6500 Packet-Optical Platform

Fault Management - Alarm Clearing for T-Series, Part 1 of 2

Release 12.0

What's inside...

See Part 2 for the following...

323-1851-544 - Standard Issue 1
January 2017

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.

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-CIENA24 (243-6224) 410-865-4961	
In Europe, Middle East, and Africa	800-CIENA-24-7 (800-2436-2247) +44-207-012-5508	
In Asia-Pacific	800-CIENA-24-7 (800-2436-2247) +81-3-6367-3989 +91-124-4340-600	
In Caribbean and Latin America	800-CIENA-24-7 (800-2436-2247) 410-865-4944 (USA)	
Sales and General Information	410-694-5700	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	+91-124-434-0500	E-mail: sales@ciena.com
In Latin America	011-5255-1719-0220 (Mexico City)	E-mail: sales@ciena.com
Training	877-CIENA-TD (243-6283) or 410-865-8996	E-mail: techtng@ciena.com

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

IMPORTANT: PLEASE READ THIS LICENSE AGREEMENT (“AGREEMENT”) CAREFULLY BEFORE INSTALLING OR USING CIENA CORPORATION (“Ciena”) SOFTWARE, HARDWARE OR DOCUMENTATION (COLLECTIVELY, THE “EQUIPMENT”).

BY INSTALLING OR USING THE EQUIPMENT, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT AND AGREE TO BE BOUND BY ITS TERMS AND CONDITIONS.

1. Right to Use License; Restrictions. Subject to these terms, and the payment of all applicable license fees, Ciena grants to you, as end user, a non-exclusive license to use the Ciena software (the “Software”) in object code form solely in connection with, and as embedded within, the Equipment,. You shall have the right to use the Software solely for your own internal use and benefit. You may make one copy of the Software and documentation solely for backup and archival purpose, however you must reproduce and affix all copyright and other proprietary rights notices that appear in or on the original. You may not, without Ciena's prior written consent, (i) sublicense, assign, sell, rent, lend, lease, transfer or otherwise distribute the Software; (ii) grant any rights in the Software or documentation not expressly authorized herein; (iii) modify the Software nor provide any third person the means to do the same; (iv) create derivative works, translate, disassemble, recompile, reverse engineer or attempt to obtain the source code of the Software in any way; or (v) alter, destroy, or otherwise remove any proprietary notices or labels on or embedded within the Software or documentation. You acknowledge that this license is subject to Section 365 of the U.S. Bankruptcy Code and requires Ciena's consent to any assignment related to a bankruptcy proceeding. Sole title to the Software and documentation, to any derivative works, and to any associated patents and copyrights, remains with Ciena or its licensors. Ciena reserves to itself and its licensors all rights in the Software and documentation not expressly granted to you. You shall preserve intact any notice of copyright, trademark, logo, legend or other notice of ownership from any original or copies of the Software or documentation.

2. Audit: Upon Ciena's reasonable request, but not more frequently than annually without reasonable cause, you shall permit Ciena to audit the use of the Software at such times as may be mutually agreed upon to ensure compliance with this Agreement.

3. Confidentiality. You agree that you will receive confidential or proprietary information (“Confidential Information”) in connection with the purchase, deployment and use of the Equipment. You will not disclose Confidential Information to any third party without prior written consent of Ciena, will use it only for purposes for which it was disclosed, use your best efforts to prevent and protect the contents of the Software from unauthorized disclosure or use, and must treat it with the same degree of care as you do your own similar information, but with no less than reasonable care. You acknowledge that the design and structure of the Software constitute trade secrets and/or copyrighted materials of Ciena and agree that the Equipment is Confidential Information for purposes of this Agreement.

4. 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 Equipment and any accompanying technical data (collectively “Materials”) are commercial within the meaning of applicable Federal acquisition regulations. These Materials were developed fully at private expense. U.S. Government use of the Materials is restricted by this Agreement, and all other U.S. Government use is prohibited. In accordance with FAR 12.212 and DFAR Supplement 227.7202, software delivered to you is commercial computer software and the use of that software is further restricted by this Agreement.

5. Term of License. This license is effective until terminated. Customer may terminate this license at any time by giving written notice to Ciena [or] and destroying or erasing all copies of Software including any documentation. Ciena may terminate this Agreement and your license to the Software immediately by giving you written notice of termination in the event that either (i) you breach any term or condition of this Agreement or (ii) you are wound up other than voluntarily for the purposes of amalgamation or reorganization, have a receiver appointed or enter into liquidation or bankruptcy or analogous process in your home country. Termination shall be without prejudice to any other rights or remedies Ciena may have. In the event of any termination you will have no right to keep or use the Software or any copy of the Software for any purpose and you shall destroy and erase all copies of such Software in its possession or control, and forward written certification to Ciena that all such copies of Software have been destroyed or erased.

6. Compliance with laws. You agree to comply with all applicable laws, including all import regulations, and to obtain all required licenses and permits related to installation and use of Equipment. Software, including technical data, is subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Customer agrees to comply strictly with all such regulations and acknowledges that it has the responsibility to obtain licenses to export, re-export, or import Software.

7. Limitation of Liability. ANY LIABILITY OF Ciena SHALL BE LIMITED IN THE AGGREGATE TO THE AMOUNTS PAID BY YOU 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 THIRD-PARTY SUPPLIER OF Ciena. NEITHER Ciena NOR ANY OF ITS THIRD-PARTY SUPPLIERS 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

8. General. Ciena may assign this Agreement to any Ciena affiliate or to a purchaser of the intellectual property rights in the Software, but otherwise neither this Agreement nor any rights hereunder may be assigned nor duties delegated by either party, and any attempt to do so will be void. This Agreement shall be governed by the laws of the State of Maryland (without regard to the conflict of laws provisions) and shall be enforceable in the courts of Maryland. The U.N. Convention on Contracts for the International Sale of Goods shall not apply hereto. This Agreement constitutes the complete and exclusive statement of 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

This Technical Publication supports 6500 Packet-Optical Platform (6500) Release 12.0 software and subsequent maintenance releases for Release 12.0.

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. Part 2 continues sequential chapter numbering from Part 1. 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.

You are reading Part 1 of *Fault Management - Alarm Clearing, for T-Series*, 323-1851-544. The following section details what’s new in *Fault Management - Alarm Clearing for T-Series, Part 1 of 2*, 323-1851-544, Standard Issue 1 for Release 12.0.

Issue 1

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

- Shelf type and related modules
  - Control and timing module (CTM)
  - Control and timing extender module (CTMX)
- Photonics hardware
  - Multi-function Carrier (MFC)
  - OTDR4 Pluggable Module
  - 8-Degree 4-Channel Colorless Mux/Demux
  - Fiber Interconnect Module Type 1

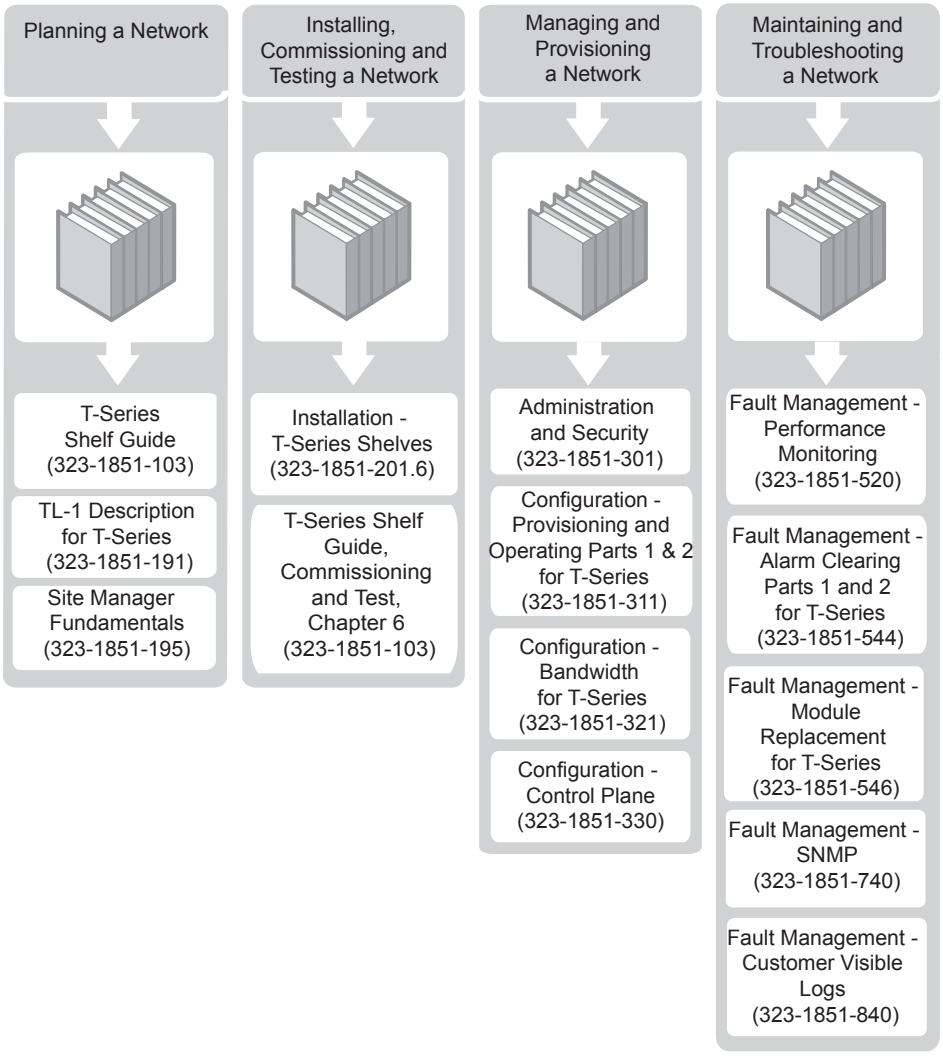
- Packet/OTN hardware
  - 5x100G WL3n CFP2-ACO PKT/OTN I/F
  - 5x100G/12x40G QSFP28/QSFP+ PKT/OTN I/F
  - 40x10G SFP+ PKT/OTN I/F

  Note: Contact Ciena for information on using Packet functionality on the 6500 T-12 or T-24 shelf.

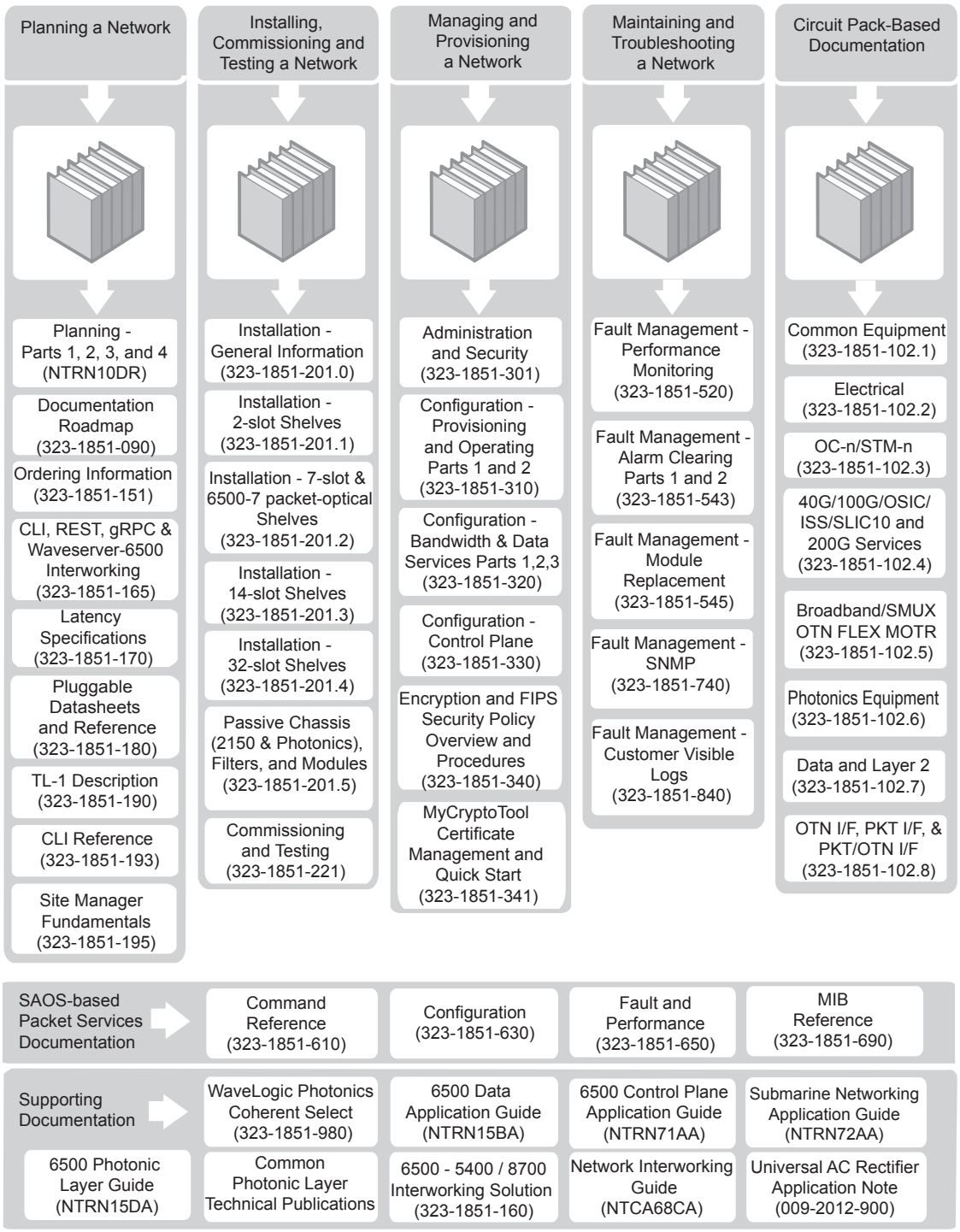
6500 technical publications

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 12.0.

6500 T-Series roadmap



6500 D-Series and S-Series roadmap



Alarm and trouble clearing strategy

This release of 6500 Packet-Optical Platform (6500) supports PKT/OTN switch modules and Photonic services for different modules. The combination of two or all services is also supported.

For more information on the services (and the modules related to each service), refer to the *6500 - T_Series Shelves- Guide*, 323-1851-103.

Site level alarm correlation

The site level alarm correlation feature reduces the number of alarms reported at each site to a minimum. It does not reduce the number of sites in a network reporting alarms. This is performed by the Network level alarm correlation feature. Once Alarm Correlation is enabled, it automatically enables both Site level and Network level alarm correlation. One cannot exist without the other.

The feature requires the system to have full knowledge of topology and connectivity within the network, including channel routing at OADM sites. The physical topology of the network is represented by adjacency objects. The shelf level correlation uses these adjacency objects to notify downstream facilities that an upstream failure has occurred and suppresses alarms on modules within the same site. The service photonic layer interoperability module is responsible for messaging and auditing the fault information which spans shelves within the site.

Alarm correlation requires that physical adjacency information be provisioned between Photonic equipment at a site. For systems controlled by the Domain Optical Controller (DOC), no extra information is required from a user perspective as this adjacency information already exists in order to build the channel topology information (to automatically add/delete photonic channels). In order for alarm correlation to work all the way down to the service layer (that is, service modules connected to the photonic equipment), physical adjacency information must be provisioned. The Physical Adjacency information between the service layer equipment and the CMD is provided by the SPLI feature. If the discovered far-end address is nil then that channel is not considered when calculating the “all in-use channels failed” condition.

At least two channels must be in-use before the “backwards” alarm correlation is initiated.

The Alarm Correlation parameter within the Site Manager Node Information application and the System tab must be set to On for the “backwards” alarm correlation to function.

Backwards alarm correlation only functions if all service modules connected to the CCMD 8x4, or CCMD16x12, support alarm correlation.

