is maintained until reversion to the working channel.

Impact

Warning

Step	Action
	<p>Note: No action is required if you are performing a test or maintenance operation. This alarm is a reminder not to leave a potentially service-affecting condition on the system.</p> <ol style="list-style-type: none"> 1 Check the traffic protection status. Refer to the “Retrieving Protection Status details” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i>, 323-1851-310. 2 If automatic protection switching has occurred, check for signal failure or degraded signal alarms related to this facility (including but not limited to Signal Fail or Signal Degrade). Clear these alarms by following the appropriate trouble clearing procedure. 3 Determine if any user request resulted in a dropped protection switch. Check for protection switching alarms. 4 If the alarm remains active, ensure that no other alarm is active, then contact your next level of support or Ciena support group. <p style="text-align: center;">—end—</p>

- 1 Check the traffic protection status. Refer to the “Retrieving Protection Status details” procedure in Part 2 of *Configuration - Provisioning and Operating*, 323-1851-310.
- 2 If automatic protection switching has occurred, check for signal failure or degraded signal alarms related to this facility (including but not limited to Signal Fail or Signal Degrade). Clear these alarms by following the appropriate trouble clearing procedure.
- 3 Determine if any user request resulted in a dropped protection switch. Check for protection switching alarms.
- 4 If the alarm remains active, ensure that no other alarm is active, then contact your next level of support or Ciena support group.

—end—

Procedure 5-239 **Span protection Switch Fail**

Alarm ID: 1231, 1232

Probable cause

This alarm is raised when the system attempts to span switch traffic from the working to the protection channels in a 4-Fiber BLSR/MS-SPRing/HERS configuration and fails. This alarm is raised when one of the following conditions occurs on either the local or remote network element:

- a faulty circuit pack
 - a degraded signal
 - a higher priority switch status exists
 - an incorrect BLSR/MS-SPRing/HERS provisioning

Impact

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

Prerequisites

To perform this procedure, you require an account with at least a level 3 UPC.

—end—

Procedure 5-240

Span Protection Exerciser Fail

Alarm ID: 1235, 1236

Probable cause

This alarm is raised when the span protection exerciser has failed to complete the exercise routine on the selected facilities.

This alarm is caused by one of the following conditions:

- a faulty circuit pack
- an exerciser is running somewhere else in the 2-Fiber BLSR/MS-SPRing or 4-Fiber BLSR/MS-SPRing/HERS
- crossed fibers
- an incorrect node on an adjacent node
- LOW-S applied at the adjacent end of the span where the exerciser is run on the ring

Impact

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

Prerequisites

To perform this procedure, you require an account with at least a level 3 UPC.

Step	Action
1	Ensure that there is no active protection switch on the 2-Fiber BLSR/MS-SPRing or 4-Fiber BLSR/MS-SPRing/HERS. Refer to the “Retrieving protection status details” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
2	If protection switches are
	idle
	not idle
	Then go to
	step 3
	step 8
3	Verify if any exerciser is scheduled to run on another network element in the 2-Fiber BLSR/MS-SPRing or 4-Fiber BLSR/MS-SPRing/HERS at approximately the same time. Refer to the “Retrieving the exerciser schedule” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
4	If the exerciser is running on another network element in the 2-Fiber BLSR/MS-SPRing or 4-Fiber BLSR/MS-SPRing/HERS, inhibit the exerciser. Refer to the “Running/Inhibiting the exerciser” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.

Procedure 5-240 (continued)
Span Protection Exerciser Fail

Step	Action
5	If the “Protection Invalid K-bytes” or “Protection Default K-bytes” alarms are active, follow the alarm clearing procedure to clear the alarms.
6	Initiate the exerciser on the selected equipment. Refer to the “Running/Inhibiting the exerciser” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
7	If the alarm does not clear, contact your next level of support or Ciena support group. The procedure is complete.
8	Clear any of the following alarms if active: <ul style="list-style-type: none">• OC/STM, STS/HO VC facility<ul style="list-style-type: none">— AIS (OC/STM)— Loss of Frame (OC/STM)— Loss Of Signal (OC/STM)— Signal Fail (OC/STM)— Trace Identifier Mismatch (STS/HO VC)— Manual Ring Switch Active— Manual Span Switch Active— Forced Ring Switch Active— Forced Span Switch Active— Lockout Working Ring Active— Lockout Working Span Active— Lockout Protection Span Active
9	Release all user-initiated protection switches. Refer to the “Releasing a protection switch” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
10	If the wait-to-restore is active, a Wait-to-Restore event active is raised against the 2-Fiber BLSR/MS-SPRing or 4-Fiber BLSR/MS-SPRing/HERS configuration. Wait for the event to clear.
11	Initiate the exerciser on the selected equipment. Refer to the “Running/Inhibiting the exerciser” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
12	If the alarm does not clear, repeat step 3 through step 7 .

—end—

Procedure 5-241

Switch Shelf ID Mismatch Detected

Alarm ID: 269

Probable cause

This alarm is raised following a shelf processor replacement when it is not clear whether the transport cards or shelf processor have shelf mastership. This mastership indicates whether the shelf processor should retrieve the shelf provisioning data from the transport cards or deliver the provisioning data to the transport cards.

ATTENTION

Do not reseat or replace circuit packs while this alarm is active.

Impact

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

Step	Action
1	Contact your next level of support or your Ciena support group. —end—

- 1 Contact your next level of support or your Ciena support group.

—end—

Procedure 5-242

Synchronization Protection alarms

Use this procedure to clear alarms associated with synchronization protection.

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.

Timing Distribution Forced Switch - n Ref

Alarm ID: (389, 390, 391, 392)

Probable cause

This alarm is raised when a user issues a forced switch request on the **n-th** (where n can be 1, 2, 3, or 4) timing reference member of the timing distribution hierarchy.

Impact

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

Timing Distribution Manual Switch - n Ref

Alarm ID: (2005, 2006, 2007, 2008)

Probable cause

This alarm is raised when a user issues a forced switch request on the **n-th** (where n can be 1, 2, 3, or 4) timing reference member of the timing distribution hierarchy.

Impact

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

Timing Distribution Lockout - n Ref

Alarm ID: (393, 394, 395, 396)

Probable cause

This alarm is raised when a user issues a lockout switch request on the **n-th** (where n can be 1, 2, 3, or 4) timing reference member of the timing distribution hierarchy.

Impact

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

Procedure 5-242 (continued)
Synchronization Protection alarms

Timing Generation Forced Switch - n Ref

Alarm ID: (413, 414, 415, 416)

Probable cause

This alarm is raised when a user issues a forced switch request on the **n-th** (where n can be 1, 2, 3, or 4) timing reference member of the timing generation hierarchy.

Impact

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

Timing Generation Lockout - n Ref

Alarm ID: (417, 418, 419, 420)

Probable cause

This alarm is raised when a user issues a lockout switch request on the **n-th** (where n can be 1, 2, 3, or 4) timing reference member of the timing generation hierarchy.

Impact

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

Timing Generation Manual Switch - n Ref

Alarm ID: (2001, 2002, 2003, 2004)

Probable cause

This alarm is raised when a user issues a forced switch request on the **n-th** (where n can be 1, 2, 3, or 4) timing reference member of the timing distribution hierarchy.

Impact

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

Prerequisites

To perform this procedure, you require an account with at least a level 2 UPC.

Step	Action
1	No action is required if a user is performing a test or maintenance operation. If testing/maintenance is complete, release the indicated switch request. Refer to the “Releasing a protection switch” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
2	If the alarm does not clear, is unexpected, contact your next level of support or your Ciena support group.

—end—

Procedure 5-243

TACACS Server 1/2 Unavailable

Alarm ID: 2043, 2044

Probable cause

Use this procedure to clear the following alarms:

- TACACS server 1 unavailable
- TACACS server 2 unavailable

The “TACACS server 1 unavailable” alarm is raised when all requests to the server 1 times out and a server 2 is provisioned.

The “TACACS server 2 unavailable” alarm is raised when all requests to the server 2 times out and a server 1 is provisioned.

If only the Server 1 is provisioned (no server 2 provisioned) and all requests time out, the “All Provisioned TACACS Servers Unavailable” alarm is raised. Refer to the “All Provisioned TACACS Servers Unavailable” alarm clearing procedure in Part 1 of this document).

Impact

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

Prerequisites

To perform this procedure, you must use an account with at least a level 4 UPC.

Step	Action
1	The alarm clears when connectivity is re-established between the shelf and the TACACS server.
2	If the alarm does not clear, perform one of the following: <ul style="list-style-type: none">• clear the security alarms. Refer to “Clearing security alarms” procedure in part 1 of this document• provision a new IP address or Port for server 1 or server 2. Refer to the “Provisioning the TACACS+ server” procedure in <i>Administration and Security</i>, 323-1851-301• disable server 1 or server 2• disable TACACS Refer to <i>Administration and Security</i>, 323-1851-301
3	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-244 Tamper Detected

Alarm ID: 1819

Probable cause

This alarm is raised when tamper condition is detected on the 4x10G OTR w/ Encryption circuit pack.

For the NTK530QE circuit pack, the FIPS security boundary is protected by a hard aluminum enclosure with anti-intrusion circuitry. Upon removal of the enclosure cover, this alarm is raised.

Impact

Critical, service-affecting (C, SA) alarm

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

Prerequisites

To perform this procedure, you must

- use an account with at least a level 2 UPC
- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545
- have an antistatic wrist strap to dissipate electrostatic charges

Tamper Detected

Step	Action
<p>Note: For security reasons, once a circuit pack has been tampered with, the encryption/decryption block is permanently disabled. Traffic will be down.</p>	
1	<p>CAUTION</p> <p>Risk of traffic loss</p> <p>The 4x10G OTR (NTK530QE variant) circuit pack requires a valid Time of Day (TOD) in order to perform the certificate validation before bringing up traffic. The TOD information is received from the SP on every circuit pack restart.</p> <p>If the 4x10G OTR (NTK530QE variant) circuit pack is reseated while an SP is not present, traffic does not recover automatically on this circuit pack until the SP is available to provide the system TOD. Ensure the SP is installed in the chassis before you reseat the 4x10G OTR circuit pack.</p>
<p>Replace the circuit pack. Refer to the replacement procedures in <i>Fault Management - Module Replacement</i>, 323-1851-545.</p>	
<p>Note: Certificates must be re-enrolled on the new circuit pack using MyCryptoTool. Refer to the “Performing Data Encryption Certificate Enrollment” procedure in <i>Encryption and FIPS Security Policy Overview and Procedures</i>, 323-1851-340.</p>	
2	<p>If the alarm does not clear, contact your next level of support or your Ciena support group.</p>

—end—

Procedure 5-245

Target Unachievable

Alarm ID: 1514, 1717

Probable cause

This alarm is raised when the provisioned power value for one or more lasers on the Idler facility of Submarine Line Idler 10 Channel (SLIC10 or SLIC10 Flex C-Band) circuit pack is out of range.

For the SRA circuit pack, this alarm is raised when the measured gain is not within 3 dB of the target gain.

Impact

Minor, non-service-affecting (m, NSA) alarm
Major, service-affecting (M, SA) alarm

Prerequisites

To perform this procedure, you require an account with at least a level 3 UPC.

Step	Action	
1	If the alarm is raised against the	Then go to
	SLIC10 or SLIC10 Flex C-Band circuit pack	step 2
	SRA circuit pack	go to step 6
2	Verify the provisioned power value of the first laser on the Idler facility (TARGPOWER1/MINPOWER1/MAXPOWER1).	
3	Verify that target power1 is within the range of the minimum power1 and maximum power1. If it is out of range, change the value of target power1 such that it falls in the range. Refer to the “Provisioning photonic parameters” procedure in the <i>Photonic Equipment</i> , 323-1851-102.6.	
4	Repeat step 2 and step 3 for the Idler’s second laser (represented by TARGPOWER2/MINPOWER2/MAXPOWER2). Go to step 11 .	

Procedure 5-245 (continued)

Target Unachievable

Step	Action	
5	If the alarm is raised	Then
	at the first channel turn-up on dark fiber and for spans less than 35 dB on the RAMAN facility	go to step 6
	at the first channel turn-up on dark fiber and for spans greater than 35 dB on the RAMAN facility	repeat step 6 and step 7 , then go to step 9
	otherwise	contact your next level of support or your Ciena support group
6	Verify the fibers of the alarmed facility to ensure they are clean and there are no pinched fibers.	
	Note: When fibers are connected and disconnected, the OTDR traces are triggered automatically. Wait until traces are completed before reconnecting or disconnecting the fiber.	
7	Verify that the correct fiber type was provisioned at the far-end line adjacency. If the far-end fiber is different from the last 20 kms of fiber connected to the SRA Line A In port, provision the TELEMETRY facility fiber type. Refer to the “Provisioning photonic parameters” procedure in <i>Commissioning and Testing</i> , 323-1851-221.	
8	If the alarm is	Then
	cleared	this procedure is complete.
	otherwise	go to step 11
9	If the alarm is raised because the recommended gain is lower than the calculated gain, reduce the total target power on the RAMAN facility. Refer to the “Editing facility parameters” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.	
10	If the RAMAN target power is set to the maximum and the calculated gain is lower than the recommended gain, then the fiber may be impaired. Set the RAMAN mode to MAXGAIN using TL1 commands.	
	Note: This mode can only be applied if the span loss is more than 25 dB. Otherwise contact your next level of support or your Ciena support group.	
11	If the alarm does not clear, contact your next level of support or your Ciena support group.	

—end—

Procedure 5-246

TCM Loss of Tandem Connection

Alarm ID: 1505, 1506, 1612

Probable cause

This alarm is raised when there is a Loss of Tandem Connection (LTC) due to provisioning the TCM facility at one end only.

Impact

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

Prerequisites

To perform this procedure, you require an account with at least a level 3 UPC.

Step	Action
1	Verify at which end the TCM facility is not provisioned. Refer to the “Retrieving equipment and facility details” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
2	Provision the TCM facility on the end that is not provisioned. Refer to the facility provisioning procedures in <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
3	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-247

Telemetry Loss of Signal

Alarm ID: 1715

Probable cause

This alarm is raised when the SRA RAMAN amplifier cannot receive the telemetry gain signal from upstream.

This alarm can also be raised when the upstream network element is running an OTDR trace.

Impact

Major, service-affecting (M, SA) alarm

Prerequisites

To perform this procedure, you must have:

- replacement fibers
- a fiber cleaning kit

Step	Action
1	If the upstream network element is running an OTDR trace and the OTDR Trace In Progress alarm is active, wait until the OTDR trace is complete. The alarm will clear when the OTDR trace is complete.
2	If there is no OTDR trace in progress, verify that there is no “Circuit Pack Fail” alarm on the upstream SRA circuit pack and the facility is in-service.
3	Verify if there are any other alarms related to the link (for example, Shutoff Threshold Crossed, Loss of Signal, and OSC Loss of Signal) and clear the alarms.
4	If the alarm is not cleared, ensure that the far-end telemetry facility is in-service.
5	If the alarm is not cleared, verify the fiber connection for the interface circuit pack that connects to the alarmed shelf.
6	Use a fiber cleaning kit to clean all the connectors then reconnect the output fibers and connectors at the amplifier. Refer to the “Cleaning Connectors” chapter in <i>Installation - General Information</i> , 323-1851-201.0.
7	If the alarm does not clear, replace the fiber.
8	If the alarm does not clear, provision the circuit pack manually, run another OTDR trace, or use a different maximum trace time (the maximum provisionable value is 120 seconds).