Site level alarm correlation is supported on the CCMD 8x4, and CCMD16x12, configurations provided that all of the following conditions apply:

- Alarm correlation is set to On in the Site Manager Node Information application and the System tab.
- All adjacencies are manually provisioned.
- All cascading equipment (CCMD 8x4, CCMD16x12) are provisioned in the same shelf.
- Service modules used in the configuration must support alarm correlation.
- SPLI based Alarm Correlation is supported on the PTP, ODUTTP and the OTUTTP facilities for PKT/OTN, modules.

When alarm correlation is enabled, the PTP, ODUTTP, and OTUTTP alarms are masked. The masked alarms can be viewed in Site Manager 'Active Disabled Alarms' window.

The following alarms are masked downstream when Alarm Correlation is on and when an upstream channel, port level or service layer fault occurs:

- Loss Of Signal
- Loss of Clock
- Loss Of Frame
- Loss Of Multiframe
- ODU BDI (masked by an special algorithm when alarm correlation is on, and not by upstream faults)
- OTU BDI (masked by an special algorithm when alarm correlation is on, and not by upstream faults)
- OTU Trace Identifier Mismatch
- ODU Signal Fail
- ODU Trace Identifier Mismatch
- OPU Payload Type Mismatch
- Pre-FEC Signal Fail

- OPU AIS
- ODU AIS
- ODU LCK
- ODU OCI
- MSI Mismatch
- Far End Client Signal Fail
- Loss Of Channel

The following faults trigger downstream masking when Alarm Correlation is on. These are port level issues, where all channels are affected, which will continue to propagate the downstream masking in the Demux direction:

- Loss Of Signal
- Loss of Clock
- Loss Of Frame
- Loss of Channel
- Loss Of Multiframe
- ODU AIS
- ODU LCK
- ODU OCI
- Pre-FEC Signal Fail
- ODU Signal Fail
- Circuit Pack Failed
- Circuit Pack Missing
- Circuit Pack Mismatch
- Circuit Pack Mismatch – Pluggable
- Circuit Pack Missing – Pluggable
- Circuit Pack Failed – Pluggable

For the list of supported module combinations refer to the *6500 - T_Series Shelves- Guide*, 323-1851-103.

The alarm correlation functionality can be enabled/disabled on a per shelf basis by editing the Alarm correlation parameter using the Site Manager Node Information application and the System tab. Refer to the “Editing the nodal system parameters” procedure in *Administration and Security*, 323-1851-301 for more information.

Network level alarm correlation

Network level alarm correlation (NLC) builds on the Site Level Alarm Correlation feature. Site Level Alarm Correlation masks alarms within a site based on a detected fault. However, Site Level Alarm Correlation does not share fault information with neighboring nodes in the network. It also does not track per-channel failures when channels are muxed and mixed together with non-failed channels.

Essentially, NLC will perform site level alarm correlation but it will also perform network level alarm correlation. Network Level Alarm Correlation addresses the gaps of the SLC feature based on wavelength topology. Network Level Alarm Correlation expands adjacency discovery (AD) messaging to support OTS to OTS (intra-node and inter-node) Network Level Alarm Correlation messaging. NLC shares and collects channel status information with neighbors. With knowledge of the channel statuses, NLC performs alarm correlation and masks alarms.

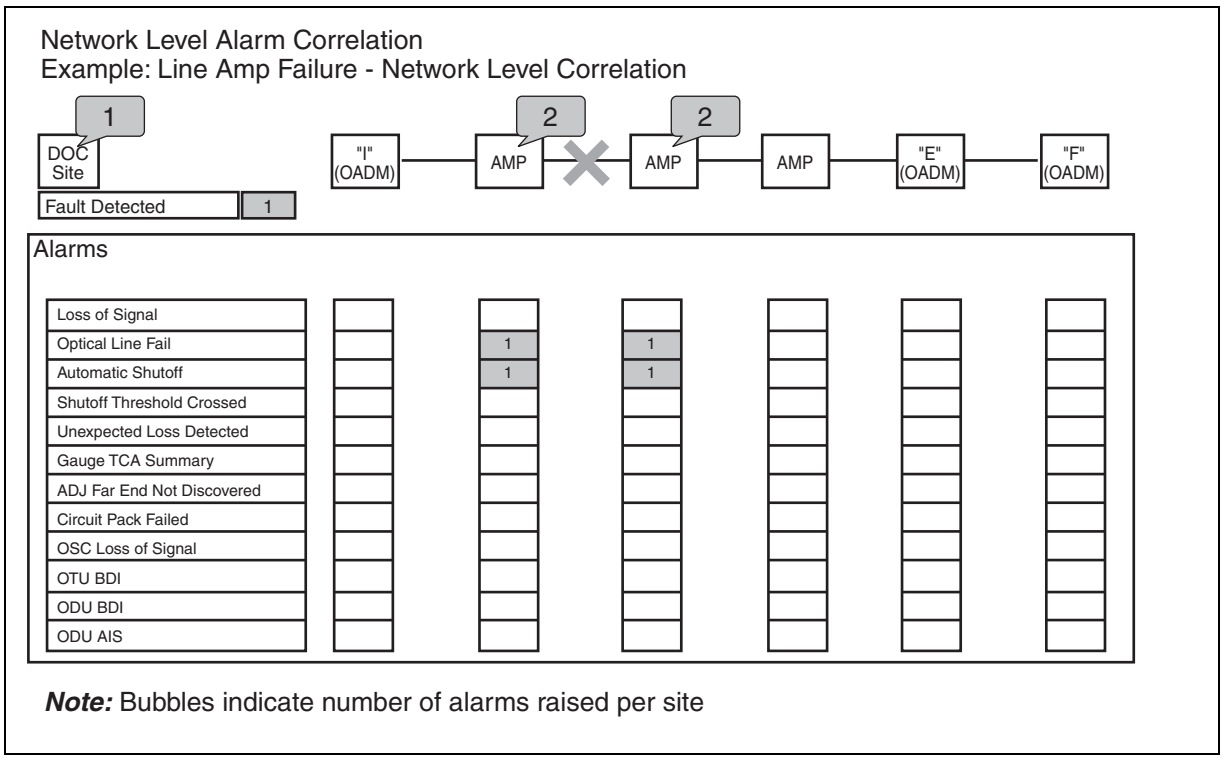
Network Level Alarm Correlation:

- Suppresses symptomatic (downstream and lower level) alarms
- Suppresses “Hard” faults if all channels on that port are failed (Hard faults are the faults that affect all channels on a port; for example, LOS, AIS, Shutoff Crossed)
- Suppresses “Soft” faults if any channel on that port is failed (Soft faults are the faults that affect only some channels or partial power loss; for example, PM TCAs, Unexpected Loss)
- Suppresses alarms in the network within one minute of the failure

When the photonic network is single-channel, the NLC may be unable to distinguish between a hard fault and a soft fault since there is only one channel within the line port. In these situations, manual isolation of the fault may be required to determine where the root cause of the failure is within the photonic network.

Figure 1-1 on page 1-5 shows an example of Network Level Alarm Correlation.

Figure 1-1
Network level alarm correlation



Provisionable severity for alarms and events

Two types of events are supported:

- Standing Conditions (SC), for which a raised and a clear Autonomous Output (AO) are generated
- Transient Conditions (TC), for which a raised AO is generated but not a clear

Site Manager supports Critical, Major, Minor, and Warning severity types for alarms. If a Warning severity is selected for a given alarm, the alarm will be raised by the network element as an SC. The Warning severity can be applied to all alarms independently of their default severity (Critical, Major, or Minor). By default, the Warning severity of Standing Conditions is also provisionable in the Alarms Profile application to any of Critical, Major or Minor.

By default each alarm has two severities assigned to it, a Service Affecting (SA) and a Non-Service Affecting (NSA) severity, both of which are generally provisionable in the Alarms Profile application. Environmental alarm severities can be provisioned by changing the attributes of the specific environmental alarm. Some alarms on the 6500 support only one severity, which could be either SA or NSA. In the Alarms Profile application, Site Manager displays a "-" for a non-provisionable severity and disables the capability to edit the field. If for any of the SA or NSA severities a Warning is selected, the alarm would be raised as a Standing Condition (SC) for the selected severity.

The severity of an alarm is indicated by the following designations: Critical (C), Major (M) or minor (m). A warning (w) is used for Standing Conditions. It is important to note that the impact of a SC, SA or NSA, is not reported by the network element, hence the Active Alarms application in Site Manager would report the SC as a "w" and displays a "-" in the Service column.

The capability to provision the severity does not apply to Transient Conditions, non provisionable alarms, or output external alarms.

Alarm clearing strategy

The 6500 hardware and software performs automatic fault detection and identification. When a network element detects a fault, it issues autonomous alarms, activates office alarms, and displays alarms through LEDs.

In addition to raising alarms on a shelf, 6500 also supports the generation of northbound simple network management protocol (SNMP) traps for network element alarms and events. Refer to the *"*Editing and deleting SNMP trap destinations" procedure in *Fault Management - SNMP*, 323-1851-740.

The alarm clearing strategy is based on several assumptions:

- No external problem causes the alarm, such as power fluctuation.
- Primary fault generates primary and secondary alarms that you can clear with a single fault clearing procedure.
- The network element is provisioned correctly, and works until the time of the alarm.
- If protection circuitry exists, traffic is switched before performing the alarm clearing.

The network elements report alarms in the following ways:

- alarm LEDs on the network element and modules
- lamps and audible alarms on the
  - — access panel in a 6500 T-Series shelf
- northbound SNMP trap reporting for the NE-level alarms
- network element alarm messages retrieved locally through Site Manager or TL1
- office alarms (optional)

The following steps make up the strategy for fault and alarm clearing:

- Detect there is a fault.
- Identify the network element that raised the alarm.
- Check for illuminated Fail LEDs on the modules.
- If a Fail LED is illuminated, perform the procedure to replace a failed module, pluggable module, or pluggable transceiver.
- If the Fail LED is not illuminated, retrieve alarm messages through Site Manager.
- Identify the local and remote alarms during the procedure.
- Identify the alarm severity.
- Identify which network element to clear.
- Perform trouble-clearing procedures.
- Determine if there are additional alarms.
- If alarms continue to be active, begin the process again.
- If the alarms are cleared, end the process.

For more information on the steps, see Figure 1-2, “Fault clearing strategy” on page 1-9.

Alarm priority

Critical alarms have the highest priority and are reported before Major, minor or Warning alarms. Major alarms are reported before minor alarms and minor alarms are reported before warnings. Clear alarms in order of severity:

- Critical, service-affecting (C, SA) alarm
- Major, service-affecting (M, SA) alarm
- Major, non-service-affecting (M, NSA) alarm
- failed module non-service-affecting (NSA) alarm
- minor, service-affecting (m, SA) alarm
- minor, non-service-affecting (m, NSA) alarm

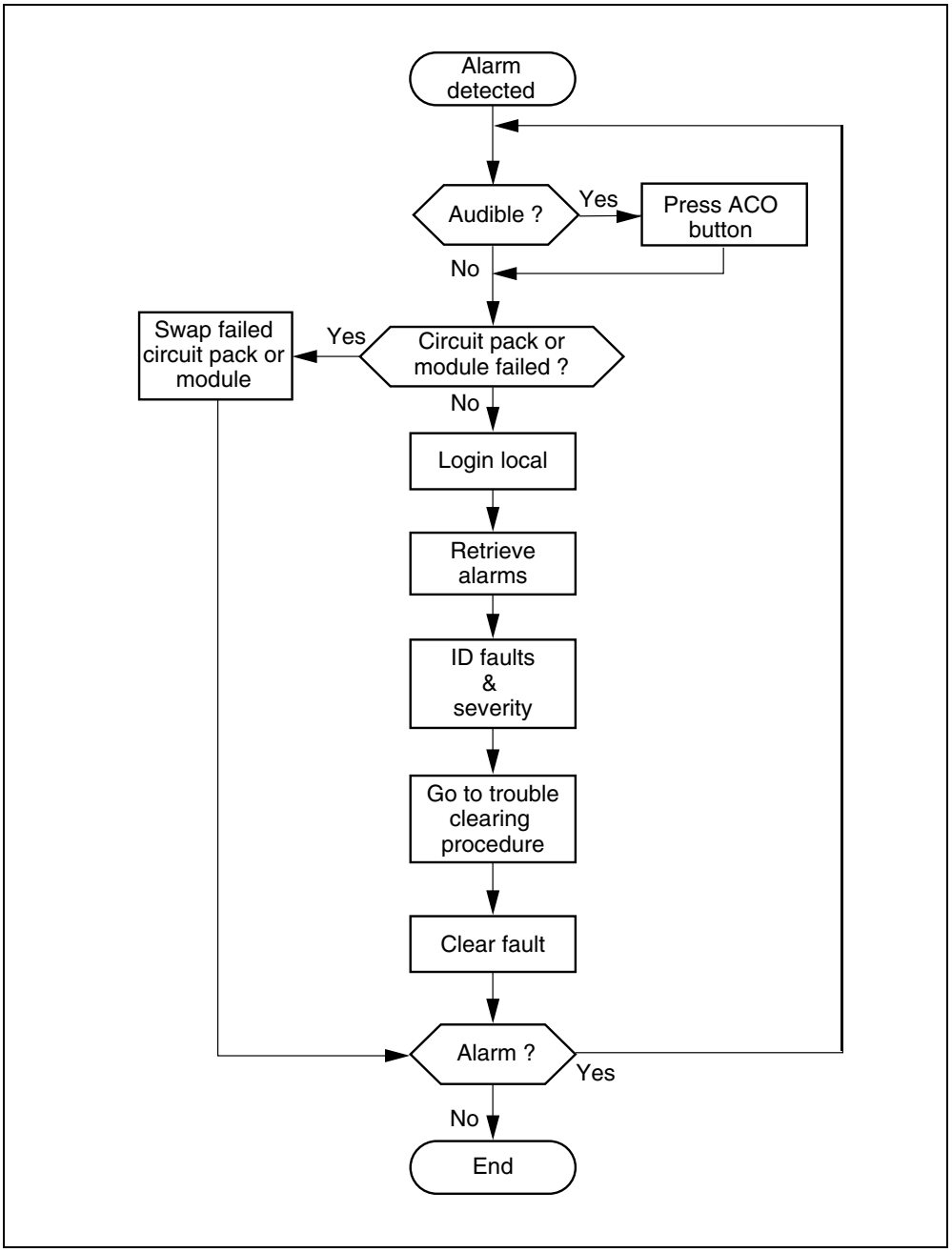
One fault can cause more than one alarm. Clearing the alarm with the highest severity can clear other alarms.

You can change the alarm severity of both high and low entities using the **Alarms Profile** application in Site Manager. Refer to Procedure 2-8, "Editing an alarm profile" in Chapter 2, "Alarm surveillance".

The alarm notification codes (service affecting, SA, or non-service affecting, NSA) are unaffected by change of alarm severity. The alarm severities in the ALL ENABLED, ALL DISABLED, and FACTORY DEFAULT alarm profiles cannot be changed.

Refer to the "Service-affecting and non-service-affecting severities" on page 3-2 for further details on alarm severities.

Figure 1-2
Fault clearing strategy



LED indications

The 6500 uses an LED indication scheme, where:

- red indicates failure (requires replacement)
- green indicates active (powered and operational)
- yellow indicates warning (something missing or activity in progress)
- blue indicates do not unseat (removing the module will impact service)

Module LEDs

After a module is inserted, reseated, or a cold restart is performed, all the LEDs turn on for approximately five seconds.

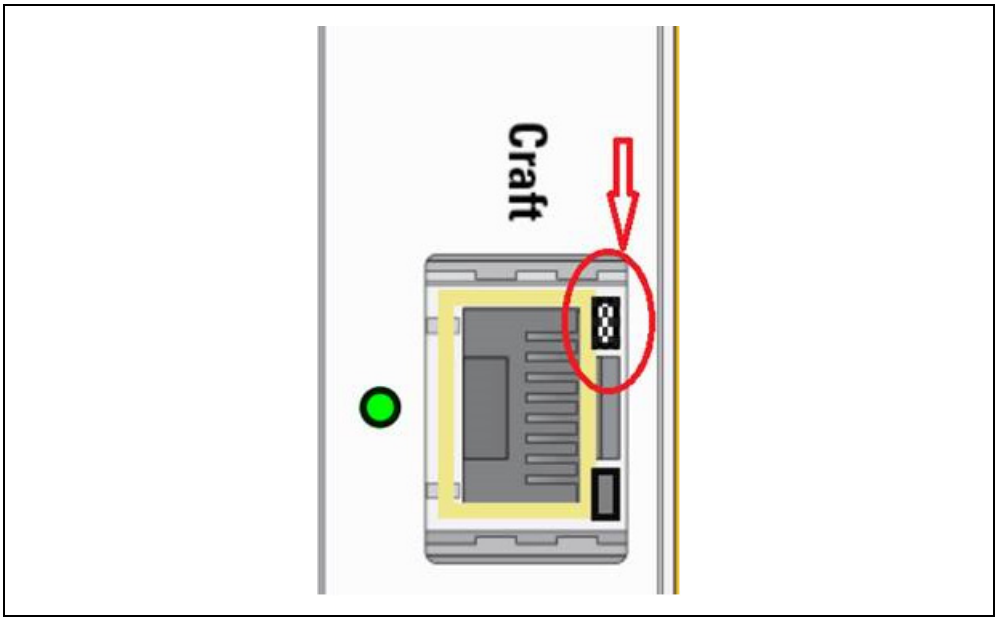
Each module contains the following status LEDs:

- triangular red Fail LED
- rectangular green Ready LED
- diamond blue In Use LED

Exceptions include the Power Input Modules (PIM), fan module, filler cards, and any equipment connected to external slots (with an RJ45 inventory cable) such as the FIM3 module.

The LED unknown status in Shelf Level View (SLV) is represented as shown in Figure 1-3.

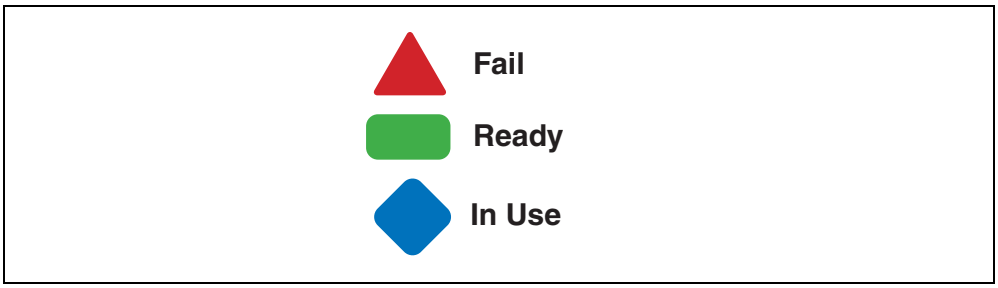
Figure 1-3
LED unknown status



Some modules and pluggable modules also contain a:

- circular green/yellow bi-color port LED
- circular green/yellow Synchronization status LED
- circular red/green/yellow tri-color port LED

Figure 1-4
Module LEDs



Red Fail LED

The triangular red Fail LED indicates a hardware or software failure state of the module or pluggable module.

The red LED turns on when an equipment failure has been isolated to that module or pluggable module and must be replaced (for example, a Circuit Pack Failed alarm is active on the module).

The red LED turns on for approximately 30 seconds when a lamp test is initiated.

The red LED flashes when a user intervention flash test is being performed.

The Red LED turns on while Green LED stays on to indicate that the module has partial failure. Partial failures are normally indicated by some module related alarms. It is recommended to verify every alarm raised against the module to identify the partial failure.

Green Ready LED

The rectangular green Ready LED indicates the module or pluggable module is powered-up and does not have a module fail condition.

The green LED turns on when the module or pluggable module initialization is completed and a module fail condition is not present.

The green LED turns off when a module fail condition is detected on the module or pluggable module.

The green LED turns on for approximately 30 seconds when a lamp test is initiated.

The green LED flashes when:

- a module is initializing
- a software auto-upgrade is being performed
- a user intervention flash test is being performed

Blue In Use LED

The diamond blue In Use LED indicates the module is in-service and powered up.

The blue LED turns on when the module is in-service and powered up.

The blue LED turns on for approximately 30 seconds when a lamp test is initiated.

The blue LED flashes when a user intervention flash test is being performed.

The blue LED turns off when the:

- module is out-of-service
- module has been inserted or cold restarted and cannot be provisioned by the CTM. This occurs for failed modules, mismatched modules, modules that are not powered up, or modules that have their database rebuilt.

CAUTION
Risk of traffic loss
Do not remove a module while the blue In Use LED is illuminated.

Green/Yellow bi-color circle LED

The green/yellow bi-color port LED is used to indicate the port status.

The green LED turns on when the facility is provisioned and the facility is not in a failed state.

The yellow LED turns on when the facility is provisioned and the facility is in a failed state.

The LED turns yellow, then green for approximately 15 seconds each when a lamp test is initiated.

The green LED flashes when a user intervention flash test is being performed.

Green/yellow/red tri-color LED

The green/yellow/red tri-color LED located beside each port is used to communicate the pluggable optical module status, as well as the port status.

The green LED turns on when the facility is provisioned, the pluggable optical module has not failed, and the facility is not in a failed state.

The yellow LED turns on when the facility is provisioned, the pluggable optical module has not failed, and the facility is in a failed state.

The red LED turns on when a pluggable transceiver is present and provisioned but the pluggable transceiver has failed.

The LED turns red, then yellow, then green for approximately 10 seconds each when a lamp test is initiated. The green LED flashes when a user intervention flash test is performed.

Some modules contain additional LEDs as detailed in the following sections.

Power Input Module (PIM)

The Power Input Modules have one or more Power OK LEDs. The green LED turns on to indicate the power feed is active and a minimum voltage is detected and flowing through to the backplane (through any breaker, fuse or power converter if applicable to the equipped PIM). In the case of a DC PIM, the feed must also be in the correct polarity for its associated Power OK LED to illuminate. In any case where the Power OK LED is not illuminated and the PIM is working correctly, an operational CTM should assert any applicable alarms such as Power Failure -A/B, Power Failure - Low Voltage or Power Failure - Fuse Blown. However, in some cases a Power OK LED may be illuminated indicating that a minimum voltage is detected on a feed but the CTM may still assert one or more of the following alarms based on the shelf's operating specification: Power Failure -A/B, Power Failure - Low Voltage or Power Failure - Fuse Blown (if applicable). See Part 2 of *Fault Management - Alarm Clearing_T-Series*, 323-1851-544 for details.

Access Panel

The Access Panel contains the following circular LEDs that indicate the alarm status of the shelf:

- The red Critical LED turns on if one or more Critical alarm exists on the shelf.
- The red Major LED turns on if one or more Major alarm exists on the shelf.
- The orange Minor LED turns on if one or more minor alarm exists on the shelf.
- The white ACO LED turns on when the ACO button is pressed and at least one Critical, Major, or Minor alarm exists on the shelf. The ACO LED turns off if:
  - no alarms exist on the shelf
  - a new Major or Critical alarm is raised

Control Timing Module (CTM)

The CTM contains the following circular LEDs:

- The yellow Ref Loss LED indicates a loss of timing reference. Two indicators are provided, one for each clock domain.
- The white unlabeled LED to the left of the Craft RJ-45 port. Indicates which CTM you should connect your PC to.

10/100/1000BT RJ45 on CTM and Access Panel

The CTM contains the following circular LEDs:

- The Green LNK LED indicates a link up condition.
- The Yellow ACT LED indicates data activity.

Control and Timing Module Extenders (CTMX)

The CTMX contains the following LEDs:

- The Green LED indicates a Ready condition
- The Blue LED indicates an In Use status
- The Red LED indicates a Failure

During a cold restart of the CTM module with or without the CTMX module in place, the LEDs go through the following sequence:

- the module LED flashes
- the Green LED flashes
- the Green LED turns solid and if the CTM module is in-service, the Blue LED turns on

If the CTMX module is present, the CTMX LEDs go through the above sequence after 30 seconds.

For more information about the LED sequence during the installation, refer to “Installing the CTMXs (Control and Timing Module Extenders) and CTMs (Control and Timing Modules) procedure in *Installation - 6500-T Series Shelves*, 323-1851-201.6.

Fan modules

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

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

For 6500-T 12 shelves, the red LED will be ON during a single power zone failure if a fan is powered by that zone. In this case, address the power feed failure first to restore the complete power to the fan.

Ethernet ports

Each Ethernet port on the CTM and access panel has two LEDs (one green and one yellow) integrated in the RJ45 connector.

- The green LED turns on when a link pulse is received.
- The yellow LED turns on when data is being received on the receive port.

The Ethernet port LEDs are not turned on during a power-up or a cold restart sequence of the CTM.

The CTMX does not include an RJ-45 craft port, USB port, or Sync LED.

Interface modules without pluggable transceivers

Modules without pluggable transceivers (for example, 2x100G WL3n PKT/OTN interface module) have a circular bi-color port LED.

If a terminal loopback is applied to the optical facility while a loss of signal condition exists, the yellow LED turns off as the loss of signal detection circuit is bypassed.

Interface modules with pluggable transceivers

Modules with pluggable transceivers (for example, 20x10G SFP+ PKT/OTN interface module) have a tri-color green/yellow/red port LED.

The red LED turns on when a pluggable is present and the pluggable has failed.

If a terminal loopback is applied to the optical facility while a loss of signal condition exists, the yellow LED turns off as the loss of signal detection circuit is bypassed.

LED sequences

During a power up (module insertion or reseat) or a restart, the red Fail, the green Ready, and the blue In Use status LEDs on the front of the module go through a sequence as detailed in the following sections.

Module insertion/reseat and cold restart LED sequence

For a module insertion/reseat or a cold restart, the red Fail, the green Ready, and the blue In Use status LEDs go through the following sequence:

- The red LED turns on momentarily.
- After a few seconds, the red, green and blue LEDs turn on.
- After a few seconds, the red and blue LEDs turn off and the green LED flashes to indicate the software is initializing.
- When software initialization is complete, the green status LED turns on (does not flash).

- If the module is in-service and powered up, the blue LED turns on after the green LED while the module is in use. If the module has failed, the green LED turns off and the red LED turns on.

During a module insertion/reseat or a cold restart, the port and Ethernet port status LEDs remain off.

When the green LED is steadily lit (after the software initialization), an auto-upgrade of the module may occur. During an auto-upgrade, the green LED remains steadily lit and the blue LED remains off (a Software Auto-Upgrade in progress alarm is raised and clears after the auto-upgrade is complete).

Warm restart sequence

For a warm restart, the red Fail, the green Ready and the blue In Use status LEDs go through the following sequence:

- The red and blue LEDs remain in the state they were before the restart.
- After a few seconds, the green LED flashes to indicate the software is initializing.
- When software initialization is complete, the green status LED turns on (does not flash).
- If the module has failed, the green LED turns off and the red LED turns on.

Lamp test

A lamp test can be initiated using the ACO/Lamp Test button found near the shelf's Critical, Major and Minor LEDs or using Site Manager.

When initiated, the lamp test is performed on all the applicable LEDs on the network element (does not apply to any power input LEDs, LEDs on shelf peripherals provisioned in virtual slots or connected to RJ45 external slot inventory interfaces, LEDs on RJ-45 ports used for Telemetry In/Out or any equipped module that is not in a ready state). A lamp test times out after approximately 30 seconds and the LEDs revert to the previous status. For bi-color port LEDs, one color is lit for first 15 seconds and the other color is lit for the remaining 15 seconds. For tri-color LEDs, each color is lit for 10 seconds.

When initiated from Site Manager, the test can be performed on all the applicable LEDs on the network element or on a single module.

ATTENTION

You cannot perform a lamp test on the LEDs on the Power Input Cards. On some access panels, the RJ45 external slot inventory interfaces appear to have two LEDs but there is only one that is used during normal operation and that will illuminate during a lamp test.

In addition, the user has the option to perform a user intervention flash test on a slot or port basis that causes the LEDs to flash, allowing a user at the site to identify a module, pluggable module, or pluggable transceiver. When initiated for a slot, the status LEDs (red Fail, green Ready, and blue In Use) on the specified module flash for 15 minutes and the status of all port LEDs remain the same. When initiated for a pluggable module in a sub-slot, the status LEDs (red Fail and green Ready) on the specified pluggable modules flash, as well as the status LEDs on the module, for 15 minutes and the status of all port LEDs remain the same. When initiated for a port, the status LEDs (red Fail, green Ready, and blue In Use) on the module, the pluggable module, and the specified port LED flash for 15 minutes (only the green color flashes for port LEDs).

Consider the following:

- Only ports which have LEDs present can be selected for a port user intervention flash test.
- A user intervention flash test cannot be performed on the LEDs on the Power Input Module, the access panel, the fan modules, or the LAN port on the CTM/CTMX.
- A user intervention flash test can be stopped by performing a non-flash lamp test or using the on/off radio buttons on Site Manager.

For information on initiating a lamp test:

- using the ACO button, refer to Procedure 2-13, “Clearing audible alarms and performing lamp tests”.
- from Site Manager, refer to the “Performing a lamp test and clearing audible alarms using the Visualization tool” procedures in *Administration and Security* 323-1851-301.

Viewing active alarms and events

Active alarms are indicated on the 6500 equipment and are visible from the Site Manager user interface. Alarm history, events, and logs are stored on the network element. Login sessions using Site Manager craft user interface, Optical Manager Element Adapter, and Optical Application Platform provide details of network element alarms.

The types of 6500 network element alarms are:

- equipment
- common equipment
- facility

Color-coded alarm severity

Color is used to highlight the severity value in the application summary tables for the following Site Manager applications:

- Consolidated Alarms
- Active Alarms
- Historical Fault Browser
- Active Disabled Alarms
- Visualization tool display of filtered active alarms

Alarm severity color codes can be configured by modifying the values of color codes defined in the “gui.properties” file, which can be found at the base directory located on the “Site Manager” installation directory on your computer.

The format of color codes in “gui.properties” should be in Hex format. The standard alarm severity color codes are shown below.

```
# Standard alarm severity colors.
COLOR_ALARM_CRITICAL=0xFF0000
COLOR_ALARM_MAJOR=0xFF0000
COLOR_ALARM_MINOR=0xFFB200
COLOR_ALARM_WARNING=0xFFCC00
COLOR_ALARM_INFO=0xE0E0E0
COLOR_ALARM_INDETERMINATE=0xFFFFFF
COLOR_ALARM_DEFAULT=0xE0E0E0
COLOR_ALARM_ALERT=0xFFCC00
```

If the above color codes are commented in “gui.properties”, the default alarm color codes are displayed.

The color coding is defined as follows in Table 1-1.

Table 1-1
Alarm severity color coding

Alarm severity		Site Manager default alarm color coding
Critical, service-affecting	(C, SA)	red
Critical, non-service-affecting	(C, NSA)	red
Major, service-affecting	(M, SA)	red
Major, non-service-affecting	(M, NSA)	red
Minor, service-affecting	(m, SA)	orange
Minor, non-service-affecting	(m, NSA)	orange
Warning	(w, -)	yellow
Note: Site Manager Alarm Colors are user configurable. When Site Manager is launched from OneControl, the OneControl Color definitions are used as defined in the Alarm Indicators and severities section of *OneControl Unified Management System Standard Operations Guide,* 450-3201-301.		

Viewing active alarms

Site Manager provides the user with a visual summary of all active alarms for all 6500 network elements logged in to, through the alarm banner. The user views a list of active alarms on a 6500 shelf by selecting the **Active Alarms** application on the **Fault** menu of Site Manager. A maximum of 4600 active alarms are supported on the 6500 network element.