Procedure 5-247 (continued)

Telemetry Loss of Signal

Step	Action
9	If the alarm does not clear, replace the SRA amplifier.
10	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-248

Test Access in Progress alarms

Use this procedure to clear the following alarms:

- Test Access in Progress - Monitor E
- Test Access in Progress - Monitor F
- Test Access in Progress - Monitor EF
- Test Access in Progress - Split A
- Test Access in Progress - Split B
- Test Access in Progress - Split E
- Test Access in Progress - Split F
- Test Access in Progress - Split EF

For L2 MOTR circuit pack ETH facilities, the following alarms are raised:

- Test Access in Progress - Monitor E
- Test Access in Progress - Monitor F
- Test Access in Progress - Monitor EF

Alarm IDs: 742 - 781, 1755, 1756, 1757

Probable cause

This alarm is raised when a Test Access Session is provisioned from an existing cross-connect to Test Access Port. The alarm is raised against the cross-connect under the test.

The alarm is raised against the endpoints of a connection which has a Test Access connection provisioned against it.

When a facility is provisioned as a test access port, the Loss Of Signal LED will lit if a signal is not present on this facility.

For L2 MOTR circuit pack ETH facilities, the alarm is raised when a L2 port mirroring session is created to mirror traffic from an Ethernet facility (monitored) to another Ethernet facility (test access facility). The alarm is raised against the monitored facility.

For L2 MOTR circuit pack ETH facilities, the Test Access facility will be in a TS secondary state. When an ETH facility is provisioned as a test access port, the Loss of Signal LED will be lit if no signal is present on this facility.

Procedure 5-248 (continued)

Test Access in Progress alarms**Impact**

Warning

Prerequisites

To perform this procedure, you require an account with at least a level 3 UPC.

Step	Action	
1	If the alarm is raised during facility testing, no action is required. The alarm will clear once the testing is complete and the test access session is removed.	
2	If the alarm is unexpected, identify the circuit pack raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document.	
3	If the alarm is raised against a L2 MOTR circuit pack ETH facility otherwise	Then go to step 4 step 5
4	Remove the port mirroring session from this ETH facility. Refer to the “Releasing selected test access session(s) manually” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310. Go to step 6 .	
5	Remove the test access session from the test access port. Refer to the “Releasing selected test access session(s) manually” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.	
6	If the alarm does not clear, contact your next level of support or your Ciena support group.	

—end—

Procedure 5-249 **Threshold AIS ESO-A/ESO-B**

Alarm IDs: 265, 266

Probable cause

This alarm is raised when AIS is inserted in an ESO signal or the 2 MHz ESO signal is squelched because the signal quality of the active ESO reference (determined by the SSM) is at or below (SONET mode) or below (SDH or SDH-J mode) the provisioned threshold AIS level. The alarm can be raised against the ESO A and ESO B signals.

Impact

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

Prerequisites

To perform this procedure, you require an account with at least a level 3 UPC.

Step	Action
Provisioned threshold AIS value	
1	Retrieve and record the provisioned threshold AIS value for the timing distribution reference (ESO A or ESO B). Refer to the “Retrieving synchronization data for a network element” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
2	If the provisioned threshold AIS value is
	incorrect
	Then go to step 3
	correct
	Then go to step 5
3	If required, modify the provisioned threshold AIS value. Refer to the “Provisioning ESO parameters” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
4	If the original alarm has
	cleared
	Then the procedure is complete
	not cleared
	Then go to step 5

Checking the provisioned incoming quality level override (if applicable)

- 5** Check if there is a provisioned incoming quality level override for the active timing distribution reference. Refer to the “Retrieving synchronization data for a network element” procedure in Part 2 of *Configuration - Provisioning and Operating*, 323-1851-310.

**Procedure 5-249 (continued)
Threshold AIS ESO-A/ESO-B**

Step	Action	
6	If the incoming quality level override for the active timing distribution reference is	Then
	not provisioned	go to step 9
	incorrectly provisioned	go to step 7
	correctly provisioned and is supposed to be at or below (SONET mode) or below (SDH or SDH-J mode) the threshold AIS value you recorded in step 1	go to step 8
	correctly provisioned and is supposed to be above (SONET mode) or at or above (SDH or SDH-J mode) the threshold AIS value you recorded in step 1	contact your next level of support or your Ciena support group. The procedure is complete.
7	Provision the correct incoming quality level override. Refer to the “Setting the synchronization status message override quality level” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.	
	Go to step 9 .	
8	The quality of this timing reference signal is too low to be used as an ESO reference. Select a different ESO reference. Refer to the “Provisioning ESO references” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.	
	The procedure is complete.	

Checking the actual quality level

- 9** On the network element that raised the alarm, verify the actual quality for the active timing distribution reference. Refer to the “Retrieving synchronization data for a network element” procedure in Part 2 of *Configuration - Provisioning and Operating*, 323-1851-310.

10 If the actual quality is **Then go to**

equal or below (SONET mode) or below (SDH or SDH-J mode) the provisioned threshold AIS value	go to step 11
equal (SONET mode) or equal or above (SDH or SDH-J mode) the provisioned threshold AIS value	contact your next level of support or your Ciena support group. The procedure is complete.

Procedure 5-249 (continued)
Threshold AIS ESO-A/ESO-B

Step	Action	
Source of the active timing distribution at other network elements in the network		
11	Working from the network element that raised the alarm, follow step 12 to step 17 for each network element to find the source of the problem.	
12	Verify the source of the active timing distribution reference (the alarm is raised on network element D in the example Figure 5-4 on page 5-548).	
13	Clear any synchronization alarms.	
14	If the original alarm has	Then
	cleared	the procedure is complete
	not cleared	go to step 15
15	Check if there is a provisioned outgoing quality level override at the source of the active timing distribution reference for the original network element. Refer to the synchronization procedures in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.	
16	If the outgoing quality level override is	Then
	not provisioned	go to step 20
	incorrectly provisioned	go to step 17
	correctly provisioned and is supposed to be at or below (SONET mode) or below (SDH or SDH-J mode) the threshold AIS value you recorded in step 1	go to step 18
	correctly provisioned and is supposed to be above (SONET mode) or at or above (SDH or SDH-J mode) the threshold AIS value you recorded in step 1	contact your next level of support or your Ciena support group. The procedure is complete.
17	Provision the correct outgoing quality level override. Refer to the “Setting the synchronization status message override quality level” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.	
	Go to step 19 .	

Selecting a different timing reference

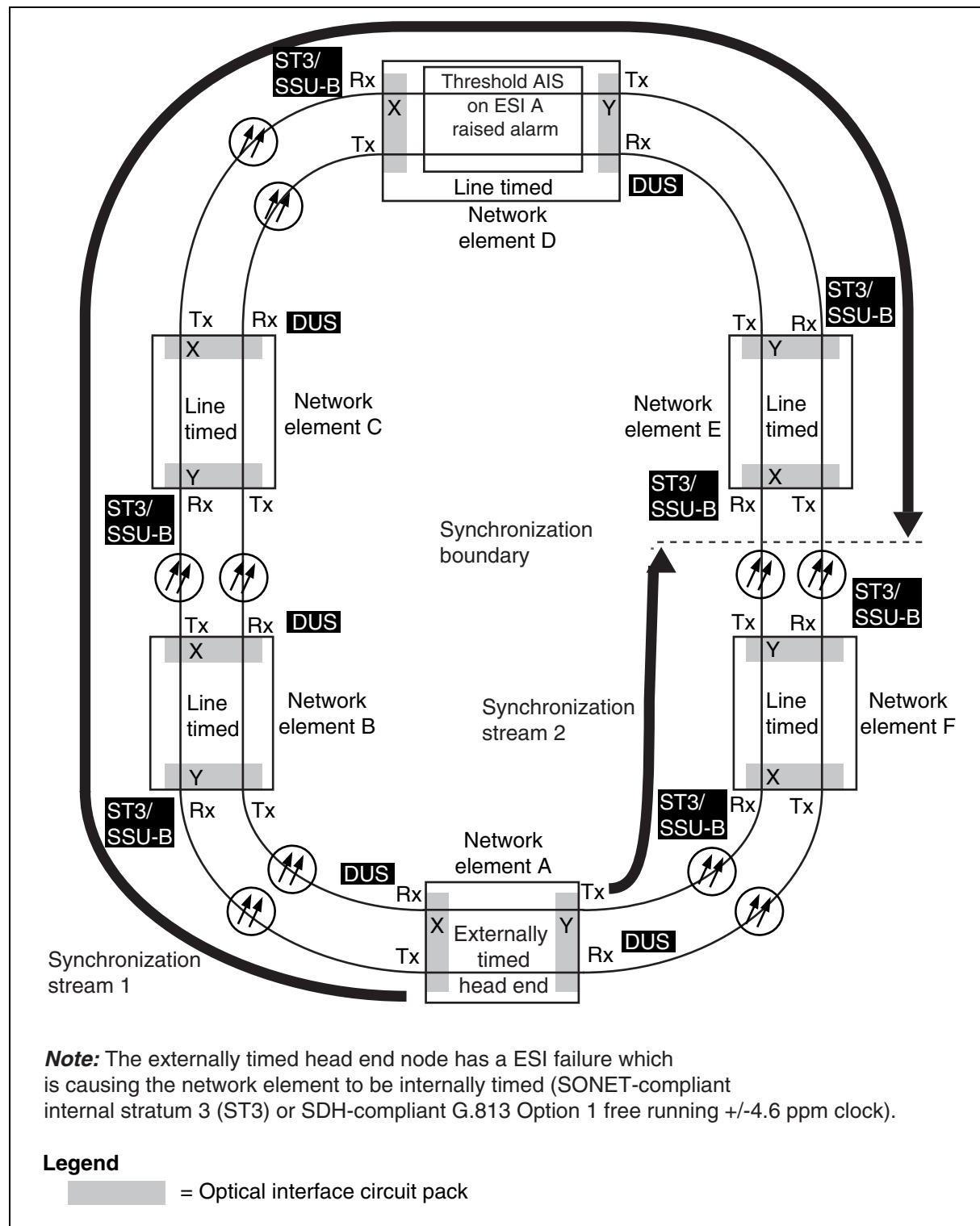
- 18** The quality of this timing reference signal is too low to be used as an ESO reference. Select a different ESO reference. Refer to the “Provisioning ESO references” procedure in Part 2 of *Configuration - Provisioning and Operating*, 323-1851-310.

Procedure 5-249 (continued)
Threshold AIS ESO-A/ESO-B

Step	Action						
19	<p>If the original alarm has</p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 40%;">cleared</td> <td style="width: 60%;">Then the procedure is complete</td> </tr> <tr> <td>not cleared</td> <td>go to step 20</td> </tr> </table>	cleared	Then the procedure is complete	not cleared	go to step 20		
cleared	Then the procedure is complete						
not cleared	go to step 20						
20	<p>Verify the actual quality for the active timing distribution reference.</p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 40%;">If the actual quality is</td> <td style="width: 60%;">Then</td> </tr> <tr> <td>equal or below (SONET mode) or below (SDH or SDH-J mode) the provisioned threshold AIS value</td> <td>verify the source of the active timing distribution reference, then repeat from step 11</td> </tr> <tr> <td>equal (SONET mode) or equal or above (SDH or SDH-J mode) the provisioned threshold AIS value</td> <td>contact your next level of support or your Ciena support group. The procedure is complete.</td> </tr> </table>	If the actual quality is	Then	equal or below (SONET mode) or below (SDH or SDH-J mode) the provisioned threshold AIS value	verify the source of the active timing distribution reference, then repeat from step 11	equal (SONET mode) or equal or above (SDH or SDH-J mode) the provisioned threshold AIS value	contact your next level of support or your Ciena support group. The procedure is complete.
If the actual quality is	Then						
equal or below (SONET mode) or below (SDH or SDH-J mode) the provisioned threshold AIS value	verify the source of the active timing distribution reference, then repeat from step 11						
equal (SONET mode) or equal or above (SDH or SDH-J mode) the provisioned threshold AIS value	contact your next level of support or your Ciena support group. The procedure is complete.						

—end—

Figure 5-4
Synchronization



Procedure 5-250

Time Out

Alarm ID: 1134

Probable cause

This alarm is raised when:

- On a major-ring or sub-ring, a node is not receiving any R-APS messages on a ringlet port for at least 3.5 consecutive long R-APS frame intervals while that ring port does not report any link level failures and is not administratively disabled.
- A ringlet instance that is not the RPL owner receives no R-APS OK message while it is transmitting R-APS RIM messages for more than 13 minutes (longer than the maximum Wait To Restore time).
- A circuit pack on the ring does a warm restart.
- The Ring ID-Ringlet ports are consistent across the network for a particular ring.

ATTENTION

For a L2 MOTR circuit pack provisioned with an infinite wait-to-restore period, the Time Out alarm will not be raised when the ring fails to revert.

Impact

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

Step	Action
1	If the alarm is raised due to a warm restart of a circuit pack, wait for the restart to be completed and the circuit pack to start sending the APS messages. If this is not the case or the alarm did not clear, go to the step 2 .
2	Verify if the Ring ID-Ringlet port is consistent across the network for a particular ring. In case of inconsistency, provision the Ring ID-Ringlet port to be the same at each node.
3	For all shelves in the ringlet, launch Data Services: G.8032 ERP Management. On the Ringlet Provisioning tab, perform a retrieval, filtering by Ring ID and Group ID, to find the ringlet which has raised the Time Out alarm.
4	Identify the RPL owner. This is the G.8032 ERP with a ring port in the RPL Port column. Note the State of the RPL owner.
5	If the state of the RPL owner is
	Then go to
	Idle or Protected
	step 6
	Init
	step 10

Procedure 5-250 (continued)

Time Out

Step	Action
6	Launch Performance: Operational Measurements. Select a Type of RLE. Select a Facility, Ring ID and Group ID for the ringlet port to monitor. Click Start Monitoring. In Idle state, the RPL owner originates R-APS(OK) messages. All other nodes in the ringlet receive and forward these messages. In the Protected state, the nodes which have detected the failure originate R-APS (FIM) or R-APS (RIM) messages. All other nodes in the ringlet receive and forward these messages.
7	Use the OM counters to verify that the appropriate messages are being originated, received and forwarded as expected.
8	Once it is determined which port is not forwarding messages, return to the G.8032 ERP Management application. Verify that an RLE for the ringlet is provisioned for that port.
9	The alarm clears if the expected R-APS messages are received for the given ringlet. If the alarm does not clear, contact your next level of support or Ciena support group. This procedure is completed.
10	Init state may indicate that provisioning is incomplete on the RPL owner. Verify that RLEs for the ringlet are provisioned for that node.
11	The alarm clears if the expected R-APS messages are received for the given ringlet. If the ringlet state changes from Init to Protected or Idle, but the Time Out alarm does not clear, start this procedure again from step 6 .
12	If after the expiry of the Wait to Restore timer, the state is still Init, contact your next level of support or Ciena support group.

—end—

Procedure 5-251

Timing Distribution Loss of Reference - n Ref

Alarm IDs: 385, 386, 387, 388

Probable cause

This alarm is raised when all of the following are true:

- At least one timing reference is provisioned for timing distribution.
- The **n**-th provisioned timing reference in the timing distribution hierarchy fails.

Up to four timing references can be provisioned. That is, **n** can be 1, 2, 3, or 4.

When this alarm is raised, the **n**-th timing reference is not available. A timing protection switch occurs when another timing reference is provisioned and available for timing distribution. Otherwise, an AIS is transmitted on the ESO output (DS1 and E1 signals) or the ESO signal is squelched (2 MHz signal).

Impact

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

Prerequisites

To perform this procedure, you require an account with at least a level 3 UPC.