The active alarm application provides the user with the ability to filter and sort alarms and perform manual or automatic refresh of the active alarm list. Alarms details are available for each active alarm in the list.

Alarm reports can be affected by the primary state of the module and facilities. For example, an alarm is not reported until the primary state of a module or facility changes from out-of-service to in-service.

Auto In Service (AINS)

AINS is the ability to setup traffic on a network without alarms prior to the end user signal being applied and error-free. This allows entities to be put in-service, but remain alarm free until a module is inserted or cables (traffic) plugged into the module.

When an equipment/facility was created with equipment/facility AINS enabled or edited to enable AINS, and the equipment or clean facility signal is missing, the equipment/facility enters the AINS state. When in the AINS state, the equipment/facility primary and secondary states indicate the equipment/facility is in an alarmed condition but alarms are suppressed for that equipment/facility.

When a valid module is inserted or a clean signal is detected for an equipment or facility in AINS, a timer starts. If the equipment or facility remains fault free for the specified AINS timeout value, the equipment or facility is automatically transitioned from the AINS state. Subsequent conditions that result in alarms will result in alarms being generated on the NE.

If a module supports equipment AINS, then any pluggable modules or pluggable transceivers supported on that module also support equipment AINS.

Two independent system-wide AINS timeout parameters are supported - one for Facility AINS, and the other for Equipment AINS, applicable to all entities supporting the AINS on the shelf. The supported AINS timeout value range is from five minutes (default) to 96 hours. The AINS timeout value can be set in increments of five minutes. Refer to “Editing the nodal system parameters” in *Administration and Security*, 323-1851-301.

When an equipment or facility is in an AINS state, suppressed alarms can be retrieved in the Active Disabled Alarms application within Site Manager.

Traffic alarms and events are suppressed for the facility with the AINS state, explicitly including the following:

- Traffic faults, near end and far end
- PM TCA reports
- WAN alarms/PMs on a LAN facility
- Alarms which require manual action to clear, such as “Loopback Active”

Protection switch alarms/events are not suppressed.

Facility alarms for received signal-affecting faults such as the following alarms, as well as others, prevent the AINS timer from counting down:

- Loss of Signal
- Loss of frame
- Loss of clock
- Loss of Data Sync
- Frequency Out Of Range

- Signal Fail
- Signal Degrade
- Loss Of MultiFrame
- Excessive Error Ratio
- Link Down
- Rx Power Out Of Range

The following equipment alarms are not AINS impacting and do not reset AINS timer:

- Circuit Pack Failed
- Cold Restart Required: FPGA Changed
- Intercard Suspected
- Internal Mgmt Comms Suspected
- High Received Span Loss
- Low Received Span Loss
- Autoprovisioning Mismatch - Pluggable
- Circuit Pack Mismatch - Pluggable
- Circuit Pack Failed - Pluggable
- Circuit Pack Unknown - Pluggable
- Intercard Suspected - Pluggable
- Provisioning Incompatible - Pluggable

PM collection is also inhibited when a facility is in an AINS state. PM counts will not be recorded/calculated for facilities and paths. Analog PMs, such as power levels which are measured, will continue to be recorded. Bins will be set to IDF when the AINS state is active. A system parameter indicates whether PMs are collected during AINS.

Viewing events

The **Historical Fault Browser** application supports the following functionality:

- viewing of historical (current and cleared) alarms for the 6500 network element
- viewing of logs
- filtering of alarms based on severity
- details for specific events (alarms or logs)

The 6500 supports three types of events.

- non-reflective event, Event Code (EC)=0

- reflective event, EC=1
- saturated or clipped reflective event, EC=2

The 6500 also supports the generation of northbound SNMP traps for network element alarms and events. For more details on supported SNMP functionality, refer to the:

- "SNMP support" section in *Fault Management - SNMP*, 323-1851-740
- external alarm provisioning, external controls in Chapter 2, "Alarm surveillance"

The 6500 network element stores up to 5500 events. 5000 of those are from alarms/events that were enabled, and the other 500 are for alarms/events that were disabled at the time they were generated. The Historical Fault Browser application provides the user with the ability to filter and sort events and perform manual refresh of the event list.

Alarm profiles

The alarm profiles application gives the user the ability to view, edit, and delete alarm profiles.

A profile contains all the alarm points applicable for the alarm class and a status, enabled or disabled, for each alarm point. A profile can be applied to an individual facility or module of that alarm class to quickly disable multiple alarm points. A default profile can be set for an alarm class so that when a new facility or module of that class is first provisioned, the default alarm profile is applied to it automatically.

The alarm profile also contains the severity (C, M, m, w) for each alarm, which can be edited by the user.

The 6500 network element provides two non-editable predefined profiles (All Enabled which is the default, and All Disabled) and allows for three more predefined profiles to be user editable on the network element.

The Common alarm class supports an additional non-editable profile, Factory Default. For the Common alarm class, the Factory Default profile enables all common alarms except for the Disk 75 percent Full, Disk 90 percent Full, and LAN Link Failure alarms, which are disabled.

> ***Note:*** On SONET and L0 control plane, active alarm profile is not applicable for OSRPNODE, OSRPLINK, OSRPLINE/ OSRPLINE0, SNC, and SNCG objects. Alarms against these objects are raised according to the default alarm profile.

The following is a list of alarms that do not appear in any alarm profile (which means these alarm points cannot be disabled):

- Automatic Shutoff Compromised
- Autoprovisioning Mismatch
- Autoprovisioning Mismatch - pluggable
- Circuit pack unknown
- Circuit pack unknown - pluggable
- Circuit Pack Upgrade Failed
- Fan Failed
- Fan Missing
- High Optical Power
- Provisioning Incompatible
- Provisioning Incompatible - pluggable
- Software Auto-Upgrade in Progress
- Slot Empty

Alarm hold-off

Alarm hold-off period is the time delay between the time that the alarm condition occurs and the time that the alarm is raised. The user can manually change the alarm hold-off from 2.5 seconds (default) to 0 seconds for alarms associated with PKT/OTN interface modules and Photonic modules. The alarm hold-off feature applies to AMP, OPTMON, and OSC facilities in Photonic modules, and all facilities on PKT/OTN interface modules.

This feature allows you to see alarms for fast transient conditions that would normally be filtered by the 2.5 second hold-off. The alarm hold-off period is changed using the **System** tab in the **Node Information** application in Site Manager. Refer to the “Editing the nodal system parameters” procedure in *Administration and Security*, 323-1851-301.

ATTENTION

When Alarm hold-off is set to 2.5, alarms which are raised and cleared within 2.5 seconds time-frame are not acknowledged.

Viewing disabled alarms

Alarms that have been disabled from the alarm profiles application, AINS, or SP alarm correlation are not displayed in the **Active Alarms** application. Active alarms that have been disabled can be viewed in the **Active Disabled Alarms** application in the **Faults** menu of Site Manager. A manual refresh is required to see the latest Active Disabled Alarms.

External alarm provisioning and controls

The 6500 network element has 16 parallel telemetry input points and four external control relays.

The input points allow remote monitoring of other equipment in the office in which the network element is located. For example, the input points can monitor room temperature alarms or office door open alarms. Specific external alarms must be set up during provisioning. The alarm types are assigned to a specific contact pin.

The **External Alarm Provisioning** application in the **Configuration** menu of Site Manager supports the following functionalities:

- displaying external alarm attributes (telemetry input points)
- editing the environmental alarm attributes on the network element
- deleting defined environmental alarm attributes on the network element

The external controls application allows the user to retrieve and display the labels and status of the four external controls relays for the 6500 network element. The 6500 network elements allow the user to operate or release these relays to turn external equipment on and off (for example, air conditioning, fan, sprinkler) and edit the labels of the relays.

Power cycling of the network element

If the network element time is not provisioned to retrieve its time of day from an NTP server and a power cycle occurs on the network element, you must reprovision the network element date and time as the date and time are reset to the default values. If the time of day (TOD) synchronization feature is enabled, you do not have to reprovision the date and time. Refer to the “Editing the nodal general parameters” procedure in *Administration and Security*, 323-1851-301.

Signal conditioning for PKT/OTN interface modules

The following signal conditioning is applied for PKT/OTN interface module triggered events.

Table 1-2
PKT/OTN interface module signal conditioning—PTP facility

Defect	Faceplate Conditioning	Fabric Conditioning	Notes
SA CP Fail	PTP_CONDTYPE	Not applicable	
Terminal Loopback	Laser off	Not applicable	Occurs when OTU TTP, ETTP or STTP is in terminal loopback
Facility Loopback	None (Laser on)	Not applicable	Occurs when OTU TTP, ETTP or STTP is in facility loopback
OOS-MA	PTP_CONDTYPE	Not applicable	
Child ODU term CTP OOS-MA	PTP_CONDTYPE	Not applicable	
No Cross Connections on child ODU term-CTP	Laser off	Not applicable	PTP service type of ETTP, STTP, etc. (non-OTU)
	None (no conditioning as to not interfere with GCC0 (OTU) and GCC 1 & 2 (ODU)	Not applicable	PTP service type of OTU
No CTP	PTP_CONDTYPE	Not applicable	No child ODU CTPs present
Loss of Signal	None	Send Faceplate Defect indication to children	
SM Intercard Fail	PTP_CONDTYPE	Not applicable	
Receive at least one Fabric Defect indication from children	PTP_CONDTYPE	Not applicable	WAN defect, Rx ODU defect on ODU term-CTP only

Table 1-3
PKT/OTN interface module signal conditioning—OTUTTP facility

Defect	Faceplate Conditioning	Fabric Conditioning	Notes
SA CP Fail	None	Not applicable	
Loopback	None	Not applicable	Clears active conditioning when a facility or terminal loopback is active
OOS-MA	None	Not applicable	
Faceplate Signal Fail	OTU BDI	Send Faceplate Defect indication to children	OTU LOS, LOF, LOC, LOM, SF, TIM, AIS
OTU IAE	OTU BIAE	Not applicable	
OTU Signal Degrade	OTU BEI	Not applicable	

Table 1-4
PKT/OTN interface module signal conditioning—ETTP facility

Defect	Faceplate Conditioning	Fabric Conditioning	Notes
SA CP Fail	ETTP_CONDTYPE	Not applicable	
Loopback	None	Not applicable	Clears any active hold timer or conditioning when a facility or terminal loopback is active
OOS-MA	ETTP_CONDTYPE	Not applicable	
Child ODU term CTP OOS-MA	ETTP_CONDTYPE	Not applicable	
SM Intercard Fail	Holdoff/ETTP_CONDTYPE	Not applicable	ETH IDLE conditioning during holdoff period
Faceplate Signal Fail	None	Send Faceplate Defect indication to children	LOS, LOC, LODS, Link Down, EER
Receive at least one Fabric Defect from children (WAN or ODU term-CTP)	Holdoff/ETTP_CONDTYPE	Not applicable	ETH IDLE conditioning during holdoff period

Table 1-5
PKT/OTN interface module signal conditioning—STTP facility

Defect	Faceplate Conditioning	Fabric Conditioning	Notes
SA CP Fail	AIS-L	Not applicable	
Loopback	None	Not applicable	Clears active conditioning when a facility or terminal loopback is active
OOS-MA	AIS-L	Not applicable	
Child ODU term CTP OOS-MA		Not applicable	
SM Intercard Fail	AIS-L	Not applicable	
Faceplate Signal Fail	AIS-L	Send Faceplate Defect indication to children	LOS, LOF, LOC, SF/B2 BER
Receive at least one Fabric Defect from children (WAN or ODU term-CTP)	AIS-L	Not applicable	

Table 1-6
PKT/OTN interface module signal conditioning—ODUTTP facility

Defect	Faceplate Conditioning	Fabric Conditioning	Notes
SA CP Fail	ODU AIS	Not applicable	
Loopback	None	Not applicable	Clears active conditioning when a facility or terminal loopback is active
OOS-MA	ODU LCK	Not applicable	
SM Intercard Fail	ODU AIS	Not applicable	
PST = USPC	None	Not applicable	Placeholder ODU TTP until ODU TTP/CTP is provisioned by end user
Receive Faceplate Defect from parents	ODU BDI	Not applicable	

Table 1-6
PKT/OTN interface module signal conditioning—ODUTTP facility (continued)

Defect	Faceplate Conditioning	Fabric Conditioning	Notes
Faceplate ODU Signal Fail	ODU BDI	Send Faceplate Defect indication to children	Rx ODU LCK, OCI, AIS, LOF, TIM
Faceplate OPU MSIM	ODU BDI	Send Faceplate Defect indication to children	Detected at Higher-Order ODU TTP
Faceplate OPU Signal Fail	None	Send Faceplate Defect indication to children	Rx OPU PTM, MSIM, CSF, AIS

Table 1-7
PKT/OTN interface module signal conditioning—WAN facility

Defect	Faceplate Conditioning	Fabric Conditioning	Notes
SA CP Fail	Not applicable	None	
OOS-MA	Not applicable	None	
Terminal Loopback	Not applicable	None	Clears active conditioning when a facility or terminal loopback is active
Facility Loopback	Not applicable	WAN_CONDTYPE	
Receive Faceplate Defect from parent	Not applicable	WAN_CONDTYPE	
Fabric FESF	Send Fabric Defect indication to parents (ETTP & PTP)	None	
Fabric CSM	Send Fabric Defect indication to parents (ETTP & PTP)	None	
Fabric LOFD	Send Fabric Defect indication to parents (ETTP & PTP)	None	

Table 1-8
PKT/OTN interface module signal conditioning—ODU monitor-CTP, ODU transparent-CTP facilities

Defect	Faceplate Conditioning	Fabric Conditioning	Notes
SA CP Fail	ODU AIS	ODU AIS	
Facility Loopback	None	ODU AIS	Faceplate traffic is looped back
Terminal Loopback	None	None	All active conditioning is cleared when a facility or terminal loopback is active
OOS-MA	ODU LCK	ODU LCK	
OPU MSIM	None	ODU AIS	Detected at Higher-Order ODU TTP
SM Intercard Fail	ODU AIS	None	
Mate Intercard Fail	None	ODU AIS	XCIF only
Receive Faceplate Defect from parent	ODU BDI	ODU AIS	
No cross-connect	ODU OCI	ODU OCI	No CRS in either direction
Fabric ODU defect	None	None	
Fabric OPU defect	None	None	ODU/OPU Defects are passed from fabric to faceplate

Table 1-9
PKT/OTN interface module signal conditioning—ODU terminated-CTP facility

Defect	Faceplate Conditioning	Fabric Conditioning	Notes
SA CP Fail	Not applicable	ODU AIS	
Facility Loopback	Not applicable	None	Faceplate traffic is looped back
Terminal Loopback	Not applicable	ODU AIS	All active conditioning is cleared when a facility or terminal loopback is active
OOS-MA	Not applicable	ODU LCK	
Mate Intercard Fail	Not applicable	ODU AIS	XCIF only

Table 1-9
PKT/OTN interface module signal conditioning—ODU terminated-CTP facility (continued)

Defect	Faceplate Conditioning	Fabric Conditioning	Notes
Receive at least one Faceplate Defect from parent	Not applicable	CTP_CONDTYPE (If CTP_CONDTYPE is 'OPUK_NONE', conditioning is ODU AIS)	
Fabric ODU Signal Fail	Send Fabric Defect indication to parents	ODU BDI	ODU LCK, OCI, AIS, LOF, TIM
Fabric OPU Signal Fail	Send Fabric Defect indication to parents	None	OPU PTM, MSIM, CSF, AIS
No cross-connect	Tell parent PTP and xTTP there are no CRSs	ODU OCI	

Table 1-10
PKT/OTN interface module signal conditioning—TCM TTP facility

Defect	Faceplate Conditioning	Fabric Conditioning	Notes
SA CP Fail	TCM AIS	Not applicable	
Loopback	None	Not applicable	All active conditioning is cleared when a facility or terminal loopback is active
OOS-MA	TCM LCK	Not applicable	
No Connection on sibling ODU	TCM OCI	Not applicable	
SM Intercard Fail	TCM AIS	Not applicable	
Receive Faceplate Defect from parents	TCM BDI	Not applicable	
Faceplate TCM defect	TCM BDI	Not applicable	TCM AIS, LCK, OCI, LTC, LOF, TIM
Faceplate TCM IAE	TCM BIAE	Not applicable	
Faceplate TCM Signal Degrade	TCM BEI	Not applicable	

Table 1-11
PKT/OTN interface module signal conditioning—TCM monitor-CTP facility

Defect	Faceplate Conditioning	Fabric Conditioning	Notes
SA CP Fail	TCM AIS	TCM AIS	
Terminal Loopback	None	None	All active conditioning is cleared when a facility or terminal loopback is active
Facility Loopback	None	TCM AIS	
OOS	TCM LCK	TCM LCK	
No Connection on sibling ODU	TCM OCI	TCM OCI	
SM Intercard Fail	TCM AIS	TCM AIS	
Mate intercard Fail	None	None	
Receive Faceplate Defect from parents	None	None	
Faceplate TCM defect	None	None	TCM AIS, LCK, OCI, LTC, LOF, TIM - all defects are passed through from faceplate to fabric
Faceplate TCM IAE	None	None	Passed through from faceplate to fabric
Fabric TCM Defect	None	None	TCM AIS, LCK, OCI, LTC, LOF, TIM - all defects are passed through from fabric to faceplate
Fabric TCM IAE	None	None	Passed through from fabric to faceplate

Table 1-12
PKT/OTN interface module signal conditioning—TCM terminal-CTP facility

Defect	Faceplate Conditioning	Fabric Conditioning	Notes
SA CP Fail	Not applicable	TCM AIS	
Terminal Loopback	Not applicable	None	All active conditioning is cleared when a facility or terminal loopback is active
Facility Loopback	Not applicable	TCM AIS	
OOS	Not applicable	TCM LCK	
No Connection on sibling ODU	Not applicable	TCM OCI	
Mate Intercard Fail	Not applicable	TCM AIS	
Receive Faceplate Defect from parents	Not applicable	TCM AIS	
Fabric TCM Defect	Not applicable	TCM BDI	TCM AIS, LCK, OCI, LTC, LOF, TIM
Fabric TCM IAE	Not applicable	TCM BIAE TCM BEI	
Fabric TCM Signal Degrade	Not applicable	TCM BIAE TCM BEI	

Automatic Power Reduction (APR) (Photonic services)

The APR feature is a controlled ramp-down and recovery mechanism used to limit potential exposure to instances of high optical power with a view of protecting personnel and preventing equipment damage on detection of high reflections, breaks, or disconnects in the optical line. It is non-provisionable, and is activated when an amplifier module is placed in service.

When the optical return loss (ORL) of an amplifier falls below the threshold, the system reduces the amplifier output power level to minimize the danger of personal eye injury. A regulatory-deemed safe level of optical power is transmitted in the period of optical discontinuity on the line to facilitate automatic detection of line restoration and recovery to normal state. It is used by lowering the optical output to a residual level suitable for making OR measurements and facilitating auto recovery when normal system connectivity resumes.

The 6500 Amplifier Module EDFA facility APR system is triggered by low return loss detected at the line out. This detection affects the EDFA immediately preceding the reflection point invoking APR on this EDFA. The low return loss condition may be due to:

- poor connection at output connector or subsequent connections in the line
- fiber break downstream

When an APR condition is triggered, an Automatic Power Reduction Active alarm is raised against any amplifier with reduced power.

Automatic Line Shut Off (ALSO) (Photonic services)

The ALSO feature is a safety laser shutdown mechanism. It is non-provisionable, and is activated when an amplifier module is placed in service or during some SLAT procedures. Amplifier power levels are turned down or turned off when a fiber break or intermediate connector disconnect occurs between two neighboring sites, where optical radiation is being fed into both ends of the optical fiber and generating a hazard on both ends of a fiber break.

When an ALSO condition is triggered, an Automatic Shutoff alarm is raised against any transmitter that was shut off.

ATTENTION
For the ALSO feature to function correctly, you must properly configure the OTS first.

Automatic Laser Shutoff (ALSO) can be disabled on the RLA interface module by setting the ALSO Disable flag to TRUE for the AMP facility.

Alarm surveillance

This chapter provides information and procedures about alarm profiles, external alarm provisioning, network alarm monitoring and events surveillance.

For a description of the 6500 alarm features, refer to Chapter 1, “Alarm and trouble clearing strategy” of this document.

Abbreviations used in this chapter

ACO	Alarm Cut-Off
CFP2	100G transceiver form factor pluggable
DCC	Data Communications Channel
BDI	Backward Defect Identifier
GCC	General Communications Channel
IPv4/6	Internet Protocol version 4/6
LAN	Local Area Network
LED	Light-emitting Diode
SFP+	Small form Factor Pluggable
SNMP	Simple Network Management Protocol
S/R	Save/Restore
SSM	Synchronization Status Messaging
TOD	Time Of Day
UPC	User Privilege Code
WAN	Wide Area Network

Alarm parameters

External control types

The external control relays support the external control types listed in Table 2-1.

Table 2-1
External control labels

External control label	External control type
Air conditioning	Air conditioning
Engine	Engine
Fan	Fan
Generator	Generator
Heat	Heater
Light	Lighting
Miscellaneous	Miscellaneous
Sprinkler	Sprinkler
(Null)	No label is associated with the specific relay. However, some external equipment can be connected to this relay.

Environmental alarm labels

Table 2-2 lists the labels and associated condition types available for the environmental alarms.

Table 2-2
Environmental alarm labels and associated condition types

Alarm label (default description)	Condition Type
48-V power supply failure (Note)	PWR-48
Air compressor failure	AIRCOMPR
Air conditioning failure	AIRCOND
Air dryer failure	AIRDRYR
Battery discharging	BATDSCHRG
Battery failure	BATTERY
Commercial power failure	POWER
Cooling fan failure	CLFAN

Table 2-2
Environmental alarm labels and associated condition types (continued)

Engine failure	ENGINE
Engine operating	ENGOPRG
Explosive gas	EXPLGS
Fire	FIRE
Fire detector failure	FIRDETR
Flood	FLOOD
Fuse failure	FUSE
Generator failure	GEN
High airflow	HIAIR
High humidity	HIHUM
High temperature	HITEMP
High water	HIWTR
Intrusion	INTRUDER
Low battery voltage	LWBATVG
Low cable pressure	LWPRES
Low fuel	LWFUEL
Low humidity	LWHUM
Low temperature	LWTEMP
Low water	LWWTR
Miscellaneous	MISC
Open door	OPENDR
Pump failure	PUMP
Rectifier failure	RECT
Rectifier high voltage	RECTHI
Rectifier low voltage	RECTLO
Smoke	SMOKE

Table 2-2
Environmental alarm labels and associated condition types (continued)

Toxic gas	TOXICGAS
Ventilation system failure	VENTN
Note: "-48 Vdc" is expressed as "48-V" in the label and default description.	

Autonomous events

Autonomous events are faults raised with a severity of "Log". Events report the activity status on the network elements, and do not always require user action. To retrieve events, refer to "Retrieving events for a network element" on page 2-15. The events listed in the **Historical Fault Browser** application include the alarms that have been raised, both cleared or not cleared, and the logged warnings and events. For more information about the logged events, refer to *Fault Management - Customer Visible Logs*, 323-1851-840.

Table 2-3 lists logged events. For a complete list of alarms that can be raised, refer to the "List of alarms" on page 4-5.

Table 2-3
Autonomous events

Event category (Note)	**Description**
Files	Remote transfer of files for '<release>' - <#> of <#> MB, <#> of <#> Files
	Release '<release>' Successfully delivered
	Remote transfer of file '<path>/<filename>' failed
	Removing files for '<release>' started
	Release '<release>' has been deleted
Upgrades	Redundant Release Synch Complete

Table 2-3
Autonomous events (continued)

Event category (Note)	Description
Load installation	Load Installation: Cancel Passed
	Load Installation: Check Failed
	Load Installation: Check Passed
	Load Installation: Commit Failed
	Load Installation: Commit Passed
	Load Installation: Committing New Release
	Load Installation: Invoke Failed
	Load Installation: Invoke Passed
	Load Installation: Load Failed
	Load Installation: Load Passed
	Load Installation: Programming Load to FLASH
	Load Installation: Running from incorrect FLASH bank
	Load Installation: Unable to Access Release Files
	Load Installation: Unable to Program Load to FLASH
Performance Monitoring	15-Min Threshold Crossing
	1-Day Threshold Crossing
	Untimed Threshold Crossing
Photonics	DOC Channel Add Completed
	DOC Channel Delete Completed
	DOC Pre-Check Fail
	DOC Pre-Check Pass
	DOC Reset TCA Baselines Failed
Protection	Protection Exerciser Complete
	Protection Switch Initiated

Table 2-3
Autonomous events (continued)

Event category (Note)	Description
Save and restore	Cancel S/R Completed
	Cancel S/R Failed
	Cancel S/R Failed: Save/Restore not in progress
	Check S/R Failed: Blocked by another application
	Check S/R Failed: Blocked by presence of alarms
	Check S/R Failed: Could not connect to destination
	Cancel SR Failed: Software Subsystem
	Check S/R Failed: FTP access denied
	Check S/R Failed: SFTP access denied
	Check S/R Failed: Invalid destination
	Check S/R Completed
	Check S/R Failed
	Check S/R: Restore Blocked by another application
	Check S/R: Save Blocked by another application
	Database Commit Failed
	Database Commit Failed: Restored backup is corrupt
	Database Commit: Restart in progress
	Database Commit Failed: Software Subsystem
	Database Restore Completed
	Database Restore Failed
	Database Restore Failed: Backup not from this node
	Database Restore Failed: Blocked by another application
	Database Restore Failed: Incompatible Shelf Assembly
	Database Restore Failed: Blocked by presence of alarms
	Database Restore Failed: Could not connect to source
	Database Restore Failed: Failure transferring file
	Database Restore Failed: FTP access denied

Table 2-3
Autonomous events (continued)

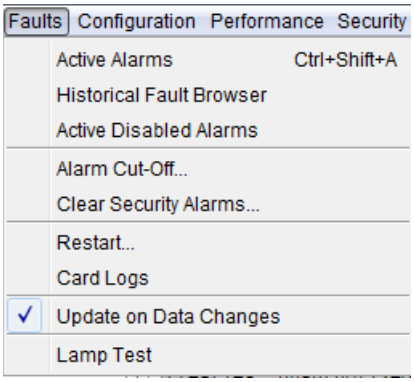
Event category (Note)	Description
Save and restore (continued)	Database Restore Failed: SFTP access denied
	Database Restore Failed: Incompatible options
	Database Restore Failed: Incompatible S/R options specified
	Database Restore Failed: Interrupted by card restart
	Database Restore Failed: Invalid source
	Database Restore Failed: Mismatched Software Releases
	Database Restore Failed: Restored backup is corrupt
	Database Restore Failed: Mismatched IXPs
	Database Restore Failed: Software Subsystem
	Database Restore Failed: Software Subsystem Unsupported
	Database Restore in progress
	Database Save Failed
	Database Restore Failed
	Database Commit Failed
	Database Save Completed
	Database Save Failed
	Database Save Failed: Blocked by another application
	Database Save Failed: Blocked by presence of alarms
	Database Save Failed: Blocked by remote application
	Database Save Failed: Could not connect to destination
	Database Save Failed: Failure transferring file
	Database Save Failed: FTP access denied
	Database Save Failed: SFTP access denied
	Database Save Failed: Interrupted by card restart
	Database Save Failed: Invalid destination
	Database Save Failed: Failure to backup data for slot

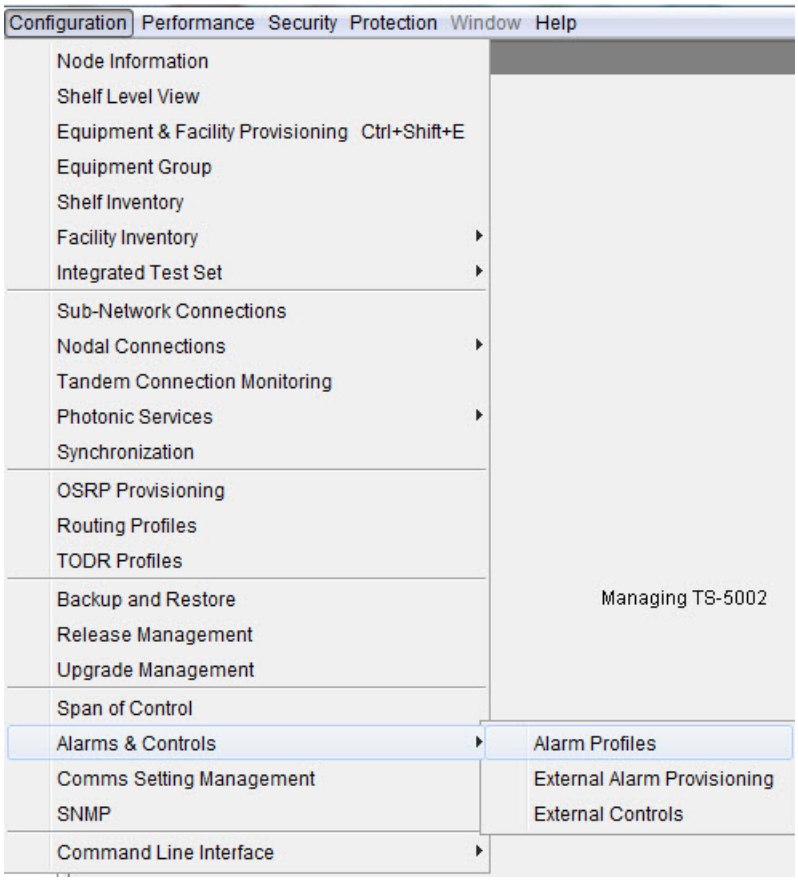
Table 2-3
Autonomous events (continued)

Event category (Note)	Description
	Database Save Failed: Software Subsystem
	Database Validate Failed
	Database Validate Failed: Restored backup is corrupt
	Redundant database synch complete
	Redundant database synch in progress
Security	Password has expired. Contact your Admin.
	Password has expired. Change it now
	Password will expire in <n> day(s) Value of n can be between1 to 14 days.
	Password will expire today
	Intrusion Attempt: <n> time(s) by “intruder” n= number of intrusion attempt(s)
Signal (for MSPP services)	Idle Code Detected
	Test Signal Out of Sync
	Test Signal Error Received
	NPU Lockup
Timing and synchronization	Secondary SETS Locking to Primary
	Timing Distribution Reference Switch Complete
	Timing Generation Reference Switch Complete
	Timing Generation Entry to Freerun
	Timing Generation Entry to Holdover
Restart	Cold Restart
Restart	Warm Restart
Note: Site Manager does not display the events as event categories. Event categories are used to organize this table only. In Site Manager, the severity of alerts and events is Log.	

Site Manager navigation

The following figures provide an overview of the Site Manager navigation associated with the **Faults** and **Configuration** menus for the 6500. The figures show the path from the Site Manager menu bar.