Step	Action	
1	Identify the OCn/STMn slot and port, or ESI port raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document.	
2	View the provisioned timing references in the timing distribution hierarchy. Refer to the “Retrieving synchronization data for a network element” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.	
3	If the failed timing reference is derived from an ESI port and any alarms (such as Loss Of Signal [ESI]) are raised against the ESI port)	Then go to step 4
	the failed timing reference is derived from an OCn/STMn signal and any alarms (such as Loss Of Signal or Loss of Frame) are raised against the corresponding OCn/STMn port.	step 5
	no alarms are raised against the corresponding ESI port or OCn/STMn port	step 7

5-552 Alarm clearing procedures—I to Z

Procedure 5-251 (continued)

Timing Distribution Loss of Reference - n Ref

Step	Action				
4	Clear any alarms against the ESI port associated with the failed timing distribution reference. Go to step 6 .				
5	Clear any alarms against the OCn/STMn port associated with the failed timing distribution reference.				
6	If the original alarm has Then <hr/> <table><tr><td>cleared</td><td>the procedure is complete</td></tr><tr><td>not cleared</td><td>go to step 7</td></tr></table>	cleared	the procedure is complete	not cleared	go to step 7
cleared	the procedure is complete				
not cleared	go to step 7				
7	If the alarm does not clear, contact your next level of support or your Ciena support group.				

—end—

Procedure 5-252

Timing Generation Entry to Freerun

Alarm IDs: 68, 971

Probable cause

This alarm is raised against:

- a shelf (XC circuit pack providing timing) when the timing mode is provisioned as external, line, or mixed
- a SuperMux timing group (only when SuperMux in Standalone or Dual mode) when a SuperMux circuit pack provides timing for an independent timing group
- an L2 MOTR circuit pack
- an eMOTR circuit pack

when:

- no timing generation references have been provisioned
- timing generation references have been provisioned but are unusable, and the synchronization hardware on the XC, L2 MOTR, eMOTR, or SuperMux circuit pack cannot lock any of the provisioned timing generation references

In the presence of an ODU AIS, ODU LCK, ODU OCI, or an ETH10G Remote Fault, this alarm can be raised on a line-timed Flex MOTR.

This alarm is raised during the commissioning of the system when the timing mode is provisioned before the timing generation references are provisioned. The alarm clears once the timing generation references are provisioned during commissioning and the synchronization hardware on the XC, L2, MOTR, eMOTR, or SuperMux circuit pack locks to one of the provisioned timing generation references that is usable.

A timing generation reference is unusable if:

- the clock signal is faulty due to a facility fault (for example, Loss Of Signal, Loss of Frame, AIS)
- the synchronization status message (SSM) quality level is below the minimum (ST3/SSU-B)

Procedure 5-252 (continued)

Timing Generation Entry to Freerun

A Timing Generation Entry to Freerun alarm is also raised if a forced switch is applied to a faulty timing reference source or all usable timing generation references have a lockout applied (before the XC, L2, MOTR, eMOTR, or SuperMux circuit pack can lock any of the provisioned timing generation references).

While the alarm is raised, the XC, L2, MOTR, eMOTR, or SuperMux circuit pack provides timing references of Stratum 3 (SONET)/G.813 option 1 (SDH) quality (± 4.6 ppm).

The alarm clears when:

- the synchronization hardware on the XC, L2, MOTR, eMOTR, or SuperMux circuit pack locks to one of the provisioned timing generation references which is usable
- the timing mode is changed to internal

Impact

Warning

Prerequisites

To perform this procedure, you require an account with at least a level 3 UPC.

Step	Action
1	<p>Check that the correct timing mode has been provisioned. Refer to the “Retrieving synchronization data for a network element” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i>, 323-1851-310.</p> <p>If necessary, provision the correct timing mode. Refer to the “Provisioning the network element timing mode and references” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i>, 323-1851-310.</p>
2	<p>If the timing mode has been provisioned, check that the correct timing generation references have been provisioned. Refer to the “Retrieving synchronization data for a network element” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i>, 323-1851-310.</p> <p>If necessary, provision the timing generation references. Refer to the “Provisioning the network element timing mode and references” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i>, 323-1851-310.</p>

Procedure 5-252 (continued)

Timing Generation Entry to Freerun

Step	Action								
3	<p>Check the synchronization protection switching to see if there are any lockouts on usable references or forced switches to unusable timing generation references. Refer to the “Retrieving synchronization protection status details” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i>, 323-1851-310.</p> <p>If there are any lockouts on usable references or forced switches to unusable timing generation references, check that the switches are still required. If the switches are not required, release them. Refer to the “Releasing a synchronization protection switch” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i>, 323-1851-310.</p>								
4	<table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; width: 40%;">If the original alarm has</th> <th style="text-align: left; width: 60%;">Then</th> </tr> </thead> <tbody> <tr> <td>cleared</td> <td>the procedure is complete</td> </tr> <tr> <td>not cleared and a Timing Generation Failure to Lock alarm is present</td> <td>go to step 5</td> </tr> <tr> <td>not cleared and a Timing Generation Failure to Lock alarm is not present</td> <td>go to step 7</td> </tr> </tbody> </table>	If the original alarm has	Then	cleared	the procedure is complete	not cleared and a Timing Generation Failure to Lock alarm is present	go to step 5	not cleared and a Timing Generation Failure to Lock alarm is not present	go to step 7
If the original alarm has	Then								
cleared	the procedure is complete								
not cleared and a Timing Generation Failure to Lock alarm is present	go to step 5								
not cleared and a Timing Generation Failure to Lock alarm is not present	go to step 7								
5	Clear the Timing Generation Failure to Lock alarm. Refer to “ Timing Generation Failure To Lock ” on page 5-560.								
6	<table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; width: 40%;">If the original alarm has</th> <th style="text-align: left; width: 60%;">Then</th> </tr> </thead> <tbody> <tr> <td>cleared</td> <td>the procedure is complete</td> </tr> <tr> <td>not cleared</td> <td>go to step 7</td> </tr> </tbody> </table>	If the original alarm has	Then	cleared	the procedure is complete	not cleared	go to step 7		
If the original alarm has	Then								
cleared	the procedure is complete								
not cleared	go to step 7								
7	<p>Check the SSM status (incoming received quality and the incoming provisioned quality) of all the timing generation references. Refer to the “Retrieving synchronization data for a network element” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i>, 323-1851-310.</p> <table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; width: 40%;">If</th> <th style="text-align: left; width: 60%;">Then go to</th> </tr> </thead> <tbody> <tr> <td>the incoming provisioned quality of a reference is ‘None’ and is below the minimum (ST3/SSU-B)</td> <td>step 8</td> </tr> <tr> <td>the incoming received quality of a reference is below the minimum (ST3/SSU-B)</td> <td>step 9</td> </tr> <tr> <td>otherwise</td> <td>step 11</td> </tr> </tbody> </table>	If	Then go to	the incoming provisioned quality of a reference is ‘None’ and is below the minimum (ST3/SSU-B)	step 8	the incoming received quality of a reference is below the minimum (ST3/SSU-B)	step 9	otherwise	step 11
If	Then go to								
the incoming provisioned quality of a reference is ‘None’ and is below the minimum (ST3/SSU-B)	step 8								
the incoming received quality of a reference is below the minimum (ST3/SSU-B)	step 9								
otherwise	step 11								
8	Check the network synchronization plan to see if the provisioned incoming quality override is correct for each timing generation reference. If necessary correct the incoming override quality level. Refer to the “Setting the synchronization status message override quality level” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.								

Procedure 5-252 (continued)

Timing Generation Entry to Freerun

Step	Action						
9	<p>Check the network synchronization plan to see if the incoming received quality level is expected. If not:</p> <ul style="list-style-type: none"> check and correct the outgoing quality override on the corresponding facility at the far-end network element. Refer to the “Setting the synchronization status message override quality level” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i>, 323-1851-310. check the far-end network element for synchronization problems that can cause the outgoing facility to transmit an SSM below the minimum (ST3/SSU-B). 						
10	<p>If the original alarm has</p> <table> <thead> <tr> <th data-bbox="532 699 579 713">Then</th> <th data-bbox="851 699 909 713"></th> </tr> </thead> <tbody> <tr> <td data-bbox="532 730 579 745">cleared</td> <td data-bbox="851 730 1157 745">the procedure is complete</td> </tr> <tr> <td data-bbox="532 760 579 775">not cleared</td> <td data-bbox="851 760 1002 775">go to step 11</td> </tr> </tbody> </table>	Then		cleared	the procedure is complete	not cleared	go to step 11
Then							
cleared	the procedure is complete						
not cleared	go to step 11						
11	If the alarm does not clear, contact your next level of support or your Ciena support group.						

—end—

Procedure 5-253

Timing Generation Entry to Holdover

Alarm IDs: 69, 972

Probable cause

This alarm is raised against:

- a shelf (XC providing timing) when the timing mode is provisioned as external, line, or mixed
- a SuperMux timing group (only when SuperMux in Standalone or Dual mode) when a SuperMux circuit pack provides timing for an independent timing group
- an L2 MOTR circuit pack
- an eMOTR circuit pack

when all the provisioned timing generation references have become unusable and can no longer be locked by the synchronization hardware on the XC, L2, MOTR, eMOTR, or SuperMux circuit pack.

A timing generation reference becomes unusable if:

- the clock signal is faulty due to a facility fault (for example, Loss Of Signal, Loss of Frame, AIS)
- the synchronization status message (SSM) quality level is below the minimum (ST3/SSU-B)

In the presence of an ODU AIS, ODU LCK, ODU OCI, or an ETH10G Remote Fault, this alarm can be raised on a line-timed Flex MOTR.

A Timing Generation Entry to Holdover alarm is also raised if a forced switch is applied to a faulty timing reference source or all usable timing generation references have a lockout applied.

The XC, L2, MOTR, eMOTR, or SuperMux circuit pack maintains synchronization based on the last valid timing reference signal for at least 24 hours at a guaranteed holdover quality (± 0.37 ppm).

The alarm clears when one of the timing generation references becomes usable and the synchronization hardware on the XC, L2, MOTR, eMOTR, or SuperMux circuit pack locks to one of the timing references.

Impact

Warning

Prerequisites

To perform this procedure, you must

- have the network synchronization plan
- use an account with at least a level 3 UPC

Step	Action								
1	<p>Check that the correct timing mode has been provisioned. Refer to the “Provisioning the network element timing mode and references” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i>, 323-1851-310.</p> <p>If necessary, provision the correct timing mode. Refer to the “Provisioning the network element timing mode and references” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i>, 323-1851-310.</p>								
2	<p>If the timing mode has been provisioned, check that the correct timing generation references have been provisioned. Refer to the “Provisioning the network element timing mode and references” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i>, 323-1851-310.</p> <p>If necessary, provision the timing generation references. Refer to the “Provisioning the network element timing mode and references” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i>, 323-1851-310.</p>								
3	<p>Check the synchronization protection switching to see if there are any lockouts on usable references or forced switches to unusable timing generation references. Refer to the “Retrieving synchronization protection status details” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i>, 323-1851-310.</p> <p>If there are any lockouts on usable references or forced switches to unusable timing generation references, check that the switches are still required. If the switches are not required, release them. Refer to the “Releasing a protection switch” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i>, 323-1851-310.</p>								
4	<table style="width: 100%; border-collapse: collapse;"><thead><tr><th style="width: 40%;">If the original alarm has</th><th style="width: 60%;">Then</th></tr></thead><tbody><tr><td>cleared</td><td>the procedure is complete</td></tr><tr><td>not cleared and a Timing Generation Failure to Lock alarm is present</td><td>go to step 5</td></tr><tr><td>not cleared and a Timing Generation Failure to Lock alarm is not present</td><td>go to step 7</td></tr></tbody></table>	If the original alarm has	Then	cleared	the procedure is complete	not cleared and a Timing Generation Failure to Lock alarm is present	go to step 5	not cleared and a Timing Generation Failure to Lock alarm is not present	go to step 7
If the original alarm has	Then								
cleared	the procedure is complete								
not cleared and a Timing Generation Failure to Lock alarm is present	go to step 5								
not cleared and a Timing Generation Failure to Lock alarm is not present	go to step 7								
5	Clear the Timing Generation Failure to Lock alarm. Refer to “ Timing Generation Failure To Lock ” on page 5-560.								

Procedure 5-253 (continued)

Timing Generation Entry to Holdover

--end--

Procedure 5-254 Timing Generation Failure To Lock

Alarm IDs: 145, 973

Probable cause

- This alarm is raised against;
- a shelf (XC providing timing) when the timing mode is provisioned as external, line, or mixed
- a SuperMux timing group (only when SuperMux in Standalone or Dual mode) when a SuperMux circuit pack provides timing for an independent timing group
- an L2 MOTR circuit pack
- an eMOTR circuit pack

when:

- there is a loss of all provisioned timing generation references
- the incoming quality of all provisioned timing generation references, as determined by the SSM, is below the quality of the internal clock
- synchronization hardware on the XC, L2, MOTR, eMOTR, or SuperMux circuit pack is not locked to a timing reference

In the presence of an ODU AIS, ODU LCK, ODU OCI, or an ETH10G Remote Fault, this alarm can be raised on a line-timed Flex MOTR.

When there is a loss of all provisioned timing references, the network element enters holdover mode. After 24 hours in holdover mode, the network element may operate in freerun mode. In holdover mode, the internal clock operates at a fixed frequency according to the last known frequency reference. In freerun mode, the network element synchronization is based on the internal Stratum 3 (SONET)/G.813 Option 1 (SDH) compliant 4.6 ppm clock.

Impact

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

Prerequisites

To perform this procedure, you require an account with at least a level 3 UPC.

Procedure 5-254 (continued)
Timing Generation Failure To Lock

Step	Action	
1	Verify the timing generation (timing mode and references) for the network element. Refer to the “Retrieving synchronization data for a network element” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.	
2	If the original alarm has	Then
	cleared	the procedure is complete
	not cleared	go to step 3
3	If Timing Generation Loss of Reference - n Ref alarms are	Then go to
	raised	step 4
	not raised	step 6
4	Clear all raised Timing Generation Loss of Reference - n Ref alarms. Refer to “Timing Generation Loss of Reference - n Ref” on page 5-562. Wait two to five minutes.	
5	If the original alarm has	Then
	cleared	the procedure is complete
	not cleared	go to step 6
6	If the alarm does not clear, verify the quality level of the timing references to determine if the synchronization quality is lower than the network element internal clock quality. Refer to the “Retrieving synchronization data for a network element” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310. If the quality level of the timing references is lower than the network element, investigate the timing reference sources.	
7	If the alarm does not clear, contact your next level of support or your Ciena support group.	

—end—

Procedure 5-255

Timing Generation Loss of Reference - n Ref

Alarm IDs: 401, 402, 403, 404, 405, 406, 407, 408

Probable cause

This alarm is raised against:

- a shelf when a XC circuit pack provides timing
- a SuperMux timing group (only when SuperMux in Standalone or Dual mode) when a SuperMux circuit pack provides timing for an independent timing group
- an L2 MOTR circuit pack
- an eMOTR circuit pack

This alarm is raised when all of the following are true:

- the timing mode for the timing group is provisioned as external, line, or mixed (only line timing is supported within independent timing groups)
- at least one timing reference is provisioned for timing generation
- the **n**-th provisioned timing reference in the timing generation hierarchy fails

In the presence of an ODU AIS, ODU LCK, ODU OCI, or an ETH10G Remote Fault, this alarm can be raised on a line-timed Flex MOTR.

When a XC circuit pack provides timing, up to four timing references can be provisioned (that is, **n** can be 1, 2, 3, or 4). When a SuperMux circuit pack provides timing, up to two timing references can be provisioned (that is, **n** can be 1 or 2).