Procedures for alarms and events

Action	Details
Setting the time zone for network element or Site Manager timestamps	Procedure 2-1 on page 2-12
Retrieving active alarms for one or more network elements	Procedure 2-2 on page 2-13
Retrieving events for a network element	Procedure 2-3 on page 2-15
Retrieving active disabled alarms	Procedure 2-4 on page 2-18
Allowing or inhibiting the display of log, inventory, and database change events	Procedure 2-5 on page 2-19
Clearing security alarms	Procedure 2-6 on page 2-20

Procedures for alarm provisioning and alarm profiles

Action	Details
Retrieving alarm profiles	Procedure 2-7 on page 2-21
Editing an alarm profile	Procedure 2-8 on page 2-22
Setting a default profile	Procedure 2-9 on page 2-25
Setting a profile as active	Procedure 2-10 on page 2-26

Procedures for alarm monitoring and management

Action	Details
Restarting an interface module or the CTM	Procedure 2-11 on page 2-27
Identifying the module, pluggable module/port, or facility that has raised an alarm	Procedure 2-12 on page 2-31
Clearing audible alarms and performing lamp tests	Procedure 2-13 on page 2-32

Procedures for external alarm provisioning and external controls

Action	Details
Provisioning environmental alarm attributes	Procedure 2-14 on page 2-35
Provisioning, operating, and releasing external controls	Procedure 2-15 on page 2-37

Procedures for Photonic system maintenance

Action	Details
Locating a reflective event	Procedure 2-16 on page 2-39
Preparing to perform fiber work on a Photonic system	Procedure 2-17 on page 2-43
Measuring Photonic amplifier output power	Procedure 2-18 on page 2-46

Associated procedures

Some procedures require the user to perform procedures relating to other topics. Before performing a procedure, if necessary ensure that 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 chapter 1 of *Administration and Security*, 323-1851-301.

Procedure 2-1
Setting the time zone for network element or Site Manager timestamps

Use this procedure to set the time zone used for displaying timestamps. You can select either the network element time zone or the local operating system (OS) time zone.

Changes do not take effect until the next launch of Site Manager.

Step	Action
1	Select the network element in the navigation tree.
2	Select **Preferences** from the **Edit** drop-down menu. The **Preferences** dialog box opens.
3	Select **6500** from the **Nodal Manager** option in the navigation area on the left of the Preferences dialog box.
4	Select the required radio button (**Network Element** or **Local OS**) to set the time zone used for displaying timestamps. — Select the **Set Defaults** button to return the setting to the default (Network Element). — The **OK** and **Apply** buttons are disabled if the current active time zone setting is selected.
5	Click **OK**. The applied changes do not take effect until the next launch of the Site Manager. To restart Site Manager, refer to the interface login and logout procedures in chapter 1 of *Administration and Security*, 323-1851-301. **—end—**

Procedure 2-2
Retrieving active alarms for one or more network elements

Use this procedure to:

- retrieve the active alarms and alarm details
- access the alarm clearing procedure
- sort active alarms
- filter active alarms
- update active alarms

Step	Action
1	Select the desired network element in the navigation tree.
2	Select **Consolidated Alarms** from the **Tools** drop-down menu or **Active Alarms** from the **Fault** drop-down menu. The **Consolidated Alarms** application opens in a separate window, and displays the active alarms according to your last filter settings and the alarm points that are not disabled. Alarms from all logged in network elements are displayed by default. You can choose to show alarms for one or a set of specific network elements. The **Active Alarms** application opens in a separate tab, and displays the active alarms according to your last filter settings and the alarm points that are not disabled. Alarms from all shelves are displayed by default. You can choose to show alarms from one specific shelf.
3	**If** you / **Then** want to sort the active alarms / go to step 4 want to filter the active alarms / go to step 6 want to update the active alarms / go to step 8 want to view details of an active alarm / go to step 9 have the required information displayed / the procedure is complete
4	Click on a column header to sort the alarms by that column, in ascending order. When you first open the **Consolidated Alarms** application, the columns are sorted from highest to lowest severity and then from most recent to oldest. All columns are sorted in alphabetical order except the Time Raised column. The Time Raised column is sorted by date, then time.

Procedure 2-2 (continued)
Retrieving active alarms for one or more network elements

Step	Action
5	Click again on the same column header to sort the alarms in descending order. Go to step 3.
6	To hide alarms of a specific severity from the Alarm List, clear the appropriate check box in the **Show** area. By default, the **Consolidated Alarms** or **Active Alarms** application displays active alarms of all severities. The **Consolidated Alarms** or **Active Alarms** application updates and no longer shows the alarms of that severity.
7	To display alarms filtered from the list, select the appropriate check box again in the **Show** area. The **Consolidated Alarms** or **Active Alarms** application updates. Go to step 3.
8	By default, the **Auto refresh** check box is checked and the alarm list is updated automatically. To manually update the active alarms, clear the **Auto refresh** check box to enable the **Refresh** button. Click **Refresh**. The **Last refresh** field displays the date (yyyy-mm-dd) and time (hh:mm:ss) of the most recent update of the **Consolidated Alarms** or **Active Alarms** application. Go to step 3.
9	To view the details of an alarm, click on the row for the alarm that you want to see in detail from the list of active alarms. The **Alarm details** area at the bottom of the **Consolidated Alarms** or **Active Alarms** application displays the details of the alarm. You can view the details of only one alarm at a time. In the **Active alarms** application, you can click on the **How to Clear** button to access the alarm clearing procedure for the selected alarm. Go to step 3.

—end—

Procedure 2-3
Retrieving events for a network element

Use this procedure to:

- retrieve all events or only disabled alarm events
- retrieve detailed information about an event. For a list of autonomous events, refer to Table 2-3 on page 2-4
- sort the event list
- filter the events to display (event severities are Critical, Major, minor, warning, cleared, and logged)
- update the events

The time stamp of alarm entries in the **Historical Fault Browser** application represents the date and time of the alarm being raised or cleared and not the actual system occurrences (alarm timestamps include the hold-on and hold-off periods). As a result, there may be a time discrepancy between an event and the corresponding alarms being raised or cleared. See the following:

- Time Raised column will be updated for all raise Events.
- Clear Time column will be updated for all Clear Events and for those Raise Events, which got Cleared.
- Date Time column indicated the date and time of both Raise and Clear events. For Raise events, this column will be same as Time Raised column and for Clear events, this column will be same as Clear Time column.

  Note: When retrieving event counts, the **Historical Fault Browser** application includes Events + Events (disabled alarms only) and provides the status bar message as the total. For example, if the maximum count is 500 for retrieving events, the status bar message indicates 521. That is, it includes Events + Events (disabled alarms only).

Step	Action
1	Select the network element in the navigation tree.
2	Select **Historical Fault Browser** from the **Faults** drop-down menu. You can identify the events by looking for Log in the Severity column. Alerts also have the Log severity. If you return to the **Historical Fault Browser** application during a session, the application displays the events according to the previous filter settings.

Procedure 2-3 (continued)
Retrieving events for a network element

Step	Action
3	In the **Show** area, select the: • **Events** radio button to display all events • **Events (Disabled Alarms Only)** radio button to display only events associated with disabled alarms ***Note:*** If the **Events (Disabled Alarms Only)** option is selected for a consolidated node, the **Historical Fault Browser** application retrieves and displays information for the primary shelf only. To retrieve events associated with disabled alarms on member shelves, you must execute the appropriate TL1 command on individual shelves.
4	

If you	**Then**
want to sort the event list	go to step 5
want to filter events	go to step 7
want to update the **Historical Fault Browser** application	go to step 9
want to retrieve events details	go to step 10
have the required information displayed	the procedure is complete

5	Click on a column header to sort the events by that column, in ascending order. When you first open the **Historical Fault Browser** application, the columns are sorted from most recent to oldest. All columns are sorted in alphabetical order except the Time Raised column, Clear Time column, and Date, Time column. The Time Raised column and the Clear Time columns are sorted by date and then time.
6	Click again on the same column header to sort the events in descending order. Go to step 4.
7	To hide events of a specific severity from the events list, clear the appropriate check box in the **Show** area. The **Historical Fault Browser** application updates and no longer shows the events of that severity.
8	To display events filtered from the list, select the appropriate check box again in the Show area. Go to step 4.

Procedure 2-3 (continued)
Retrieving events for a network element

Step	Action
9	If the **Events** radio button is selected, by default, the **Auto refresh** check box is checked and the event list is updated automatically. To manually update the events, clear the **Auto refresh** check box to enable the **Refresh** button. Click **Refresh**. **If the Events (Disabled Alarms Only)** radio button is selected, only manual refresh is supported. Click **Refresh**. The **Last refresh** field displays the date (yyyy-mm-dd) and time (hh:mm:ss) of the most recent update of the **Historical Fault Browser** application. Go to step 4.
10	From the event list, click on the row for the event that you want to see in detail. The **Event details** area at the bottom of the **Historical Fault Browser** application displays the details of the event. You can view the details of only one event at a time. Go to step 4.

—end—

Procedure 2-4
Retrieving active disabled alarms

Use this procedure to:

- retrieve list of active alarms that are raised against disabled alarm points
- retrieve detailed information about a disabled alarm
- access the alarm clearing procedure
- sort the alarms list
- update the **Active Disabled Alarms** application manually

Step	Action
1	Select the network element in the navigation tree.
2	Select **Active Disabled Alarms** from the **Faults** drop-down menu. The **Active Disabled Alarms** application opens, and displays a list of active alarms that are raised against disabled alarm points.
3	**If** you / **Then** want to sort the active alarms / go to step 4 want to update the active alarms / go to step 6 want to view details of an active alarm / go to step 7 have the required information displayed / the procedure is complete
4	Click on a column header to sort the alarms by that column, in ascending order.
5	Click again on the same column header to sort the alarms in descending order. Go to step 3.
6	To update the active alarms, click **Refresh**. The **Last refresh** field displays the date (yyyy-mm-dd) and time (hh:mm:ss) of the most recent update of the **Active Disabled Alarms** application. Go to step 3.
7	To view the details of an alarm, click on the row for the alarm that you want to see in detail from the list of inhibited alarms. The **Alarm details** area at the bottom of the **Active Disabled Alarms** application displays the details of the alarm. You can view the details of only one alarm at a time. Click on the **How to Clear** button to access the alarm clearing procedure for the selected alarm. Go to step 3.

—end—

Procedure 2-5
Allowing or inhibiting the display of log, inventory, and database change events

Use this procedure to allow or inhibit TL1 autonomous events used for application refreshes (except for alarms that operate independently of this option). The TL1 autonomous events are allowed by default.

Step	Action
1	Select the network element in the navigation tree.
2	Select the **Faults** drop-down menu. The **Update on Data Changes** menu option appears at the bottom of this menu. If a checkmark appears next to the **Update on Data Changes** option, the option is enabled and the TL1 autonomous events used for application refreshes are allowed. If a checkmark does not appear next to the **Update on Data Changes** option, the option is disabled and the TL1 autonomous events used for application refreshes are inhibited.
3	To change the status of the **Update on Data Changes** menu option (to either allowed or inhibited), select this option from the **Faults** drop-down menu.

—end—

Procedure 2-6
Clearing security alarms

Use this procedure to clear security alarms (except those raised against the Primary and Secondary RADIUS servers) on a network element (for example, Intrusion Attempt).

Step	Action
1	Select the network element in the navigation tree.
2	Select **Clear Security Alarms** from the **Faults** drop-down menu.
3	Click **Yes** in the confirmation dialog box. All security alarms (except those raised against the Primary and Secondary RADIUS servers) are cleared. The procedure does not unlock channels associated with an Intrusion Attempt alarm. Refer to the “Unlocking source addresses/users” procedure in *Administration and Security*, 323-1851-301. **—end—**

Procedure 2-7
Retrieving alarm profiles

Use this procedure to retrieve information about alarm profiles and profile details.

For more information on alarm profiles, refer to "Alarm profiles" on page 1-22.

Step	Action
1	Select the network element in the navigation tree.
2	Select **Alarms & Controls** from the **Configuration** drop-down menu.
3	Select **Alarm Profiles**.
4	Select an alarm class from the **Alarm Class** drop-down list.
5	Select a **Type** from the **Type** drop-down list.
6	As applicable, select the required criteria from the **Shelf, Slot, Port**, and **Wavelength** drop-down lists that are available. Depending on the shelf function and equipment or facility type you select, the **Shelf**, **Slot, Port**, and **Wavelength** drop-down lists become available as more selections are made.
7	Click **Retrieve**. The Profiles table in the upper section of the **Alarm Profiles** application displays all the available alarm profiles for the selection. The Active Profiles table in the centre section of the **Alarm Profiles** application displays the active profiles for the selection.
8	If you want to display details about an alarm profile, select the profile from the Profiles table in the upper section of the **Alarm Profiles** application. The Profile Details table at the bottom of the **Alarm Profiles** application displays all the alarm points applicable to the selected profile and their status.

—end—

Procedure 2-8
Editing an alarm profile

CAUTION
Risk of unidentified problem conditions
Disabling an alarm point prevents alarm notification if a fault occurs.

Use this procedure to edit an existing alarm profile. This procedure allows you to change the:

- name of the alarm profile
- status (enabled/disabled) of the alarm points
- **Service affecting severity** (SA) or **Not service affecting** (NSA) severities (Critical, Major, minor, warning)

Alarm provisioning only affects alarm notification and has no effect on the alarm function.

Note: When Shelf Synch is enabled on a consolidated node, the alarm profile cannot be edited for member shelves. For information on Shelf Synch, refer to the "Shelf Synch" section in the Node information chapter in *Administration and Security*, 323-1851-301.

ATTENTION
You cannot edit the ALL ENABLED, ALL DISABLED, or FACTORY DEFAULT profiles that the system has defined.

Prerequisites

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

Note that an account with a level 4 UPC or higher is required to edit the Alarm class of Security alarm points.

Step	Action
1	Retrieve the alarm profiles of the network element. Refer to "Retrieving alarm profiles" on page 2-21.
2	Select the profile to edit. You cannot edit the ALL ENABLED, ALL DISABLED, and FACTORY DEFAULT profiles that the system has defined.

Procedure 2-8 (continued)
Editing an alarm profile

Step	Action

3 **If** you / **Then**

If you	Then
want to change the alarm profile name	go to step 4
want to change the status of the alarm points	go to step 9
want to change the SA and NSA severity	go to step 15
have completed the required changes	the procedure is complete

4 Click **Edit** in the alarm profile list area to open the Edit Profile dialog box.

The Edit Profile dialog box contains the current name of the selected profile.

5 Click on the **profile** name field and highlight the profile name.

6 Type in the new alarm profile name.

The alarm profile name can be up to 20 characters.

7 If shelf sync is not enabled, select the **Apply to all available shelves within the TID** check box if you want to apply the profile name change to all available shelves.

8 Click **OK**.

Go to step 3.

9 Select one or more alarm points that you want to enable or disable.

To select multiple alarm points, hold down the **Shift** or **Ctrl** key when you select the alarm points.

10 Click **Edit** in the alarm point list area to open the Edit Alarm Point dialog box.

11 Click **Enabled** or **Disabled** as applicable from the **Alarm status** drop-down list.

12 If shelf sync is not enabled, select the **Apply to all available shelves within the TID** check box if you want to apply the alarm point change to all available shelves.

13 Click **OK**.

14 Repeat step 9 to step 11 until you have finished editing all the alarm points.

The edited alarm point status is displayed in the Profile details table at the bottom of the **Alarm Profiles** application.

Go to step 3.

15 Select one or more alarm points that you want to change the severity.

To select multiple alarm points, hold down the **Shift** or **Ctrl** key when you select the alarm points.

16 Click **Edit** in the alarm point list area to open the Edit Alarm Point dialog box.

Procedure 2-8 (continued)
Editing an alarm profile

Step	Action
17	Select the desired severity for the alarm from the **Service affecting severity** or **Not service affecting severity** drop-down list. You can provision alarm severities (SA or NSA) as Critical, Major, minor or warning.
18	If shelf sync is not enabled, select the **Apply to all available shelves within the TID** check box if you want to apply the alarm point change to all available shelves.
19	Click **OK**. Go to step 3.

—end—

Procedure 2-9
Setting a default profile

Use this procedure to set the alarm profile of an alarm class as the default profile.

CAUTION
Risk of unidentified problem conditions
Disabling an alarm point prevents alarm notification if a fault occurs.

Alarm provisioning only affects alarm notification and has no effect on the alarm function.