When this alarm is raised, the **n**-th timing reference is not available. A timing protection switch occurs when another timing reference is provisioned and available for timing generation. Otherwise, the shelf enters timing holdover mode.

Procedure 5-255 (continued)

Timing Generation Loss of Reference - n Ref**Impact**

Minor, non-service-affecting (m, NSA) alarm if another reference in the timing generation hierarchy is provisioned and available

Major, non-service-affecting (m, NSA) alarm if no other timing generation references are provisioned or available

Prerequisites

To perform this procedure, you require an account with at least a level 3 UPC.

Step Action

- 1** Identify the OCn/STMn slot and port, ETTP/ODUTTP eMOTR facilities, or ESI port raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document.

Note: On the XC circuit packs, the synchronization status LED (yellow circle) that corresponds to the failed reference (1, 2, 3, or 4) is lit if the corresponding reference (1, 2, 3, or 4) is lost. This condition occurs for a Loss Of Signal on an ESI port or a failed reference (Loss Of Signal, Loss of Frame, excessive bit error rate, or AIS) on optical interfaces.

To view the provisioned timing references in the timing generation hierarchy, refer to the “Retrieving synchronization data for a network element” procedure in Part 2 of *Configuration - Provisioning and Operating*, 323-1851-310.

- | | | |
|----------|---|------------------------|
| 2 | If | Then go to |
| | the failed timing reference is derived from an ESI port and any alarms are raised against the ESI port | step 3 |
| | the failed timing reference is derived from an OCn/STMn signal, ETTP/OTUTTP eMOTR facilities, and any alarms (such as Loss Of Signal or Loss of Frame) are raised against the corresponding OCn/STMn port | step 4 |
| | no alarms are raised against the corresponding ESI port or OCn/STMn port | step 6 |
| 3 | Clear any alarms against the ESI port associated with the failed timing generation reference. Go to step 5 . | |
| 4 | Clear any alarms against the OCn/STMn or ETTP/OTUTTP eMOTR facilities associated with the failed timing generation reference. | |

5-564 Alarm clearing procedures—I to Z

Procedure 5-255 (continued)

Timing Generation Loss of Reference - n Ref

Step	Action
5	If the original alarm has cleared the procedure is complete
	not cleared go to step 6
6	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-256 **TOD Server Not Provisioned**

Alarm ID: 575

Probable cause

This alarm is raised when the shelf is provisioned to retrieve its date and time from a Network Time Protocol (NTP) server but the NTP server attributes have not yet been provisioned.

This alarm is raised for an IPv4 and/or IPv6 provisioned server. IPv6 must be enabled if an IPv6 server is provisioned and IPv4 must be enabled if an IPv4 server is provisioned.

Impact

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

Prerequisites

To perform this procedure you must:

- confirm that the date and time will be retrieved from an NTP server
 - know the IP addresses of and have access to the NTP servers
 - use an account with at least a level 3 UPC

Step	Action	
1	Select Node Information from the Configuration menu. Select the Time of Day tab in the Node Information application. Refer to the “Displaying node information” procedure in <i>Administration and Security</i> , 323-1851-301.	
2	If the date and time should be	Then
	set manually	in the Settings area, click on Edit .
	retrieved from an NTP server	In the Time of Day Settings dialog box, set Status to Off to disable the Time of Day Mode (TOD Sync).
		The procedure is complete.
3	If the original alarm has	Then
	cleared	the procedure is complete
	not cleared	go to step 4

5-566 Alarm clearing procedures—I to Z

Procedure 5-256 (continued) **TOD Server Not Provisioned**

Step	Action
4	Verify if the “Unable to Synchronize TOD” alarm has not been raised. If so, refer to the alarm clearing procedure for the alarm to clear the alarm.
5	If the original alarm has Then
	cleared the procedure is complete
	not cleared go to step 6
6	If the alarm does not clear, contact your next level of support or your Ciena support group.

Procedure 5-257

TODR Reversion Inhibited

Alarm ID: 1828, 1829, 1834

Probable cause

This alarm is raised when all TODR profiles, assigned to OTN Control Plane SNCP protection groups and ASNCP protection groups are disabled.

The alarm is raised for ASNCP/SNCP protection groups, when they are provisioned as Revertive.

Impact

Warning

Prerequisites

To perform this procedure, you require an account with at least a level 3 UPC.

Step	Action
1	Enable at least one of the TODR profiles assigned to the ASNCP/SNCP OTN protection group. Refer to the “Editing a TODR profile” procedure in <i>Configuration - Control Plane</i> , 323-1851-330.
2	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-258

TOD Threshold Exceeded

Alarm ID: 335

Probable cause

The alarm is raised by the shelf processor when TOD server provided TOD varies from NE time by 10 minutes or more.

Impact

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

Prerequisites

To perform this procedure you must:

- confirm that the date and time will be retrieved from an NTP server
- know the IP addresses of and have access to the NTP servers
- use an account with at least a level 3 UPC

Step	Action
1	<p>Operate a time of day synchronization as follows:</p> <ul style="list-style-type: none">• Select the required network element in the navigation tree.• Select Node Information from the Configuration drop-down menu to open the Node Information window.• Select the Time Of Day tab.• Click Synchronize (in the Servers area of the window) to initiate a time of day synchronization.• If the synchronization is successful, the Detected offset field is set to 00:00:00, and the alarm clears.• Click Refresh to update the Node Information window
2	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-259 Topology Build Failed

Alarm ID: 1799

Probable cause

This warning is raised to indicate that the topology build (NCT build) is failing in the background after a successful build. The build can fail due to a COMMS failure or misprovisioning.

This warning is raised against an OTS one hour after detecting the build failure.

Impact

Warning

Step	Action
1	Verify the Customer Visible Logs (CVL) for any reasons for the build failure. Refer to the DOC logs section in <i>Fault Management - Customer Visible Logs</i> , 323-1851-840, for troubleshooting information.
2	Verify the COMMS for failure.
3	Verify the provisioning and validate that the Domain is defined properly.
4	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-260

Topology Failure

Alarm ID: 813

Probable cause

This alarm is raised when the data entered by the user in the RPR configuration is invalid or the configuration data is found to be inconsistent with network element data. Examples are, the existing RPR provisioning, or with the TID-MAC addresses pairs found in the routing tables.

The alarm is due to an RPR station mismatch, created when EAST and WEST are swapped. Therefore, the EAST of the near-end network element is connected to the EAST of the far-end network element instead of the WEST of the far-end network element. This is due to a provisioning error or misconnected cables.

This alarm applies to RPR facilities only.

Impact

Critical, service-affecting (C, SA) alarm

Step	Action
------	--------

- 1 Use the consistency icon from Site Manager to find which nodes are the source of the conflict. Refer to the “Viewing information for resilient packet rings” procedure in Part 2 of *Configuration - Bandwidth and Data Services*, 323-1851-320.
- 2 Update the configuration data to ensure the provisioned data and the configuration data is consistent. Refer to the “Retrieving ring configuration files” procedure in Part 1 of *Configuration - Bandwidth and Data Services*, 323-1851-320.
- 3 If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-261

Topology Instability

Alarm ID: 814

Probable cause

This alarm is raised when the configuration data and the data from the network element are not consistent and the instability defect has not been cleared within the instability timeout value (10 sec).

This alarm applies to RPR facilities only.

Impact

Critical, service-affecting (C, SA) alarm

Step	Action
1	Verify the configuration data and compare it to the data from the network element.
2	Use the consistency icon from Site Manager to determine which nodes are the source of the conflict. Refer to the “Viewing information for resilient packet rings” procedure in Part 2 of <i>Configuration - Bandwidth and Data Services</i> , 323-1851-320.
3	Update the configuration data to ensure the provisioned data and the configuration data is consistent. Refer to the “Retrieving ring configuration files” procedure in Part 1 of <i>Configuration - Bandwidth and Data Services</i> , 323-1851-320.
4	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-262

Trace Identifier Mismatch (OCn/STMn)

Alarm IDs: 2, 137, 152, 280, 899, 983, 1694

Probable cause

This alarm is raised when the section trace identifier value received by the facility differs from the expected provisioned section trace value. This can be the result of incorrect fibering or incorrect provisioning of the section trace value.

This alarm will not condition the STS-1 (high-speed side) on the 48 Channel Trans Mux (portless) circuit pack with path AIS, unlike all other path-terminating interfaces on the 6500.

Note that enabling path AIS insertion on the optics (general NE setting) will condition a Trace Identifier Mismatch alarm with path AIS.

For 10x10G MUX circuit packs, this alarm is masked by AIS-L.

For the HO 10 port, 20G OC-n/STM-n, section Trace failure mode can be provisioned as follows (default is “Alarm Only”):

- Off: No alarm is raised when the expected section trace and the received section trace are mismatched.
- Alarming Only: The “Trace Identifier Mismatch” Major alarm is raised when the expected section trace and the received section trace are mismatched.
- Line Fail: If the expected section trace and the received section trace are mismatched, a “Trace Identifier Mismatch” alarm is raised as Major or Minor depending on whether the facility is carrying traffic. A consequent action is triggered, causing AIS-L towards the backplane and RDI-L to be transmitted upstream. The condition is interpreted as a signal fail condition by protection.

If the Section Trace failure mode is Line Fail, the user is unable to change other section trace parameters without changing the failure mode.

If the Trace Fail mode is set to “Line Fail”, such that the “Trace Identifier Mismatch” alarm triggers a protection switch, then it is a higher priority than AIS-L and will mask AIS-L.

If the Trace Fail mode is set to “Alarm Only”, such that the “Trace Identifier Mismatch” alarm only raises an alarm and does not trigger a protection switch, then it is a lower priority than AIS-L and is masked by AIS-L.

Procedure 5-262 (continued)

Trace Identifier Mismatch (OCn/STMn)

Trace identifier mismatch detection can be enabled or disabled on a per payload instance basis. By default, detection is disabled.

The “Trace Identifier Mismatch” alarm is raised when trace identifier detection is enabled and the expected and incoming trace identifiers do not match.

Impact

Major, service-affecting (M, SA) alarm, if in Alarms on, with traffic protection mode

Major, service-affecting (M, SA) alarm for the UPSR/SNCP configuration with cross-connects, if in Alarms on, with traffic protection mode

Major, service-affecting (M, SA) alarm, if active 1+1/MSP linear, 1+1 port TPT, or 1+1 TPT or unprotected with cross-connects, if in Alarms on, with traffic protection mode

Minor, non-service-affecting (m, NSA) alarm, if inactive 1+1/MSP linear, 1+1 port TPT, or 1+1 TPT, protected 1+1/MSP linear, 1+1 port TPT, or 1+1 TPT, or without cross-connects, if in Alarms on, with traffic protection mode

ATTENTION

This alarm has dual severity in Alarms on, with traffic protection mode with 1+1/MSP linear, 1+1 port TPT, or 1+1 TPT protection.

Prerequisites

To perform this procedure, you must

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545
- have the optical fiber/cable connection information (that is, how the modules on each network element connect to other network elements)
- use an account with at least a level 3 UPC

Procedure 5-262 (continued)

Trace Identifier Mismatch (OCn/STMn)

Step	Action
1	Retrieve the section trace format and values on OC-n/STM-n facilities at the transmit network element, and at the alarmed receive network element on optical facilities at the transmit network element and at the alarmed receive network element. Refer to the “Retrieving and editing section trace messages” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
2	Compare the outgoing section trace value of the transmit signal at the transmit network element with the expected section trace value of the receive signal at the receive network element. If the values are different, change the expected section value of the receive signal to match the outgoing section trace value of the transmit signal. Refer to the “Retrieving and editing section trace messages” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310. Note: If the received section trace value is null, changing the expected section trace value to null clears the alarm.
3	Click Refresh in the Section Trace dialog box.
4	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-263

Trace Identifier Mismatch (STS/HO VC and VT/LO VC)

Alarm IDs: 50, 332, 361, 362, 457, 458, 563, 564, 2054, 2086

Probable cause

This alarm is raised against a PATH or STTP facility, STS/HO VC or VT/LO VC path when the incoming and expected path trace values are different. This alarm is also raised if a connection mismatch or an optical fiber connection mismatch exists.

If this alarm is raised against an OCn/STMn facility, refer to “[Trace Identifier Mismatch \(OCn/STMn\)](#)” on page 5-572.

Note: The path Trace Identifier Mismatch alarm can take up to 48 seconds to be raised after the mismatch exists.

For STS/HO VC paths, use the Monitoring enabled check box in the Path Provisioning dialog box to enable or disable path trace monitoring. Refer to the “Retrieving and editing path provisioning” procedure in Part 1 of *Configuration - Provisioning and Operating*, 323-1851-310. By default, path trace monitoring is disabled. When path trace monitoring is enabled, this alarm is raised when the outgoing path trace message at one end and the expected path trace message at the other end are different. In 1+1/MSP mode, path trace mismatch alarms are raised against working optical interface circuit packs.

For VT/LO VC paths, the provisioning and monitoring of the path trace message monitoring is controlled by the Extended check box in the Path Provisioning dialog box and applies to optical interface circuit packs only. Use the Extended check box to enable or disable path trace monitoring and provisioning (expected receive message only). The Extended feature can only be enabled on a maximum of 1344 VT/LO VC paths for each optical interface circuit pack.

Note: Path trace on the multi-rate optical OC-n/STM-n (MRO) circuit pack will not raise a “Trace Identifier Mismatch” alarm if the incoming path trace is a subset of the expected path trace.

Impact

- Major, service-affecting (M, SA) alarm, if on active path
- Minor, non-service-affecting (m, NSA) alarm, if on inactive path in a UPSR/SNCP configuration
- Critical, service-affecting (C, SA) alarm

Prerequisites

To perform this procedure, you must

- have the optical fiber connection information (that is, how the modules on each network element connect to other network elements)
- use an account with at least a level 3 UPC

Step	Action
1	Verify if there are alarms of higher order from the alarm hierarchy. Refer to the “Alarm hierarchies and alarm severities” chapter in Part 1 of this document.
2	Clear any alarms of higher order using the appropriate procedures.
3	If the original alarm has Then
	cleared the procedure is complete
	not cleared go to step 4
4	Identify the circuit pack raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document.
5	Use the optical fiber connection information to identify the transmit and receive ends of the STS/VT/VC path.
6	For an STS/VC4-n path, retrieve and record the path trace messages at both ends. Refer to the “Retrieving and editing path provisioning” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310. For a VT1.5/VC11 or VT2/VC12 path, verify the path trace provisioning at each node with a VT1.5/VC11 or VT2/VC12 connection. Refer to the “Retrieving and editing path provisioning” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.