ATTENTION
You cannot set the default alarm profile for an alarm class for which the default is fixed at FACTORY DEFAULT (for example, COM).

Prerequisites

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

Note that an account with a level 4 UPC or higher is required to edit the Alarm class of Security alarm points.

Step	Action
1	Retrieve the alarm profiles of the network element by alarm class. Refer to "Retrieving alarm profiles" on page 2-21.
2	Select a profile from the profiles table in the upper section of the **Alarm Profiles** application.
3	Click **Set As Default**.
4	If you want to apply the default profile to all available shelves, click **Yes** in the confirmation dialog.
5	If you do not want to apply the default profile to all available shelves, click **No** in the confirmation dialog. The word Default is displayed in the Alarm Class Default column on the row of the selected profile.

—end—

Procedure 2-10
Setting a profile as active

CAUTION
Risk of unidentified problem conditions
Disabling an alarm point prevents alarm notification if a fault occurs.

Use this procedure to set the alarm profile of an alarm class as the active profile.

Consider the following:

- Alarm provisioning only affects alarm notification and has no effect on the alarm function.
- Selecting the ALL DISABLED profile for an alarm class or a specific equipment/facility disables all alarms for the alarm class or the specific equipment or facility.
- Selecting the FACTORY DEFAULT profile for Common alarm class enables all alarms in this class (except LAN Link Failure, which is disabled).

Prerequisites

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

Note that an account with a level 4 UPC or higher is required to edit the Alarm class of Security alarm points.

Step	Action
1	Retrieve the alarm profiles of the network element. Refer to "Retrieving alarm profiles" on page 2-21.
2	Select a profile from the profiles table.
3	Click **Set as Active**. The Active profiles table in the center section of the **Alarm Profiles** application displays the active profiles for the selected alarm class. The **Set as Active** button is disabled if there are no equipment/facilities provisioned for the selected alarm class.

—end—

Procedure 2-11
Restarting an interface module or the CTM

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

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

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

Use this procedure to initialize a CTM in a cold restart mode.

CAUTION
Risk of traffic loss
Do not cold restart both CTMs at the same time. A cold restart of both CTMs causes a traffic loss.

Consider the following:

- A loss of connectivity to the CTM occurs when you restart the CTM. You must wait up to 10 minutes before logging back in.
- A “Redundant Database Synch Failed” alarm is expected after a warm or cold restart. The alarm will clear automatically.
- If both CTMs are healthy and available, and all provisioning data is synchronized between the CTM pair, a user-initiated cold restart will result in a CTM switch of activity.
- If the mate/inactive CTM is unhealthy, unavailable or is unsynchronized, a user-initiated cold restart will not result in a switch of activity. The exception is if the mate/inactive CTM is an “IS-ANR,FLT” (In-service, Abnormal, Fault Detected) state, in which case, there will be a switch of activity.

- It is an expected behavior that after a CTM restart is performed on a remote network element (RNE), the first login attempt to the RNE will fail. An “Operation Failed” error message appears and you need to log back in a second time to establish the connection to the RNE.

Impact of module restart

Impact on PM counts

For Photonic modules, current and previous bin PM statistics are stored on the CTM. Therefore, a restart of any type on a PKT/OTN interface module clears untimed, current and previous bin PM counts, and displays "0" for each monitor type along with the invalid data flag (?). Similarly, a restart of the CTM clears untimed, current and previous bin PM counts for Photonic modules provisioned on the shelf.

Impact on alarms and time of day

- After a CTM is restarted, the Duplicate Shelf alarm is masked for 20 minutes.
- If the time of day (TOD) synchronization feature is enabled, you do not have to reprovision the date and time.

Impact on CTM and timing

A cold restart of the CTM can affect traffic if the timing on the mate CTM is not locked (Secondary SETS Locking to Primary warning is present).

Prerequisites

For Photonic services, restarts are only supported on the RLA and CCMD16x12 modules.

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

Step	Action		
1	Select the network element in the navigation tree.		
2	**If** you want to perform a	**Then** go to	
	cold restart	step 3	
	warm restart	step 7	
3	**If** the module you are performing a cold restart on		**Then** go to
	is an interface module		step 5
	is a switch module		step 6
	is a CTM		step 7

Procedure 2-11 (continued)
Restarting an interface module or the CTM

Step	Action
4	Change the facility states to out-of-service for all facilities on the module. To display the facility details, you must first select the equipment from the Equipment area of the **Equipment & Facility Provisioning** application.
5	Change the equipment state of the module to out-of-service. When you place the module out-of-service, any pluggable modules and pluggable transceivers on that module are automatically placed out-of-service.
6	Select **Restart** from the **Faults** drop-down menu.
7	If applicable, select the required shelf from the **Shelf** drop-down list.
8	Select the module or CTM you want to restart from the **Card** drop-down list.
9	Select the restart type (warm or cold) from the **Restart type** drop-down list.
10	Click **OK**.
11	A **Confirm Restart** dialog box appears with a “Capture logs before restart” checkbox. This box will be unchecked by default if you have chosen a warm restart. For cold restart, the box will be checked by default. For more information about the “Capture logs” feature, refer to *Fault Management - Customer Visible Logs,* 323-1851-840.
12	Click **Restart.** For an active CTM, the restart will take 8 to 15 minutes. For other modules, the restart will take 4 to 10 minutes to complete. If after the expected time the retrieve log is not completed, Site Manager automatically issues the restart command. During a cold restart of the CTM module with or without the CTMX module in place, the LEDs go through the following sequence: • the module LED flashes • the Green LED flashes • the Green LED turns solid and if the CTM module is in-service, the Blue LED turns on If the CTMX module is present, the CTMX LEDs go through the above sequence after 30 seconds.
13	Refer to “Module LEDs” on page 1-10 for information on LED activity during a restart.

Procedure 2-11 (continued)
Restarting an interface module or the CTM

Step	Action	
14	**If** you have performed a	**Then**
	warm restart	the procedure is complete
	cold restart on a CTM	the procedure is complete
	cold restart on a switch module	go to step 15
	cold restart on a PKT/OTN interface module	go to step 15
15	Change the equipment state of the module to in-service. Refer to the "Changing the primary state of a circuit pack, module, or pluggable" procedure in Part 1 of *Configuration - Provisioning and Operating*, 323-1851-311.	
16	Change the facility states to in-service for all facilities on the module. Refer to the "Changing the primary state of a facility" procedure in Part 1 of *Configuration - Provisioning and Operating*, 323-1851-311.	

—end—

Procedure 2-12
Identifying the module, pluggable module/port, or facility that has raised an alarm

Use this procedure to identify which module, pluggable module/port, or facility has raised an alarm.

Step	Action
1	Retrieve the active alarms on the network element. Refer to Procedure 2-2, "Retrieving active alarms for one or more network elements" on page 2-13.
2	Identify the alarm in the Alarm List. The Unit column in the **Consolidated Alarms** or **Active Alarms** application specifies the module, pluggable module/port/port using the following format: <module>-<shelf-id>-slot#-subslot# (for subslot equipment alarms) or <facility type>-<shelf-id>-slot#-subslot# (for subslot facility alarms). To view details of an alarm, select the alarm in the alarm list. The Alarm details area displays the details of the alarm.

—end—

Procedure 2-13
Clearing audible alarms and performing lamp tests

Use this procedure to clear audible alarms and perform lamp tests on network elements. When you clear an audible alarm, the alarmed LEDs and fault are not cleared.

The network element relay contacts that you can connect to both visual and audible alarms. and four contact pairs for a DSM. Therefore, you can connect Critical, Major, minor, and remote alarms to separate audible alarms for a network element.

To clear audible alarms and perform lamp tests using the Site Manager **Visualization** tool, refer to the “Performing a lamp test and clearing audible alarms using the Visualization tool” procedure in *Administration and Security*, 323-1851-301.

Prerequisites

To perform the clearing audible alarms using Site Manager steps, you require an account with at least a level 2 UPC.

Procedure 2-13 (continued)
Clearing audible alarms and performing lamp tests

Step	Action	
1	**If** you want to	**Then** go to
	clear audible alarms manually	step 2
	clear audible alarms using Site Manager **Faults** menu	step 4
	perform a lamp test using the ACO button	step 9
	perform a lamp test using Site Manager	see Note
	Note: Refer to the "Performing a lamp test and clearing audible alarms using the Visualization tool" procedure in *Administration and Security,* 323-1851-301.	

Clearing audible alarms manually

2 Locate the network element with the audible alarm.

3 Press the ACO button once to reset the audible alarm relays for the network element.

The ACO LED is lit.

The procedure is complete.

Procedure 2-13 (continued)
Clearing audible alarms and performing lamp tests

Step	Action

Clearing audible alarms using Site Manager Faults menu

4 Select the network element in the navigation tree.

5 Select **Alarm Cut-Off** from the **Faults** drop-down menu.

The Alarm Cut-Off dialog box is displayed.

6 If applicable, select the required shelf from the **Shelf** drop-down list.

7 Select **All** from the **Source** drop-down list.

8 Click **OK**.

The procedure is complete.

Performing a lamp test using the ACO button

9 Locate the required network element.

10 Press the ACO button for two seconds, and then release (See the “Attention” below). If there are:

- no audible alarms, pressing the ACO button activates a lamp test.
- audible alarms, pressing the ACO button clears the audible alarms (ACO LED is lit). To perform a lamp test, you must press the ACO button a second time.

ATTENTION
The ACO button and LED is located with the shelf Critical, Major and Minor alarm LEDs.

The ACO LED remains lit until a new Major alarm is raised. Upon detection of a Major alarm, the ACO releases and the LED turns off.

—end—

Procedure 2-14
Provisioning environmental alarm attributes

Use this procedure to:

- retrieve environmental alarm attributes
- set up or change environmental alarm attributes on the network element
- delete defined environmental alarm attributes on the network element

Environmental alarm attributes require resetting if you replace an existing environmental alarm with a different type of input. For example, when you replace a humidity alarm with a toxic gas detector, you must edit the environmental alarm attributes.

ATTENTION
When you remove a device for detecting an environmental alarm, delete the environmental alarm attributes.

Prerequisites

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

Step	Action	
1	Select the network element in the navigation tree.	
2	Select **Alarms & Controls** from the **Configuration** menu.	
3	Select **External Alarm Provisioning**.	
4	Select a shelf from the **Shelf** drop-down list.	
5	Select a source from the **Source** drop-down list.	
6	**If** you want to	**Then** go to
	edit the environmental alarm attributes	step 7
	delete the environmental alarm attributes	step 16
7	Select any entry in the contact list to enable the **Edit** button.	
8	Click **Edit** to open the Edit External Alarm dialog box.	
9	Select the contact you want to set or edit from the **Contact** drop-down list.	

Procedure 2-14 (continued)
Provisioning environmental alarm attributes

Step	Action
10	Select the label from the **Label** drop-down list. Refer to "Environmental alarm labels" on page 2-2.
11	Select the severity from the **Severity** drop-down list.
12	Edit the description if you want to describe the alarm with specific text. The description can contain a maximum of 40 characters.

ATTENTION
Do not use apostrophes " ' " in the alarm text. Using apostrophes in the alarm text will cause display errors in the OneControl active events list (AEL).

13	Click **Apply**.
14	Repeat step 9 through step 13 if you want to set or edit more contacts.
15	Click **OK**. The procedure is complete.
16	Select the provisioned contact from which you want to delete attributes in the contact list as follows:

If you want to delete	**Then**
one entry	click the entry you want to delete
some, but not all entries	select the first entry in the list and hold down the **Ctrl** key while individually clicking on each required entry
all entries	select the first entry in the list and hold down the **Shift** key while clicking once on the last entry in the list or select any desired entry in the list and then **Ctrl+A** to select all entries

17	Click **Clear Entry**.
18	Click **Yes** in the confirmation dialog box.

—end—

Procedure 2-15
Provisioning, operating, and releasing external controls

Use this procedure to:

- retrieve the labels and status of all external controls
- provision control labels and types to control relays on the network element. The network element allows four external control relays to turn external equipment on and off.
- operate external controls
- release external controls

Prerequisites

To edit external controls, you require an account with at least a level 3 UPC.

To operate or release external control equipment, you require an account with at least a level 2 UPC.

Step	Action	
1	Select the required network element in the navigation tree.	
2	Select **Alarms & Controls** from the **Configuration** drop-down menu.	
3	Select **External Controls**.	
4	Select a shelf from the **Shelf** drop-down list.	
5	Select a source from the **Source** drop-down list.	
6	**If** you want to	**Then** go to
	edit external control attributes	step 7
	operate (turn on) external control equipment	step 11
	release external control equipment	step 14
7	Click **Edit**.	
8	Select the relay label from the drop-down list at the relay for which you want to set or edit attributes. Refer to “External control types” on page 2-2.	
9	Repeat step 8 if you want to set or edit more relays.	
10	Click **OK**.	
	The procedure is complete.	

Procedure 2-15 (continued)
Provisioning, operating, and releasing external controls

Step	Action
11	Select the required relay.
12	Click **Operate**.
13	Click **Yes** in the confirmation dialog box.
	The procedure is complete.
14	Select the required relay.
15	Click **Release**.
16	Click **Yes** in the confirmation dialog box.

—end—

Procedure 2-16
Locating a reflective event

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

In this procedure you will attempt to isolate the connector losses by starting at the connector that is farthest from the alarmed amplifier and then working back towards the alarmed amplifier. Refer to Figure 2-1 on page 2-42 for an example of an alarmed amplifier at a line amplifier site.

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

Prerequisites

To perform this procedure, you must:

- observe all safety requirements described in *Installation - General Information,* 323-1851-201.0
- have a network diagram that identifies all connection points at the site of the alarmed module that can be cleaned
- have the appropriate personal grounding device to dissipate electrostatic charges
- have a mandrel or screwdriver

Step	Action
1	**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.
2	Review the network diagram, and locate the connector that is farthest from the alarmed amplifier within the site.

Procedure 2-16 (continued)
Locating a reflective event

Step	Action	
3	Wind the optical fiber patchcord attached to the connector, identified in step 2, four turns around a 15-mm mandrel. You can use a screwdriver handle or other similar sized cylinder in place of a mandrel. This step checks for high reflection (low return loss) by causing attenuation of the optical power in the direction back towards the amplifier output.	
4	**If** the original alarm	**Then**
	does not clear, and there are more optical fiber patchcords before the alarmed amplifier	the reflective event is closer to the alarmed amplifier. Go to step 5.
	does not clear, and there are no more optical fiber patchcords before the alarmed amplifier at this site (you are now at the output of the alarmed amplifier)	If you were sent from another procedure, return to the step in the procedure that referred you to this procedure. Otherwise, contact your next level of support or your Ciena support group.
	clears	Go to step 6.
5	Locate the next farthest connector from the alarmed amplifier and go to step 3.	
6	Place the alarmed amplifier out-of-service (OOS).	

Procedure 2-16 (continued)
Locating a reflective event

Step	Action

7

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

CAUTION
Risk of damage to modules
Never disconnect an optical fiber that is connected to an active or powered up optical amplifier. To disconnect or reconnect an optical fiber, make sure the optical amplifier is out of service (OOS), then disconnect or reconnect the fiber.

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

Clean and then reconnect the output fibers and connectors at the amplifier. Refer to the “Inspecting and cleaning optical interface connectors” and “Cleaning optical connectors and adapters on patchcords” procedures in *Installation - General Information,* 323-1851-201.0.