- | | |
|---|--|
| 1 | Verify if there are alarms of higher order from the alarm hierarchy. Refer to the “Alarm hierarchies and alarm severities” chapter in Part 1 of this document. |
| 2 | Clear any alarms of higher order using the appropriate procedures. |
| 3 | If the original alarm has Then |
| | cleared the procedure is complete |
| | not cleared go to step 4 |
| 4 | Identify the circuit pack raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document. |
| 5 | Use the optical fiber connection information to identify the transmit and receive ends of the STS/VT/VC path. |
| 6 | For an STS/VC4-n path, retrieve and record the path trace messages at both ends. Refer to the “Retrieving and editing path provisioning” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
For a VT1.5/VC11 or VT2/VC12 path, verify the path trace provisioning at each node with a VT1.5/VC11 or VT2/VC12 connection. Refer to the “Retrieving and editing path provisioning” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310. |

Procedure 5-263 (continued)

Trace Identifier Mismatch (STS/HO VC and VT/LO VC)

Step	Action
7	<p>Ensure that path trace is provisioned correctly at each network element:</p> <ul style="list-style-type: none"> • Ensure that the path trace Format parameter is provisioned to the same setting at both ends (not applicable to VT1.5/VC11 or VT2/VC12 paths). • Ensure that the outgoing path trace string (Transmitted) at the transmit end matches the incoming expected path trace string (Expected Rx) at the receive end. • To provision path trace, ensure that the cross-connect is already provisioned. Refer to the “Retrieving path connections” procedure in Part 1 of <i>Configuration - Bandwidth and Data Services</i>, 323-1851-320. <p>Note: By default, when the STS/VC path is provisioned, path trace monitoring is disabled. The expected incoming and outgoing path trace values are set to a string of 16 bytes (SDH/SDH-J) or 64 bytes (SONET) of null characters (not applicable to VT1.5/VC11 or VT2/VC12 paths which are always 16 bytes).</p> <p>In 1+1/MSP linear mode, you can only edit the Expected Rx value and the Transmitted value on the working optical interface. You cannot edit the values on the protection optical interface. Path trace on the protection optical interface facility is automatically set to the same format and value set on the working optical interface.</p>
8	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-264

Traffic Squelched

Alarm IDs: 431, 432, 433, 434, 435, 436, 1074, 1075, 1076

Probable cause

This alarm is raised when the network element has squelched traffic on one or more STS/VC or VT paths on an OC-48/STM-16 or OC-192/STM-64 facility in 2-Fiber BLSR/MS-SPRing or 4-Fiber BLSR/MS-SPRing configuration. Path AIS is inserted into the affected incoming and outgoing STS/VC or incoming VT paths.

One of the following conditions causes this alarm:

- node failure or node isolation
- ring segmentation

Node failure, node isolation or ring segmentation can be caused by one of these conditions:

- a fiber cut
- a fiber pulled from the circuit pack
- a circuit pack failure
- a circuit pack pulled from the shelf
- any protection switch

When there is a node failure, node isolation, or ring segmentation, the ring attempts to restore as much traffic as possible through automatic protection switches.

Impact

Critical, service-affecting (C, SA) alarm

Prerequisites

To perform this procedure, you must

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545
- have an antistatic wrist strap to dissipate electrostatic charges

Procedure 5-264 (continued)

Traffic Squelched

Step	Action
1	<p>Identify the circuit pack or circuit packs raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document.</p> <p>The circuit pack performing the traffic squelching is located adjacent to the failed span or node.</p>
2	<p>Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.</p>
3	<p>Once you have identified which node has failed or where the ring is segmented, retrieve alarms from that network element and look for:</p> <ul style="list-style-type: none"> • a Loss Of Signal alarm. The presence of this alarm can indicate a fiber cut. If the fibers have been cut, replace the fibers. If the fibers are not linked, connect them as required. • a Circuit Pack Failed alarm. Refer to the “Circuit Pack Failed” alarm clearing procedure in Part 1 of this document. • a Circuit Pack Missing alarm. Refer to the “Circuit Pack Missing” alarm clearing procedure in Part 1 of this document.
4	<p>The nodes adjacent to the failed span or node are the switching nodes. Retrieve alarms for those nodes and look for:</p> <ul style="list-style-type: none"> • automatic protection switch alarms. Verify the cause of the automatic protection switch. Clear the alarms according to the applicable alarm clearing procedures in this document.
5	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-265

Transport Data Recovery Failed

Alarm ID: 76

Probable cause

This alarm is raised when data is not recovered after a shelf processor (SP) replacement or restart. If a replacement SP is running a release lower than the current release running on the shelf, this alarm may be raised and a “Software Mismatch” alarm will also be raised. An upgrade must be performed to upgrade the software on the SP to match the software release on the shelf.

If a replacement SP is running a release higher than the current release running on the shelf, and is not within the supported upgrade release window, a “Software Mismatch” alarm will also be raised, and a downgrade must be performed to downgrade the software on the SP to match the software release on the shelf.

If this alarm is raised when the SP has the same release as the shelf, then there is an issue with the recovered data, and a database restore may be required. For example, in the case where the alarm is not caused by an SP replacement. This alarm may also be raised when a SP that has data for one shelf type is placed into a different shelf type with no other circuit pack present.

This alarm can also be raised when a “Circuit Pack Failed”, “Circuit Pack Mismatch”, “Circuit Pack Missing”, “Circuit Pack Unknown” or “Intercard Suspected” alarm or condition existed on the network element before a SP replacement.

Impact

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

Step	Action
1	Check the current release running on the network element. Refer to the “Checking the current software release” procedure in <i>Commissioning and Testing</i> , 323-1851-221.
2	If the SP is running a release that is different than that of the shelf, and a “Software Mismatch” alarm is present, go to step 3 . If a Software Mismatch alarm is not present and the SP has been placed into a shelf with no other circuit pack present, go to step 4 , otherwise go to step 5 .

Procedure 5-265 (continued)
Transport Data Recovery Failed

Step	Action
3	Perform an upgrade on the network element. For the upgrade “to release”, use the current release running on the network element. Refer to the 6500 <i>Software Upgrade Procedures</i> for this release listed in the “ <i>Software Upgrade Procedures</i> ” section in <i>Planning - Ordering Information</i> , 323-1851-151. Go to step 6 .
4	Decommission the SP. Refer to the “Deleting all shelf provisioning information for a standalone shelf or all shelves of a consolidated node” procedure in <i>Administration and Security</i> , 323-1851-301. Go to step 6 .
5	Perform a database restore. Refer to the backup and restore procedures in <i>Administration and Security</i> , 323-1851-301.
6	Ensure that the system is restored to its original state by retrieving all conditions and alarms. Clear all alarms using the appropriate alarm clearing procedure.
7	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-266 TR Control Disabled

Alarm ID: 661

Probable cause

This alarm is raised when the user has provisioned the TR controls to the OFF state.

Impact

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

Prerequisites

To perform this procedure, you must

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545
- use an account with at least a level 3 UPC

Step	Action
------	--------

- | | |
|---|---|
| 1 | Provision the TR control to ON. Refer to the “Retrieving and editing TR control information” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310. |
|---|---|

—end—

Procedure 5-267

TR Control Echo Trace Mismatch

Alarm IDs: 660, 1006, 1176, 1437

Probable cause

This alarm is raised when the TR control receives a TxID from the far-end receiver that does not match its own TxID. This indicates a crossed fiber. This alarm clears when TR control receives a TxID from the far-end receiver that matches its own TxID, or when TR control receives no TxID from the far-end receiver.

The alarm is also raised when there is a terminal loopback on the far-end 40G OCLD circuit pack.

This alarm applies to OTM, OTM2, OTM3, OTM4, OTMC2, or PTP facilities of the 10G WT, 10GE LAN WT, 10G OTN WT, 40G OCLD, Wavelength-Selective 40G OCLD, 40G UOCLD, 100G WL3/WL3e OCLD, Flex2 WL3/WL3e OCLD, Flex3 WL3e OCLD, Flex4 WL3e OCLD, 100G WL3e OTR, and 100G OCLD circuit packs.

ATTENTION

On the 40G OCLD circuit pack, when Terminal Loopback is provisioned on the near-end, EOC comms from the far-end are not terminated on the near-end line card. Hence, the “TR Control Echo Trace Mismatch” alarm is raised against the far-end 40G OCLD circuit pack.

Impact

Critical, service-affecting (C, SA) alarm, an active circuit pack in 1+1/MSP linear, 1+1 port TPT, or 1+1 TPT configuration or unprotected with cross-connects provisioned

Minor, non-service-affecting (m, NSA) alarm, an inactive circuit pack in 1+1/MSP linear, 1+1 port TPT, or 1+1 TPT configuration or no cross-connects provisioned

Prerequisites

To perform this procedure, you must

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0
- use an account with at least a level 3 UPC

Procedure 5-267 (continued)
TR Control Echo Trace Mismatch

Step	Action						
1	Identify the circuit pack or circuit packs raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document.						
2	From the Site Manager Configuration menu, select Equipment & Facility Provisioning . Select the alarmed facility, and record the values from the Echoed Trace Rx , Trace Tx , and Associated Far End Rx ID columns. Refer to the “Retrieving equipment and facility details” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.						
3	<table><tr><td data-bbox="527 677 545 699">If the Echoed Trace Rx and Trace Tx values are</td><td data-bbox="1130 677 1269 699">Then go to</td></tr><tr><td data-bbox="527 713 545 732">not equal</td><td data-bbox="1130 713 1269 732">step 4</td></tr><tr><td data-bbox="527 749 545 768">equal</td><td data-bbox="1130 749 1269 768">step 5</td></tr></table>	If the Echoed Trace Rx and Trace Tx values are	Then go to	not equal	step 4	equal	step 5
If the Echoed Trace Rx and Trace Tx values are	Then go to						
not equal	step 4						
equal	step 5						
4	There is likely a misconnected fiber. Verify that the optical fiber connections are correct on the circuit pack raising the alarm and on the upstream circuit pack. The Associated Far End Rx ID value from step 2 indicates where the misconnection exists.						
5	If the alarm does not clear, contact your next level of support or your Ciena support group.						

—end—

Procedure 5-268

TR Control Initialization in Progress

Alarm ID: 658

Probable cause

This alarm is raised when TR control is performing the dispersion scan or OOS optimization process. This alarm indicates that the Tx/Rx pair is not in the IS or SS optimization state.

Typically this alarm clears autonomously within five minutes and is replaced by the TR Control IS Optimization In Progress alarm. The alarm does not clear if the far-end Rx and the near-end Rx are not able to acquire a signal (BER of approximately 3.8E-3).

Impact

Major, service-affecting (M, SA) alarm

Prerequisites

To perform this procedure, you must

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management-Module Replacement*, 323-1851-545
 - use an account with at least a level 3 UPC

Step	Action
1	Wait for the alarm to clear autonomously. When it clears, the TR Control IS Optimization In Progress alarm is raised.
2	If the original alarm has Then cleared the procedure is complete not cleared go to step 3

TR Control Initialization in Progress

Step	Action
3	<p>This indicates that the far-end Rx and the near-end Rx are not able to acquire a signal (BER approximately 3.8E-3). Check the following:</p> <ul style="list-style-type: none">• Ensure that TR Control is enabled at the upstream circuit pack. Refer to the “Retrieving and editing TR control information” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i>, 323-1851-310.• Ensure that the near-end and far-end circuit packs are the same PEC.• Ensure that the photonic layer is properly optimized. Troubleshoot any photonic-related layer alarms.• Ensure the near-end and far-end circuit packs are properly fibered.
4	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-269

TR Control IS Optimization in Progress

Alarm ID: 659

Probable cause

This alarm is raised when TR control is performing the IS optimization process and the Pre-FEC BER has reached a certain level but the system is not optimized. That is, the system is not in the SS (steady state) optimization mode.

This alarm indicates that the Tx/Rx pair is not in the SS optimization state.

This alarm clears autonomously within five minutes, no user action is required.

Impact

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

Step	Action
------	--------

- 1 Wait for the alarm to clear autonomously.
- 2 If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-270

Tributary Slots Not Available

Alarm ID: 2028

Probable cause

This alarm is raised against a ODUCTP facility on the WLAI line port if the allocated Tributary Slots of ODUCTP facility becomes unavailable because it exceeds the maximum capacity of the current provisioned Transmission Mode.

Impact

Warning

Step	Action
1	If this is due to downshifting of Transmission Mode, the alarm will clear after restoration is completed.
2	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-271

Tx AIS (DS1)

Alarm ID: 24

Probable cause

This alarm is raised when the network element detects a failed DS1 signal upstream on the other side of the connection. The network element is transmitting an alarm indication signal (AIS) to the remote end of the input.

This alarm indicates a warning to the downstream network element that the signal is not usable.

This alarm occurs when:

- a DS1 receive fault (for example, Rx Loss Of Signal, Rx loss of frame, Rx AIS) where the signal enters the network. If the DS1 mapping is byte synchronous, additional SONET/SDH alarms are active.
- a SONET fault condition (OC-3/STM-1, OC-12/STM-4, STS-1/VC-3, STS-3c/VC-4, or VT1.5/VC11 alarms) occurs
- no cross-connect assigned for the DS1

This alarm can also be raised if an intrusive test access session is in progress. No action is required if this is the cause.

Impact

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

Prerequisites

To perform this procedure, you must clear all SONET/SDH (OC-3/STM-1, OC-12/STM-4, STS-1/VC-3, STS-3c/VC-4, or VT1.5/VC11) and DS1 Rx alarms related to the circuit path in the network.

Step	Action
1	Another failure in the system normally causes this alarm. If other EC-1, OC-3/STM-1, OC-12/STM-4, STS-1/VC-3, STS-3c/VC-4, VT1.5/VC11, or DS1 Rx alarms exist on the system related to the circuit path, clear them first. Perform this procedure if the Tx AIS alarms are the only active alarms.
2	Identify the 84x DS1 DSM termination module (TM) facility raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document.
3	Retrieve the cross-connects. Refer to the “Retrieving path connections” procedure in Part 1 of <i>Configuration - Bandwidth and Data Services</i> , 323-1851-320.

5-590 Alarm clearing procedures—I to Z

Procedure 5-271 (continued)

Tx AIS (DS1)

Step	Action
4	Look for cross-connects provisioned for the DS1 raising the alarm. If there are no cross-connects for the DS1, the DS1 is in service (IS) without connections. Put the DS1 facility out of service (OOS). Refer to the “Changing the primary state of a facility procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
5	Determine where the DS1 signal enters the network. If the signal is a EC-1, OC-3/STM-1, or OC-12/STM-4, check the connecting equipment and ensure that it is correctly transmitting a DS1 signal.
6	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-272 Tx AIS (DS3/E3)

Alarm IDs: 84, 860

Probable cause

This alarm is raised when the network element detects a failed signal coming from a DS3 interface upstream on the optical fiber side. The network element is transmitting an alarm indication signal (AIS) to the remote end of the input.

The alarm indicates a warning to the downstream network element that the signal is bad.

The following causes this alarm:

- a DS3 receive fault (for example, Rx Loss Of Signal, Loss of Frame, Alarm Indication Signal) on the upstream circuit pack
- a SONET/SDH fault condition (OC-3/STM-1, OC-12/STM-4, or STS-1/VC-3 alarms)
- the DS3 facility detects an outgoing AIS signal if the DS3 frame format is other than unframed
- an E3 Tx AIS alarm is raised when the E3 facility detects an outgoing AIS signal

This alarm can also be raised if an intrusive test access session is in progress. No action is required if this is the cause.

Impact

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

The shelf cannot carry traffic on this DS3/E3 interface.

Prerequisites

To perform this procedure, you must clear all SONET/SDH (OC-3/STM-1, OC-12/STM-4, and STS-1/VC-3) and DS3/E3 Rx alarms from the network.

Step	Action
1	Another failure in the system usually causes this alarm. Clear any other OC-3/STM-1, OC-12/STM-4, STS1/VC-3, or DS3/E3 Rx alarms on the system first. Perform this procedure if the Tx AIS alarms are the only active alarms on the system.
2	Identify the DS3/E3 interface raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document.

5-592 Alarm clearing procedures—I to Z

Procedure 5-272 (continued)

Tx AIS (DS3/E3)

Step	Action
3	Record the facility in the form DS3-slot #-port # or E3-slot #-port #.
4	If there are any connections to the DS3/E3, contact your next level of support or your Ciena support group.
5	If there are no connections, the DS3/E3 is in-service without connections. Put the DS3/E3 facility out of service. Refer to the “Changing the primary state of a facility” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.

—end—

Procedure 5-273

Tx Frequency Out of Range

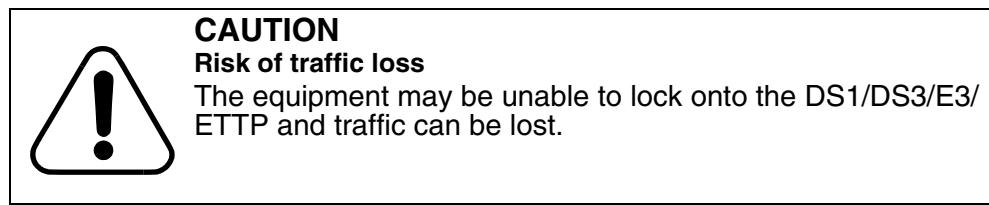
Alarm IDs: 29, 86, 861, 2030

Probable cause

This alarm is raised when the network element detects a DS1/DS3/E3/ETTP signal that is transmitting to the input is out of normal frequency range. The DS1/DS3/E3/ETTP out of frequency range on the input to the system usually causes this alarm. A DS1/DS3/E3/ETTP Rx Frequency Out of Range alarm will also be active.

Impact

Major, service-affecting (M, SA) alarm



Step	Action
1	If possible, clear all SONET/SDH and DS1/DS3/E3/ETTP Rx alarms from the network.
2	If the alarm does not clear, contact your next level of support or your Ciena support group.

- 1 If possible, clear all SONET/SDH and DS1/DS3/E3/ETTP Rx alarms from the network.
- 2 If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-274

Tx Loss of Frame (DS1)

Alarm ID: 22

Probable cause

This alarm is raised when the local network element detects that the DS1 payload from the VT1.5/VC11 transmitted from the shelf is not framed in the same format as the commissioned port.

According to Telcordia GR-253-CORE, Loss of Frame (LOF) on an async mapped DS1 does not result in AIS insertion. An alarm is raised, and the LOF signal passes downstream.

This procedure assumes that the system was operating alarm free before the Tx Loss of Frame alarm. If this alarm is raised during DS1 provisioning, verify the provisioned framing with the test traffic you are running.

Impact

Major, service-affecting (M, SA) alarm

ATTENTION

The payload continues to transmit to the input. However, the change of framing can cause the equipment to reject the DS1 signal.

Prerequisites

To perform this procedure, you must

- clear all SONET (OC-3/STM-1, OC-12/STM-4, STS-1/VC-3, STS-3c/VC-4, and VT1.5/VC11) and DS1 Rx alarms from the network
- have an antistatic wrist strap to dissipate electrostatic charges
- use an account with at least a level 3 UPC

Step	Action
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	Another failure in the system normally causes this alarm. Clear any other OC-3/STM-1, OC-12/STM-4, STS-1/VC-3, VT1.5/VC11 or DS1 Rx alarms on the system first. Perform this procedure if the Tx LOF alarms are the only active alarms on the system.
3	Identify the DSM 84xDS1 termination module (TM) raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document.

Procedure 5-274 (continued)

Tx Loss of Frame (DS1)

Step	Action
4	Record the facility in the form DS1-slot#-port#.
5	<p>Compare the frame format of the DS1. Refer to the “Retrieving equipment and facility details” procedure and “DS1 facility parameters” table in Part 1 of <i>Configuration - Provisioning and Operating</i>, 323-1851-310.</p> <ul style="list-style-type: none"> • If the two frame formats are different, determine which one is correct from company records and edit the incorrect facility. Refer to the “Editing facility parameters” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i>, 323-1851-310. • If the condition does not clear, go to step 6. • If the condition clears, the procedure is completed.
6	Determine the original source of the DS1, the framing it is provisioned for, and ensure that it is generating the correct framing by using your company procedures.
7	Manually switch the DSM 84xDS1 TM reporting the alarm into protection mode. Refer to the “Operating a protection switch” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
8	Wait 30 seconds. If the alarm clears, the working DSM 84xDS1 TM is faulty. Replace the DSM 84xDS1 TM reporting the Tx Loss of Frame alarm. Refer to the “Replacing the DSM 84xDS1 TM circuit pack” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.
9	Release the protection switch you performed at step 7 . Refer to the “Releasing a protection switch” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
10	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-275

Tx Loss of Frame (DS3/E3)

Alarm IDs: 83, 859

Probable cause

This alarm is raised against DS3 when the local network element detects that the DS3 payload from the STS-1/VC-3 transmitted from the shelf is not framed in the same format as the commissioned port.

This alarm is raised against E3 when the E3 facility detects an outgoing loss of framing.

According to Telcordia GR-253-CORE, a loss of frame on an async-mapped DS3 does not result in AIS insertion. An alarm is raised, and the LOF signal passes downstream.

This procedure assumes the system was operating alarm free before the Tx Loss of Frame alarm. If this alarm is raised during DS3 provisioning, verify the provisioned framing with the running test traffic.

Impact

Major, service-affecting (M, SA) alarm

ATTENTION

The payload continues to transmit to the input, but the change of framing can cause the equipment to reject the DS3 interface.

Prerequisites

To perform this procedure, you must

- have an antistatic wrist strap to dissipate electrostatic charges
- use an account with at least a level 3 UPC

Step	Action
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	Another failure in the system usually causes this alarm. Clear any other OC-3/STM-1, OC-12/STM-4, STS-1/VC-3, VT1.5/VC11, or DS3/E3 Rx alarms on the system first. Perform this procedure if the Tx LOF alarms are the only active alarms.
3	Identify the DS3/E3 interface raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document.

Procedure 5-275 (continued)

Tx Loss of Frame (DS3/E3)

Step	Action
4	Record the facility in the form: DS3-slot #-port # or E3-slot #-port #
5	Retrieve the attributes of the DS3/E3 facility you recorded. Refer to the “Retrieving equipment and facility details” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
6	Determine from the company records the location where the signal originates. If the source is a DS3/E3 interface in the system, go to step 7 . If the source is not a DS3/E3 interface, go to step 13 .
7	Retrieve the attributes of the DS3/E3 interfaces you identified. Refer to the “Retrieving equipment and facility details” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
8	Compare the frame (FMT) attributes of the two DS3/E3 interfaces. <ul style="list-style-type: none"> • If the two framing attributes are different, determine which one is correct from company records and edit the incorrect framing parameter. • If the condition does not clear, go to step 9. Refer to the “Retrieving equipment and facility details” and “Editing facility parameters” procedures in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
9	Perform a protection switch on the DS3/E3 interface you identified as the source to move traffic to protection circuit pack. Refer to the “Operating a protection switch” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
10	Wait 30 seconds. If the alarm clears, the working DS3/E3 interface is faulty. Replace the circuit pack you identified as the source. Refer to the “Replacing the 24xDS3/EC1 or 24xDS3/E3 circuit pack” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.
11	If the alarm clears, the procedure is complete.
12	If the alarm does not clear, contact your next level of support or your Ciena support group.
13	If the source is not a DS3/E3 interface, determine the original source of the DS3/E3 signal, the framing provisioned, and ensure that it is generating the correct framing by using your company procedures.
14	Perform a protection switch on the DS3/E3 interface reporting the alarm to move traffic to protection circuit pack. Refer to the “Operating a protection switch” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.

Step	Action
15	<p>Wait 30 seconds. If the alarm clears, the working DS3/E3 interface is faulty. Replace the DS3/E3 circuit pack reporting the Tx loss of frame alarm. Refer to the “Replacing the 24xDS3/EC1 or 24xDS3/E3 circuit pack” procedure in <i>Fault Management - Module Replacement</i>, 323-1851-545.</p> <p>Note: If the traffic does not automatically switch back to the original circuit pack when a failed DS3/E3 interface is replaced with a functional circuit pack (non-revertive), you can manually switch traffic back to the circuit pack.</p>
16	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-276

Tx Loss Of Signal

Alarm IDs: 633, 636, 1780

Probable cause

This alarm is raised when:

- the DS3/EC-1 circuit pack is faulty
- the DS3/EC-1 signal stops transmitting from the adjacent network element
- the DS3/EC-1 input cable is disconnected or misconnected from the I/O module
- the I/O module was removed
- the I/O module is not fully inserted and locked into position
- the Tx Actual Power on the Inline Submarine Supervisory (ISS) circuit pack is below -7 dBm. The cause can be failure of the subcomponents on the Tx path in the ISS circuit pack or the connection between the subcomponents.

Impact

Major, service-affecting (M, SA) alarm

Critical, service-affecting (C, SA) alarm

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

Prerequisites

To perform this procedure, you must

- use an account with at least a level 2 UPC
- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545
- have an antistatic wrist strap to dissipate electrostatic charges

Step	Action
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 circuit pack raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document.

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 circuit pack raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document.

Procedure 5-276 (continued)

Tx Loss Of Signal

Step	Action	Then go to
3	If the alarm is raised against the ISS C-Band circuit pack	step 9
	otherwise	step 4
4	Ensure the corresponding I/O module is fully inserted and locked into position.	
5	Use an DS3/EC-1 test set to determine if a valid DS3/EC-1 signal is on the cross-connect for that facility.	
	<ul style="list-style-type: none"> • If there is a LOS, the problem is in the DS3/EC-1 source and the shelf is reporting a valid condition. Perform troubleshooting on the source system according to your company procedures. The procedure is complete. • If there are no such conditions, go to step 6. 	
6	If the alarm does not clear, inspect the DS3/EC-1 cabling and physical connections. The connection may be loose or damaged. Repair any damage.	
7	Operate a manual switch on the DS3/EC-1 circuit pack raising the alarm. Refer to the “Operating a protection switch” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.	
8	Wait 30 seconds. If the alarm clears, the DS3/EC-1 circuit pack that raised the alarm is faulty. Replace the circuit pack that is detecting LOS. Refer to the “Replacing the 24xDS3/EC1 or 24xDS3/E3 circuit pack” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545. Go to step 12 .	
9	Verify the facility Tx power level.	
10	Connect an optical power meter to port 1 (Tx Monitor) and measure the Tx monitor power.	
11	If the measured power showing similar power level as Tx Actual Power, then the circuit pack is faulty. Replace the faulty circuit pack. Refer to the “Replacing an optical circuit pack” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.	
	Note: When the ISS C-Band circuit pack is replaced, all traffic will be lost until optical connections to the replacement circuit pack have been completed.	
12	If the alarm does not clear, contact your next level of support or your Ciena support group.	

—end—

Procedure 5-277

Tx Manual Provisioning Required

Alarm IDs: 669, 1007, 1177, 1435, 1673, 1675

Probable cause

This alarm is raised when a port on the circuit pack requires manual provisioning of the wavelength.

Impact

Major, service-affecting (M, SA) alarm, an active circuit pack in 1+1/MSP linear, 1+1 port TPT, or 1+1 TPT configuration or unprotected with cross-connects provisioned

Minor, non-service-affecting (m, NSA) alarm, an inactive circuit pack in 1+1/ MSP linear, 1+1 port TPT, or 1+1 TPT configuration or no cross-connects provisioned

Prerequisites

To perform this procedure, you must

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0
- use an account with at least a level 3 UPC

Step	Action
1	Provision the wavelength on the OC192/STM64, ETH10G, PTP, OTM2 or OTM3, or OTM4 facility. Refer to the “Editing facility parameters” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
2	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-278

Tx Partial Loss of Capacity - LCAS

Alarm ID: 925

Probable cause

This alarm is raised against an LCAS-enabled WAN facility of an L2SS, 20G L2SS, PDH gateway, or SuperMux circuit pack. The alarm is raised when at least one (but not all) Tx LCAS group member is in a failed state and unable to transmit data, resulting in a partial loss of capacity in the transmit direction. For example, when some near-end VCAT group Tx members are removed from the WAN, or some of the VCAT Rx members in the far-end network element are alarmed (LOS, LOF, AIS, LOP, LOM, OOM).

This alarm is not applicable when only one Tx LCAS group member added.

ATTENTION

If the Rx Total Loss of Capacity - LCAS alarm raised, then the Tx Total Loss of Capacity - LCAS and Tx Partial Loss of Capacity - LCAS alarms cannot be raised. The LCAS-enabled WAN cannot receive the LCAS protocol from the far-end network element since there are no active Rx members. Therefore, no Tx LCAS alarms can be raised at the same time. This is characteristic of the LCAS standard.

Impact

Minor, non-service-affecting (m, NSA) alarm, protected
Minor, service-affecting (m, SA) alarm, unprotected

Prerequisites

To perform this procedure, you require an account with at least a level 3 UPC.

Step	Action	
1	Identify the circuit pack raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document.	
2	Look for any other alarms in the active alarm list that are against the WAN facility. Use the appropriate alarm clearing procedure to clear the alarm.	
3	Verify that the number of VCAT members provisioned at the near-end and far-end network elements match.	
4	If the number of VCAT members	Then go to
	match	step 6
	do not match	step 5

Procedure 5-278 (continued)
Tx Partial Loss of Capacity - LCAS

Step	Action
5	Correct the mismatch by adding/restoring or removing VCAT members to the near or far-end WAN facility as required. Restore any incorrectly removed members at the near-end. Refer to the “Removing or restoring a VCAT member (LCAS-enabled) of a VCG” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
6	If the original alarm has
	cleared
	not cleared
	Then
	the procedure is complete
	go to step 7
7	Look for any alarms raised against the WAN facility of the far-end network element. Use the appropriate alarm clearing procedure in this document to clear the alarm.
8	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-279

Tx Power In Reduced State

Alarm IDs: 1858, 1869

Probable cause

This event is raised against the line facility of a WLAI, 100G WL3 OCLD, Flex2 WL3/WL3e OCLD, 100G WL3n MOTR, 100G WL3e OTR, 100G WL3n OTR, Flex2 WL3e OCLD, Flex3 WL3e OCLD, Flex4 WL3e OCLD circuit pack when Tx Power Reduction is applied on that facility.

This event can also be raised at both ends of 100G transponders when you delete a connection using the Sub-Network Connections application (edit to OOS) in Coherent Select and Flexible Grid Networks.

Note: This event is not masked when the OTM facility or the equipment is placed OOS-MA.

Impact

Warning

Prerequisites

To perform this procedure, you must:

- observe all safety requirements described in “Observing product and personnel safety guidelines” chapter in Part 1 of *Installation - General Information*, 323-1851-201.0
- have the fiber connection information (that is, how the optical modules on each network element connect to other network elements)
- if required, obtain a replacement circuit pack
- use an account with at least a level 3 UPC

Step	Action
1	<p>Note: If the event is raised when provisioning the wavelength/frequency and power for a line facility with an adjacency pointing to a Mux/Demux port that has no associated wavelength cross-connection, then no action is required. The alarm clears once the Mux/Demux port has an associated wavelength cross-connection.</p>
2	<p>Identify the facility raising the event. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document.</p> <p>Release the Tx Power Reduction on the facility identified in step 1.</p>

Note: If the event is raised when provisioning the wavelength/frequency and power for a line facility with an adjacency pointing to a Mux/Demux port that has no associated wavelength cross-connection, then no action is required. The alarm clears once the Mux/Demux port has an associated wavelength cross-connection.

- 1 Identify the facility raising the event. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document.
- 2 Release the Tx Power Reduction on the facility identified in step 1.

Procedure 5-279 (continued)

Tx Power In Reduced State

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

—end—

Procedure 5-280

Tx Power Out of Range

Alarm IDs: 1779

Probable cause

This alarm is raised on the Inline Submarine Supervisory (ISS C-Band) circuit pack when the Tx Actual Power is outside the minimum and maximum output optical power range. This can be caused by failure of the subcomponents on the Tx path of the ISS C-Band circuit pack or the connections between these subcomponents.

Impact

Major, service-affecting (M, SA) alarm, unprotected

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

Prerequisites

To perform this procedure, you must:

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545
- have an antistatic wrist strap to dissipate electrostatic charges
- have the optical fiber connection information (that is, how the optical modules on each network element connect to other network elements)
- have an optical power meter with the same optical connectors as the network element

Step	Action
1	Identify the circuit pack and facility raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document.
2	Check the corresponding upstream circuit pack and photonic layer for failures or alarms. Troubleshoot these alarms/failures before proceeding.

- 1 Identify the circuit pack and facility raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document.
- 2 Check the corresponding upstream circuit pack and photonic layer for failures or alarms. Troubleshoot these alarms/failures before proceeding.

Procedure 5-280 (continued)

Tx Power Out of Range

Step	Action
3	In the Site Manager Configuration menu, select the Equipment & Facility Provisioning application. Select the alarmed facility and retrieve the value from the Tx Actual Power (dBm) column of the facility table. Refer to the “Retrieving optical power, wavelength, and dispersion ranges” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
4	Click on the Ranges button to compare the Tx Actual Power (dBm) value with the Tx minimum power (dBm) and Tx maximum power (dBm) values displayed.
5	If the Tx Actual Power is a value Then go to
	within the Tx minimum power to Tx maximum power range step 6
	outside the minimum power to Tx maximum power range step 9
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	Use the optical power meter to measure the optical power level at the last upstream monitored point, and verify that the loss from source of the signal is an expected value.
	If the value of the loss is Then
	unexpected troubleshoot the fiber or Photonic layer equipment. Go to step 8 .
	expected go to step 9
8	If the original alarm has Then
	cleared the procedure is complete
	not cleared step 9
9	Use the optical power meter to measure the optical power level into the Tx interface.
	If the optical power is Then go to
	less than the Tx minimum value in step 4 step 10
	greater than the Tx maximum value in step 4 step 11
	within the Tx minimum power to Tx maximum power range step 12

Procedure 5-280 (continued)

Tx Power Out of Range

Step	Action				
10	Check the fiber and fiber cleanliness between the subtending equipment and the port reporting the alarm. Go to step 11 .				
11	The signal may require padding or an incorrect subtending circuit pack type. Contact your next level of support or your Ciena support group if you require more information.				
12	If the original alarm has Then <table> <tr> <td>cleared</td> <td>the procedure is complete</td> </tr> <tr> <td>not cleared</td> <td>restart the circuit pack reporting the alarm. Refer to the “Restarting a circuit pack or shelf processor” procedure in Part 1 of this document.</td> </tr> </table>	cleared	the procedure is complete	not cleared	restart the circuit pack reporting the alarm. Refer to the “Restarting a circuit pack or shelf processor” procedure in Part 1 of this document.
cleared	the procedure is complete				
not cleared	restart the circuit pack reporting the alarm. Refer to the “Restarting a circuit pack or shelf processor” procedure in Part 1 of this document.				
13	If the original alarm has Then <table> <tr> <td>cleared</td> <td>the procedure is complete</td> </tr> <tr> <td>not cleared</td> <td>reseat the circuit pack reporting the alarm. Refer to the “Reseating a circuit pack” procedure in <i>Fault Management - Module Replacement</i>, 323-1851-545.</td> </tr> </table>	cleared	the procedure is complete	not cleared	reseat the circuit pack reporting the alarm. Refer to the “Reseating a circuit pack” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.
cleared	the procedure is complete				
not cleared	reseat the circuit pack reporting the alarm. Refer to the “Reseating a circuit pack” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.				
14	If the original alarm has Then <table> <tr> <td>cleared</td> <td>the procedure is complete</td> </tr> <tr> <td>not cleared</td> <td>replace the circuit pack. Refer to the “Replacing an optical interface circuit pack” procedure in <i>Fault Management - Module Replacement</i>, 323-1851-545.</td> </tr> </table>	cleared	the procedure is complete	not cleared	replace the circuit pack. Refer to the “Replacing an optical interface circuit pack” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.
cleared	the procedure is complete				
not cleared	replace the circuit pack. Refer to the “Replacing an optical interface circuit pack” procedure in <i>Fault Management - Module Replacement</i> , 323-1851-545.				
15	If the alarm does not clear, contact your next level of support or your Ciena support group.				

—end—

Procedure 5-281

Tx Remote Alarm Indication

Alarm IDs: 640, 682

Probable cause

This alarm is raised when the remote network element detects a defective DS1 or DS3 signal (for example, LOS, LOF, or AIS) from the 6500 network element and returns a Remote Alarm Indication signal in the DS1, E1, or DS3 overhead.

This alarm is applicable to the DSM DS1, 24xDS3/EC-1, 24xDS3/E3, or 48 Channel Trans Mux circuit pack.

For the 24xDS3/E3 circuit pack, this alarm is raised on the DS3 facility if the DS3 frame format is provisioned other than unframed.

For the 48 Channel Trans Mux circuit pack, this alarm is raised against the DS1 and E1 facilities.

Impact

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

Prerequisites

To perform this procedure, you must

- use an account with at least a level 2 UPC
- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545
- have an antistatic wrist strap to dissipate electrostatic charges
- have a test set

Step	Action
1	Identify the DSM DS1, 24xDS3/EC-1, 24xDS3/E3, or 48 Channel Trans Mux circuit pack raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document.
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	Use a test set to determine if a valid signal is on the cross-connect for that facility.

- | | |
| --- | --- |
| 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 | Use a test set to determine if a valid signal is on the cross-connect for that facility. |

Step	Action
4	If there is no valid signal, the problem is in the source and the shelf is reporting a valid condition (for Remote Alarm Indication alarm, there is a valid signal on the transmit side and there is Remote Alarm Indication on the receive side). Perform troubleshooting on the source system according to your company procedures.
5	If there is a valid signal, operate a protection switch on the circuit pack you identified. Refer to the “Operating a protection switch” procedure in Part 2 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
6	Wait 30 seconds. If the alarm clears, the working circuit pack is faulty. Replace the circuit pack that is detecting the alarm. Refer to the “Replacing the 24xDS3/EC1 or 24xDS3/E3 circuit pack”, “Replacing the DSM 84xDS1 TM circuit pack”, or “Replacing 48 Channel Trans Mux (Portless) circuit pack” procedures in <i>Fault Management - Module Replacement</i> , 323-1851-545, for instructions.
	Note: If traffic does not automatically switch back to the original circuit pack when a failed DSM DS1, 24xDS3/EC-1, 24xDS3/E3, or 48 Channel Trans Mux circuit pack is replaced with a functional circuit pack (non-revertive), you can manually switch traffic back to the circuit pack.
7	If the alarm does not clear, inspect the cabling and connections. The cabling may be loose or damaged. Repair any damage. If the alarm does not clear, replace the DSM DS1, 24xDS3/EC-1, 24xDS3/E3, or 48 Channel Trans Mux interface carrying this facility. Refer to the “Replacing the 24xDS3/EC1 or 24xDS3/E3 circuit pack”, “Replacing the DSM 84xDS1 TM circuit pack”, or “Replacing 48 Channel Trans Mux (Portless) circuit pack” procedures in <i>Fault Management - Module Replacement</i> , 323-1851-545, for instructions.
8	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-282

Tx Remote Defect Indication

Alarm ID: 934

Probable cause

This alarm is raised against an E1 facility when the remote network element detects a defective E1 signal (for example, LOS, LOF, LOM, or AIS) from the 6500 network element, and returns a Remote Defect Indication (RDI) signal in the E1 overhead.

This alarm is only applicable to the 48 Channel Trans Mux circuit pack.

Impact

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

Step	Action
1	Identify the Trans Mux circuit pack raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document.
2	Use the cable connection information to identify the transmit and receive sites of the alarmed signal.
3	If the network element is not connected to a 6500 network element at the far-end, or if the network element is part of a mid-span meet and the far-end network element is from another vendor, use the alarm system of the other vendor to find the problem.
4	Log into the remote network element at the transmit end. If you cannot log in remotely from the local network element, you must travel to the remote site.
5	Retrieve all alarms from the transmit end.
6	Look for an alarm message at the transmit-end circuit pack connected to the original shelf.

Step	Action
7	If there are no alarms at the transmit end
	Then ensure that the equipment and facility of the remote circuit pack are in-service. Refer to the “Retrieving equipment and facility details” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310. Go to step 8 .
	additional alarms at the transmit end refer to the appropriate alarm clearing procedures. The Tx Remote Defect Indication alarm may be expected if the local alarm is AIS, Loss Of Signal, Loss of Frame, Loss of Multiframe.
8	At the local network element, retrieve all alarms to determine if the original alarm has cleared.
	If the original alarm has cleared
	Then the procedure is complete
	not cleared go to step 9
9	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
10	Verify the cable connection for the interface circuit pack that connects to the original shelf. Repair, clean, and reconnect the cable as required.
11	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-283

Tx Total Loss of Capacity - LCAS

Alarm ID: 926

Probable cause

This alarm is raised against an LCAS-enabled WAN facility of an L2SS, 20G L2SS, PDH gateway, or SuperMux circuit pack. The alarm is raised when all Tx LCAS group members are in a failed state and unable to receive data, resulting in total loss of capacity in the transmit direction. For example, when all near-end VCAT group Tx members are removed from the WAN, or all the VCAT Rx members in the far-end network element are alarmed (LOS, LOF, AIS, LOP, LOM, OOM).

ATTENTION

If the Rx Total Loss of Capacity - LCAS alarm raised, then the Tx Total Loss of Capacity - LCAS and Tx Partial Loss of Capacity - LCAS alarms cannot be raised. The LCAS-enabled WAN cannot receive the LCAS protocol from the far-end network element since there are no active Rx members. Therefore, no Tx LCAS alarms can be raised at the same time. This is characteristic of the LCAS standard.

Impact

Minor, non-service-affecting (m, NSA) alarm, protected
Major, service-affecting (M, SA) alarm, unprotected

Prerequisites

To perform this procedure, you require an account with at least a level 3 UPC.

Step	Action
1	Identify the circuit pack raising the alarm. Refer to the “Identifying the circuit pack, pluggable module/port, or facility that has raised an alarm” procedure in Part 1 of this document.
2	Look for any other alarms in the active alarm list that are against the WAN facility. Use the appropriate alarm clearing procedure to clear the alarm.
3	Verify that the number of VCAT members provisioned at the near-end and far-end network elements match.
4	If the number of VCAT members
	match
	do not match
	Then go to
	step 6
	step 5

5-614 Alarm clearing procedures—I to Z

Procedure 5-283 (continued)

Tx Total Loss of Capacity - LCAS

—end—

Procedure 5-284 TX Tuning in Progress

Alarm IDs: 663, 1008, 1178, 1436, 1515, 1672, 1674

Probable cause

This alarm is raised when Tx wavelength tuning is in progress on a port of a circuit pack.

For Submarine Line Idler 10 Channel (SLIC10 or SLIC10 Flex C-Band) circuit packs, this alarm is raised when Tx wavelength tuning is in progress for one or more lasers in the Idler facility.

Impact

Major, service-affecting (M, SA) alarm, an active circuit pack in 1+1/MSP linear, 1+1 port TPT, or 1+1 TPT configuration or unprotected with cross-connects provisioned

Minor, non-service-affecting (m, NSA) alarm, an inactive circuit pack in 1+1/ MSP linear, 1+1 port TPT, or 1+1 TPT configuration or no cross-connects provisioned

Step	Action
------	--------

- 1 No action is required. This alarm clears when Tx wavelength tuning is completed successfully.
- 2 If the alarm does not clear, is unexpected, contact your next level of support or your Ciena support group.

—end—

Procedure 5-285

Unable to Synchronize TOD

Alarm ID: 336

Probable cause

This alarm is raised when the following occurs:

- at least one time of day server is provisioned, and none of the provisioned time of day servers are reachable or valid
- at least one time of day server is provisioned and there is a problem with external communications from the shelf. The network element is unable to communicate with the provisioned time of day server.
- at least one time of day server is provisioned and there was a restart, upgrade, or momentary problem with external communications from the shelf, and the TOD polling has not yet taken place to re-synchronize the NE with the TOD server

ATTENTION

This alarm displays in the Additional Information column the specific TOD server the alarm is raised against. The Additional Information field is only available for SP-2.

This alarm is raised for an IPv4 and/or IPv6 provisioned server. IPv6 must be enabled if an IPv6 server is provisioned and IPv4 must be enabled if an IPv4 server is provisioned.

Impact

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

Prerequisites

To perform this procedure, you require an account with at least a level 3 UPC.

Step	Action
1	Select Node Information from the Configuration menu. Select the Time of Day tab in the Node Information application. Refer to the “Displaying node information” procedure in <i>Administration and Security</i> , 323-1851-301.
2	Ensure that the IP address for all provisioned time of day servers is correct. You can provision up to five time of day servers. Also ensure that the Settings Status is ON with the expected Polling Interval. Refer to the “Editing time of day synchronization parameters” procedure in <i>Administration and Security</i> , 323-1851-301.

Procedure 5-285 (continued)

Unable to Synchronize TOD

Step	Action	
3	If the original alarm has cleared	Then the procedure is complete
	not cleared	Then go to step 4
4	Check if external comms are available to the shelf by trying to ping the shelf. If comms are not available, they must be restored before the network element can communicate with the TOD server. For more information refer to the “Using the ping command” procedure in <i>Administration and Security</i> , 323-1851-301.	
5	If the alarm is still active, check if the TOD server itself is unavailable by trying to ping the TOD server. If the TOD server is available and comms are working, verify if the SNTP server has been adjusted or was temporarily unavailable recently due to a restart, upgrade, or a momentary problem with external communications from the shelf.	
6	If the SNTP server	Then go to
	has been adjusted or momentary unavailable recently	step 7
	has not been adjusted or momentary unavailable recently	step 8
7	Either wait for the polling interval to occur, or operate a time of day synchronization. Refer to the “Operating a time of day synchronization” procedure in <i>Administration and Security</i> , 323-1851-301.	
8	If the alarm does not clear, contact your next level of support or your Ciena support group.	

—end—

Procedure 5-286

Unassigned Channel Detected

Alarm ID: 1864

Probable cause

This alarm is raised against the OBMD 1x8 Mux port when a signal is detected and no cross-connect is provisioned.

This alarm is raised against ADJ-TX facilities of an OBMD 1x8 module in a WaveLogic Photonics Coherent Select network when unexpectedly high input power (that is, greater than OPTMON LOS Threshold + 3 db) is measured on an unused Tx port. An unused Tx port in this context is defined as one with no cross-connection provisioned on it.

Due to the broadcast nature of the Coherent Select hardware, such unexpected input power is not blocked and propagates throughout the Coherent Select network, potentially trampling an existing channel using the same wavelength.

To clear this alarm, fibering must be verified between the alarmed port on the OBMD 1x8 module and the transponder, or the input power must be dropped below the OPTMON LOS Threshold.

Impact

Major, service-affecting (M, SA) alarm

Prerequisites

To perform this procedure, you require an account with at least a level 3 UPC.

Step	Action
1	Verify the fibering between the alarmed port on the OBMD 1x8 module and the transponder. Confirm the expected transponder is connected to the expected/provisioned OBMD 1x8 port.
2	If the ADJ-TX is connected to an SPLI-enabled WL3 transponder which supports Tx Power Reduction, verify that the transponder connected to the alarmed port on the OBMD 1x8 module is not assigned to carry traffic yet. If this is the case, the Tx Power Reduction must be enabled on that transponder by setting its OTM4 or PTP facility OOS, then set the Tx Power Reduced State to On in Site Manager Equipment & Facility Provisioning. Refer to the “Editing facility parameters” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.

Procedure 5-286 (continued)
Unassigned Channel Detected

Step	Action
3	If the transponder is not SPLI-enabled or does not support Tx Power Reduction (such as foreign wavelength), verify that the transponder connected to the alarmed port on the OBMD 1x8 module is not assigned to carry traffic yet. If it is assigned to carry traffic, the laser must be manually turned off (for example, by placing the transponder facility OOS).
4	If the alarm does not clear or is unexpected, contact your next level of support or your Ciena support group.

—end—

Procedure 5-287 Unequipped

Alarm IDs: 13, 49, 57, 115, 126, 190, 239, 276, 461, 467, 2085

Probable cause

This alarm is raised when:

- there is an improper connection or a facility at the far-end network element is out-of-service. For example, no cross-connect is provisioned at the far-end.
- the optical facility pair at the local network element is provisioned for 1+1 /MSP linear protection, but the optical facilities at the far-end network element are not provisioned for 1+1/MSP linear protection. The local network element provisioned for 1+1/MSP linear protection will raise Unequipped alarms for all paths/connections on the protection (even) slot.
- For the (2+8)OC-n/STM-n 20G circuit packs, when the incoming label is 0x00 (unequipped), the “Unequipped” alarm is raised.

ATTENTION

While provisioning, the likelihood of Unequipped alarms being raised is high. If the alarm is raised during provisioning, allow two to three minutes for the condition to clear prior to troubleshooting the alarm.

This procedure assumes that provisioning is not taking place, the system has been running without STS/HO, VC VT/LO or VC unequipped errors, and that all fail LEDs are cleared.

Impact

Major, service-affecting (M, SA) alarm, if on an active path or if STS1s are VT managed

Minor, non-service-affecting (m, NSA) alarm, if on an inactive path in a UPSR/ SNCP configuration

Critical, service-affecting (C, SA) alarm

ATTENTION

The payload is not available to be demapped and the STS/HO or VC VT/LO path is unprotected, so the system cannot determine if path protection will be successful. Path protection occurs where the path terminates. If the protection path is available, the path-terminating network element switches to that path to protect traffic.

Procedure 5-287 (continued)

Unequipped

Prerequisites

To perform this procedure, you must

- observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0 or *Fault Management - Module Replacement*, 323-1851-545
 - use an account with at least a level 3 UPC
 - have the optical fiber/cable connection information (that is, how the circuit packs on each network element connect to other network elements and how each OC-3 connects to the DSM)

Procedure 5-287 (continued)

Unequipped

Step	Action
8	Verify that the far-end facilities of the connection are in-service. Refer to the “Retrieving equipment and facility details” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310. If the far-end facilities of the connection are out-of-service, change the facility primary state to in-service. Refer to the “Editing facility parameters” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
9	Verify cross-connects for the entire path to ensure an end-to-end connection exists. If an end-to-end connection does not exist, provision the necessary cross-connects to make a complete end-to-end connection. Refer to the “Provisioning a bidirectional connection in a 1+1/MSP linear configuration” procedure in Part 1 of <i>Configuration - Bandwidth and Data Services</i> , 323-1851-320.
10	If the optical facilities on the local network element are provisioned for 1+1/MSP linear protection, check that the associated facilities at the far-end are provisioned for 1+1/MSP linear protection.
11	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-288 Unpaired SSH Key

Alarm ID: 936

Probable cause

This alarm is raised against the shelf when the SSH keys are invalid. That is, the public and private keys are unpaired.

Impact

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

Prerequisites

To perform this procedure, you require an account with at least a level 3 UPC.

Step	Action	Then go to
1	If you want to create a new valid key pair use a specific public/private key pair	step 2 step 3
2	Regenerate a new public/private key pair. Refer to the “Regenerating SSH/SFTP keys” procedure in <i>Administration and Security</i> , 323-1851-301. If the alarm does not clear, go to step 4 .	
3	Enter the desired public/private key pair.	
4	If the alarm does not clear, contact your next level of support or your Ciena support group.	

—end—

Procedure 5-289 Unsupported Channel Provisioned

Alarm ID: 1944

Probable cause

This alarm is raised when a channel is provisioned and the channel is not supported by one or more equipment present in the network path the channel traverses.

After the add/drop connections are provisioned in the network, NCT tries to build the channel. If the channel is not supported by some equipment in the path, it marks the channel as unsupported and raises the alarm.

Impact

Warning

Prerequisites

To perform this procedure, you require an account with at least a level 3 UPC.

Step	Action
1	Find out which channel is not supported in network. De-provision the unsupported channel. Note: The channel can be provisioned successfully only if the equipment that is not capable of supporting the channel is replaced by the one that can support it.
2	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-290

Validation Certificate About to Expire

Alarm ID: 2040

Probable cause

This alarm is raised when a validation certificate in the SP2/SPAP2 is about to expire based on a provisioned number of days before the certificate expiry.

The CA (Certificate Authority) issues a validation certificate with a given expiry date. If the time of day on the SP2/SPAP2 passes the provisioned number of days before the certificate expiry date, this alarm is raised. The default number of days is 60 days and is provisionable from 0 to 180 days.

Impact

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

Prerequisites

To perform this procedure, you require an account with at least a level 3 UPC.

Step	Action
1	Connect to Network Element using Site Manager.
2	Select Manage keys from Security menu, and click on TLS Validation Certificate .
3	To clear the alarm perform one of the following:
	a. Upload a new certificate.
	b. Delete the certificate.
4	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-291

Validation Certificate Expired

Alarm ID: 2039

Probable cause

This alarm is raised when a validation certificate in the SP2/SPAP2 is expired.

The CA (Certificate Authority) issues a validation certificate with a given expiry date. If the time of day on the SP2/SPAP2 passes the certificate expiry date, this alarm is raised.

Impact

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

Prerequisites

To perform this procedure, you require an account with at least a level 3 UPC.

Step	Action
1	Connect to Network Element using Site Manager.
2	Select Manage keys from Security menu, and click on TLS Validation Certificate .
3	To clear the alarm perform one of the following: a. Upload a new certificate. b. Delete the certificate.
4	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-292

VOA Output LOS

Alarm ID: 1626

Probable cause

This alarm is raised when the total output optical power after the VOA has fallen below the provisioned output threshold value.

The alarm can be raised between the erbium-doped fiber amplifier (EDFA), and the VOA due to a hardware failure that could cause the power at the output of the EDFA to be very low.

When the alarm correlation is on, this alarm can be masked by the “Shutoff Threshold Crossed” alarm or the “Input Loss Of Signal” alarm.

Impact

Major-service-affecting (M, SA) alarm

Prerequisites

Before you perform this procedure, you must

- ensure you have all the documentation referenced in this procedure
- use an account with level 3 or higher user privilege code (UPC)

Step	Action
1	Ensure the alarm correlation is off.
2	If the “Shutoff Threshold Crossed” or the “Input Loss Of Signal” alarms are active, clear the alarms by improving input power into the amplifier.
3	Increase the power that goes through the VOA by reducing the VOA attenuation or increasing the amplifier gain. Refer to the “Editing facility parameters” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.
4	If the alarm does not clear, contact your next level of support or your Ciena support group.

-
- | | |
|---|--|
| 1 | Ensure the alarm correlation is off. |
| 2 | If the “Shutoff Threshold Crossed” or the “Input Loss Of Signal” alarms are active, clear the alarms by improving input power into the amplifier. |
| 3 | Increase the power that goes through the VOA by reducing the VOA attenuation or increasing the amplifier gain. Refer to the “Editing facility parameters” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310. |
| 4 | If the alarm does not clear, contact your next level of support or your Ciena support group. |

—end—

Procedure 5-293

VT-STS bandwidth near limit

Alarm ID: 1065

Probable cause

The 240G+/80G cross-connect circuit pack supports up to 1536 VT-STS channels. A new VT-STS channel is required when the following provisioning actions are being taken:

- provisioning a new VT connection that does not share common STS endpoints of existing VT connections
- provisioning a LO-VC3 connection on a PDH card
- initial provisioning of an equipment (for example, E1) protection group on the NE. Subsequent provisioning of equipment protection groups does not require additional VT-STS channels.

This alarm is raised against the shelf to indicate that VT bandwidth is nearly exhausted when 90% (1382 VT-STS1 channels) of the available 1536 VT-STS1 channels have been used on the 240G+/80G cross-connect circuit pack.

This alarm is masked by the “[Low Order Bandwidth Near Limit](#)” alarm.

Impact

Warning

Prerequisites

To perform this procedure, you must have an account with at least a level 3 UPC.

Procedure 5-293 (continued)
VT-STS bandwidth near limit

Step	Action
1	<p>Retrieve the number of available VT-STS connections using the Count Path Connections application. Determine if you are on the verge of exhausting the VT-STS bandwidth, in which case this alarm is cause for concern. If you have just exceeded the 90% threshold, you may want to ignore or mask this alarm.</p> <p>Refer to the “Retrieving path connections counts” procedure in Part 1 of <i>Configuration - Bandwidth and Data Services</i>, 323-1851-320.</p>
2	Delete any VT-STS channels that are not required. Refer to the “Deleting path connections” procedure in Part 1 of <i>Configuration - Bandwidth and Data Services</i> , 323-1851-320.
3	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-294

Warm Restart Required

Alarm ID: 1426

Probable cause

This alarm is raised during MRO reconfiguration, if a card under reconfiguration has transparent DCC provisioned on one of its ports (“mated” to a port on another card on the shelf), and the reconfiguration involves a port number change (for example, line rate reconfiguration of an OC48 facility to a OC192 facility on a 20G MRO, or circuit pack reconfiguration of a 2xOC48 to a 10G 16xOCn MRO). In this case, any “DCC mate” cards of the card being reconfigured need to be warm restarted to appropriately handle the change to “their” own Slot-Based Files (SBFs).

If the DCC mate card is not restarted, then any transparent DCC link between the cards will not recover after the reconfiguration, staying permanently in a DISCONNECTED state.

This alarm can be raised against any card type which supports DCC link provisioning.

This alarm is also raised when OSRP is provisioned with type L0 Provisioning [PROV] and the shelf IP address has changed.

Impact

Minor, non-service-affecting (m, NSA) alarm
Major, service-affecting (M, SA) alarm

Prerequisites

To perform this procedure, you require an account with at least a level 3 UPC.

Step	Action
------	--------

- 1 Perform a warm restart on the circuit pack that is raising the alarm. Refer to the “Restarting a circuit pack or shelf processor” procedure in Part 1 of this document.
- 2 If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 5-295

Wavelength Measurement Error

Alarm ID: 879

Probable cause

This alarm is raised against an OPTMON facility when the channel has been detected to have drifted by more than 25 GHz from its start of monitoring reference point.

Impact

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

Step	Action
1	No action is required. This alarm clears when Tx wavelength tuning is completed successfully.
2	If the alarm does not clear, perform a warm restart on the circuit pack that is raising the alarm. Refer to the “Restarting a circuit pack or shelf processor” procedure in Part 1 of this document.
3	If the alarm does not clear after the circuit pack warm restart, warm restart the SP. Refer to the “Restarting a circuit pack or shelf processor” procedure in Part 1 of this document.
4	If the alarm does not clear, is unexpected, contact your next level of support or your Ciena support group.

—end—

Procedure 5-296

Wavelength Measurement Warning

Alarm ID: 878

Probable cause

This alarm is raised against an OPTMON facility when the channel has been detected to have drifted by more than 20 GHz from its start of monitoring reference point.

This alarm can also be raised during an upgrade. If the alarm is raised during an upgrade, there is no need to back out the upgrade. Contact your next level of support or your Ciena support group.

Impact.

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

Step	Action
------	--------

- 1 No action is required. This alarm clears when Tx wavelength tuning is completed successfully.
- 2 If the alarm does not clear, perform a warm restart on the circuit pack that is raising the alarm. Refer to the “Restarting a circuit pack or shelf processor” procedure in Part 1 of this document.
- 3 If the alarm does not clear after the circuit pack warm restart, warm restart the SP. Refer to the “Restarting a circuit pack or shelf processor” procedure in Part 1 of this document.
- 4 If the alarm does not clear, is unexpected, contact your next level of support or your Ciena support group.

—end—

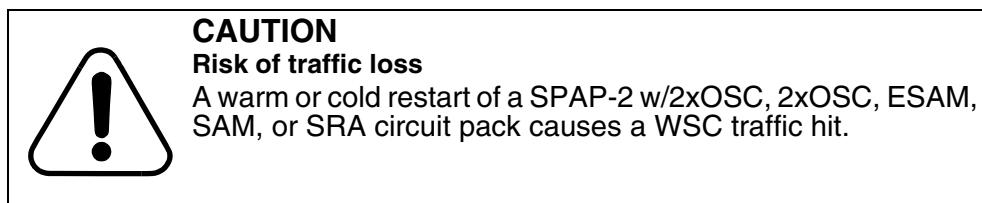
Procedure 5-297 **WAYSIDE 1/2 Port Failure**

Alarm IDs: 573, 574

Probable cause

This alarm is raised against a wayside channel (WSC) port facility of a SPAP-2 w/2xOSC, 2xOSC, ESAM, SAM, or SRA circuit pack when the wayside port cannot connect to another wayside port or when the port is provisioned and enabled, but the link is down.

Wayside traffic enters the system through one wayside port and exits the system through another wayside port.



Impact

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

Prerequisites

To perform this procedure, you must:

- use an account with at least a level 3 UPC
 - observe all the safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information*, 323-1851-201.0
 - have an antistatic wrist strap to dissipate electrostatic charges
 - have DCN information for the network

Step	Action						
1	<p>Check the DCN information to determine if the wayside port should be enabled.</p> <p>If the WSC facility should be</p> <table><tr><td data-bbox="528 1548 576 1554">disabled</td><td data-bbox="953 1548 1098 1554">Then go to</td></tr><tr><td data-bbox="528 1564 576 1571">enabled</td><td data-bbox="953 1564 1098 1571">step 2</td></tr><tr><td data-bbox="528 1581 576 1588"></td><td data-bbox="953 1581 1098 1588">step 3</td></tr></table>	disabled	Then go to	enabled	step 2		step 3
disabled	Then go to						
enabled	step 2						
	step 3						

Step	Action	
2	Delete the alarmed WSC facility from the Comms Setting Management Site Manager application (Interfaces tab, Interface type =LAN). Refer to the “Deleting an entry in the communications settings” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310.	
	ATTENTION By deleting the WSC facility, you lose any established connections that use this port.	
	The procedure is complete.	
3	Verify that the wayside configuration at both ends of the Ethernet link match. Correct any WSC LAN parameter mismatches from the Comms Setting Management Site Manager application (Interfaces tab, Interface type =LAN). Refer to the “Editing the communications settings” procedure in Part 1 of <i>Configuration - Provisioning and Operating</i> , 323-1851-310. For further details on wayside interface, refer to the “Wayside channel (WSC) interface” section in Part 4 of the 6500 <i>Planning</i> , NTRN10EG.	
4	If the original alarm has	Then
	cleared	the procedure is complete
	not cleared	go to step 5
5	Ensure both ends of the wayside cable are connected and the ports are enabled on both devices.	
6	If the original alarm has	Then
	cleared	the procedure is complete
	not cleared	go to step 7
7	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.	
8	The cable connected to the wayside port may be defective. Replace the cable.	
9	If the alarm does not clear, contact your next level of support or your Ciena support group.	

—end—

6500 Packet-Optical Platform

Fault Management - Alarm Clearing, Part 2 of 2

Copyright© 2010-2018 Ciena® Corporation. All rights reserved.

Release 13.0

Publication: 323-1851-543

Document status: Standard

Issue 1

Document release date: September 2018

CONTACT CIENA

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