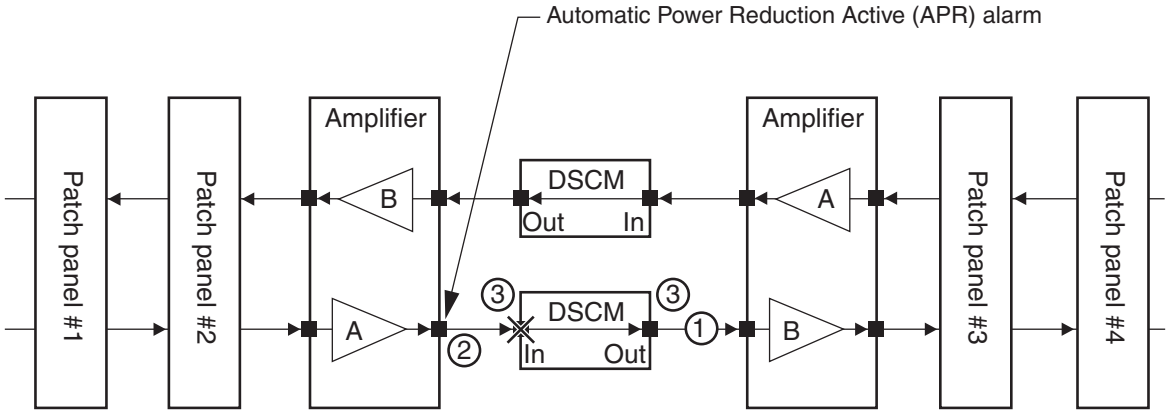
8 Place the amplifier back in-service (IS).

9

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

—end—

Figure 2-1
Locating connector losses at a Photonic line amplifier site (with DSCM)



Legend

× Indicates the reflection point (actual problem point in this example).

① Perform mandrel test on optical fiber patch cord at ① . In this example, the APR alarm is not cleared, because the optical power attenuation is occurring after the reflection point (×).

② Backtrack in direction towards alarmed amplifier port. Perform mandrel test on optical fiber patch cord ②. In this example the alarm clears because attenuated optical power is reflected.

③ Clean connectors at ③ on both sides of the DSCM. Ensure amplifier is OOS before cleaning connectors.

Note 1: If alarm does not clear, the problem is likely with the patch panel or DSCM.
Note 2: Although the measurement is done at the output port, the APR alarm is raised against the AMP facility attached to the input port. Therefore, the APR alarm is raised against the input port.

Procedure 2-17
Preparing to perform fiber work on a Photonic system

Use this procedure to record existing power levels and amplifier gain settings before performing fiber maintenance/repair and to re-adjust these parameters if the fiber maintenance/repair causes power levels to change.

Note that this procedure cannot be used to repair a fiber cut that occurred. This procedure can only be used to prepare in advance for a fiber cut that you know will occur (for example, related to scheduled maintenance activities).

CAUTION
Risk of traffic loss
Placing an amplifier module OOS causes a traffic loss. It is recommended that this procedure be performed during a maintenance window (when traffic is lightest), or that all traffic be routed away from the affected network element before performing this procedure.

CAUTION
Risk of damage to downstream amplifier
You must complete this procedure on an amplifier that is downstream of the location where the fiber cut or maintenance activity will be performed. Not performing this procedure can result in power levels at the amplifier that are high enough to damage the module.

Prerequisites

To perform this procedure, you must:

- use an account with at least a level 3 UPC
- observe all safety requirements described in *Installation - General Information,* 323-1851-201.0
- have a network diagram that identifies all connection points at the site of the alarmed module that can be cleaned

Step	Action
1	Log into the network element containing the amplifier that is downstream of the location where the fiber cut or maintenance activity will be performed.
2	From the **Configuration** menu, select **Equipment & Facility Provisioning**.

Procedure 2-17 (continued)
Preparing to perform fiber work on a Photonic system

Step	Action
3	Select the LIM module supporting the AMP facility (of the amplifier that is downstream of the location where the fiber cut or maintenance activity will be performed) in the **Equipment** area.
4	From the **Facility Type** drop-down menu, select AMP.
5	Record the **Target Gain** for the AMP facility of the amplifier that is downstream of the location where the fiber cut or maintenance activity will be performed.
6	From the **Performance** menu, select **Performance Monitoring** and then **New**.
7	From the **Type** drop-down list, select AMP.
8	From the **Facility** drop-down list, select the AMP facility of the amplifier that is downstream of the location where the fiber cut or maintenance activity will be performed.
9	Retrieve the PMs for the AMP facility.
10	Record the current (Untimed) Input Power (OPIN).
11	From the **Configuration** menu, select **Photonics Services** and then **Domain Optical Controller (DOC)**.
12	Change the DOC Primary State to out of service (OOS).
13	**CAUTION** **Risk of traffic loss** Placing an amplifier module OOS causes traffic loss. It is recommended that this procedure be performed during a maintenance window (when traffic is lightest), or that all traffic be routed away from the affected network element before performing this procedure. Place the amplifier downstream of the fiber cut/maintenance OOS.
14	Perform the maintenance/repair fiber according to the safety requirements of your company and the safety requirements described in *Installation - General Information,* 323-1851-201.0.
15	Repeat step 1 to step 10.
16	Compare the current (Untimed) Input Power (OPIN) to the previously recorded value in step 10.

Procedure 2-17 (continued)
Preparing to perform fiber work on a Photonic system

Step	Action	
17	**If** the Input Power (OPIN) value has	**Then**
	decreased by more than 3 dB	check the fiber splice and fiber connections. It is likely that the splice is poor or there is a dirty connection. Correct the problem and go to step 18.
	increased by more than 3 dB	provision the downstream OOS amplifier **Target Gain** downwards by the difference in the input power. For example, if the input power increased by 4 dB and the previous amplifier **Target Gain** was 18 dB, the new amplifier **Target Gain** will be 18 dB - 4 dB = 14 dB. Go to step 18.
	otherwise	go to step 18
18	Place the amplifier downstream of the fiber cut/maintenance from step 13 back in service (IS).	
19	Place the DOC **Primary state** back in service (IS).	
20	Reset all threshold crossing alert (TCA) baselines for the DOC domain.	
21	Record the current DOC **Automation mode**. Change the DOC **Automation mode** to “Enhanced”.	
22	Wait for DOC to perform optimization. This may take up to five minutes to begin.	
23	Once optimization is complete, return the DOC **Primary state** and DOC **Automation mode** to their original settings.	

—end—

Procedure 2-18
Measuring Photonic amplifier output power

Use this procedure to measure the output power of an amplifier to facilitate Photonic line troubleshooting.

Prerequisites

To perform this procedure, you must:

- use an account with at least a level 3 UPC
- observe all safety requirements in *Installation - General Information,* 323-1851-201.0
- have a network diagram that identifies all connection points at the site of the alarmed module that can be cleaned
- have a high-powered optical power meter with the same optical connectors as the network element that can read power levels as high as +11 dB
- have a 10 dB fixed-pad optical attenuator (ensure the attenuator loss value has been calibrated)
- have a personal grounding device

CAUTION
Risk of traffic loss
Disconnecting fibers causes traffic loss on the associated facilities. It is recommended that this procedure be performed during a maintenance window (when traffic is lightest), or that all traffic be routed away from the affected network element before performing this procedure.

Step	Action
1	In the **Domain Optical Controller (DOC)** application in Site Manager, record the current **Automation mode** for the two DOC network elements that manage each optical direction of the amplifier. Change the **Automation mode** to “Enhanced Auto Monitor Only” (if not already).

Procedure 2-18 (continued)
Measuring Photonic amplifier output power

Step	Action

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

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

3 Place a 10 dB fixed-pad optical attenuator at the input to the optical power meter (to prevent raising the Automatic Power Reduction Active alarm).

4

If you want to measure the amplifier output power of	**Then** go to
port 5 (Line B)	step 5
port 7 (Line A)	step 10

5 In the **Equipment & Facility Provisioning** application in Site Manager, record the current AMP facility **Shut Off Threshold (dBm)** value for Line A (port 8) on both line-facing ends of the amplifier.

6 Provision the AMP facility **Shutoff Threshold** to -60 dBm for Line A (port 8) on both line-facing ends of the amplifier. Perform this action using the ED-AMP TL1 command:

```
ED-AMP::<AID>:CTAG:::,,,,,,SHUTTHRES=-60,,,,,:,,;
```

Refer to ED-AMP command in *TL1 Description,* 323-1851-190.

ATTENTION
Provisioning the SAM, ESAM or AMP facility **Shutoff Threshold** to -60 dBm disables the ALSO safety feature, and injury can occur.

The Automatic Shutoff Disabled alarm will raise.

ATTENTION
ALSO can be disabled on the LIM cards (C-Band and L-Band) by setting the ALSO Disable flag to TRUE for the OPTMON facility. This action should only be performed when there is no OSC in the OTS for automatic recovery from optical line fail condition.

7 Remove the OSC B In (port 3) fiber from the amplifier. This allows you to measure the amplifier output only. If the OSC B In (port 3) fiber is not removed, you are also including the OSC channel in the measurement.

Procedure 2-18 (continued)
Measuring Photonic amplifier output power

Step	Action

8

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

CAUTION
Risk of traffic loss
Disconnecting fibers causes traffic loss on the associated facilities. It is recommended that this procedure be performed during a maintenance window (when traffic is lightest), or that all traffic be routed away from the affected network element before performing this procedure.

Measure the port 5 (Line B) amplifier output power using the high-powered optical power meter. Add the calibrated attenuator loss to the measured value. This total power is 10 dB lower due to the attenuator inserted into the power meter.

9 Clean and reinstall the OSC B In (port 3) fiber removed in step 7. Refer to the cleaning connectors procedures in *Installation - General Information,* 323-1851-201.0.

Go to step 11.

10

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

CAUTION
Risk of traffic loss
Disconnecting fibers causes traffic loss on the associated facilities. It is recommended that this procedure be performed during a maintenance window (when traffic is lightest), or that all traffic be routed away from the affected network element before performing this procedure.

Procedure 2-18 (continued)
Measuring Photonic amplifier output power

Step	Action
	Measure the port 7 (Line A) amplifier output power using the optical power meter. Add the calibrated attenuator loss to the measured value. This total power is 10 dB lower due to the attenuator inserted into the power meter.
11	When the power measurement is complete, clean all connections of the optical fiber link following your company standards, and restore the fiber connection to the amplifier output port. Refer to the cleaning connectors procedures in *Installation - General Information*, 323-1851-201.0.
12	If port 5 (Line B) was measured, then restore the AMP facility **Shut Off Threshold (dBm)** value for Line A (port 8) to the original settings recorded in step 5 for both line-facing ends of the amplifier. This must be performed using the ED-AMP TL1 command: `ED-AMP::<AID>:CTAG:::,,,,,,SHUTTHRES=<`**`step 5 recorded value`**`>,,,,,:,,;`
13	In the **Domain Optical Controller (DOC)** application in Site Manager, restore the **Automation mode** to the original settings recorded in step 1 for both DOC network elements.

—end—

Alarm hierarchies and alarm severities

ATTENTION
Alarm severities described in this chapter are the default alarm severities provisioned on the system. Alarm severities can be modified by using different alarm profiles. Refer to Chapter 2, "Alarm surveillance" of this document for details on how to change alarm severities.

Alarm severities

The level of severity for alarms are Critical (C), Major (M), and minor (m). Alarm reports always contain a notification code that identifies the alarm severity, or the code CL to indicate that the fault has been cleared. The w code indicates a warning. The A code indicates an alert (only applicable to alarm banner). Event reports have a logged (Log) severity.

Note: Alarm severities can be modified (protected/unprotected). Refer to Procedure 2-8, "Editing an alarm profile" on page 2-22.

Critical alarms (C)

Critical alarms are the most severe. Critical alarms always indicate a service-affecting fault. For example, unprotected facility losses and unprotected facility-carrying equipment failures raise critical alarms.

Major alarms (M)

Major alarms are less severe than critical alarms but can be service-affecting or non-service-affecting.

Major alarms are raised when something has an effect on a low-speed facility. For example, a Major alarm is raised when tributary signals fail or unprotected provisioned modules are missing.

Minor alarms (m)

Minor alarms are less severe than Major alarms, but can be service-affecting or non-service-affecting.

For example, a non-service-affecting minor alarm is raised when a protected circuit fails. However, an AIS service-affecting minor alarm raises when a linear protected configuration does not have protection available.

Cleared alarm notification (CL)

The cleared notification code indicates that the fault no longer exists. The automatic output cache stores the cleared alarm reports.

Warning (w)

Warning events are raised by the network element as Standing Conditions (SC), and are less severe than minor alarms. A warning is an indication a problem exists on the network element that can eventually escalate into an alarm of higher severity.

Alert (A)

Threshold-crossing alerts are less severe than alarms. An alert can indicate that the threshold crossed does not affect service but requires further investigation.

Alerts are indicated in the alarm banner and appear with a Logged (Log) severity in the Events window.

> ***Note:*** Performance high and low threshold crossings are not displayed in Site Manager as alarms, but they are displayed in OneControl as alarms.

Logged (Log)

Event reports are generated from changes of state and other important transient conditions.

Service-affecting and non-service-affecting severities

By default, alarms generally have both a service-affecting (high impact) severity and non-service-affecting (low impact) severity. The triggered severity depends on the system state when the alarmed conditions occurred. For some alarms, there is only one severity. The user can perform alarm provisioning, which can be used to enable/disable alarm points, and change the service-affecting (high impact) severity and non-service-affecting (low impact) severities of alarms. Refer to "Procedures for alarm provisioning and alarm profiles" on page 2-10.

For example, a Circuit Pack Fail alarm can be raised with a:

- high impact of Critical, service-affecting (C, SA) for a module in an unprotected configuration with cross-connects
- low impact of minor, non-service-affecting (m, NSA) for a module without cross-connects

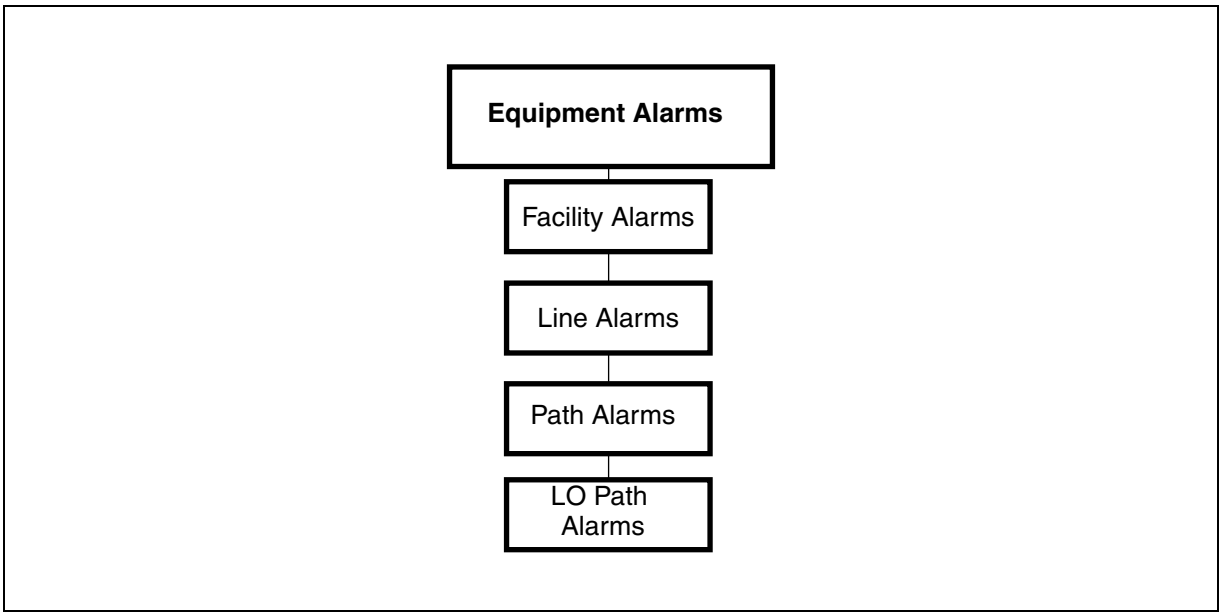
Photonic services alarms

Photonic alarms do not support multiple severity levels. That is, there is only one severity per alarm.

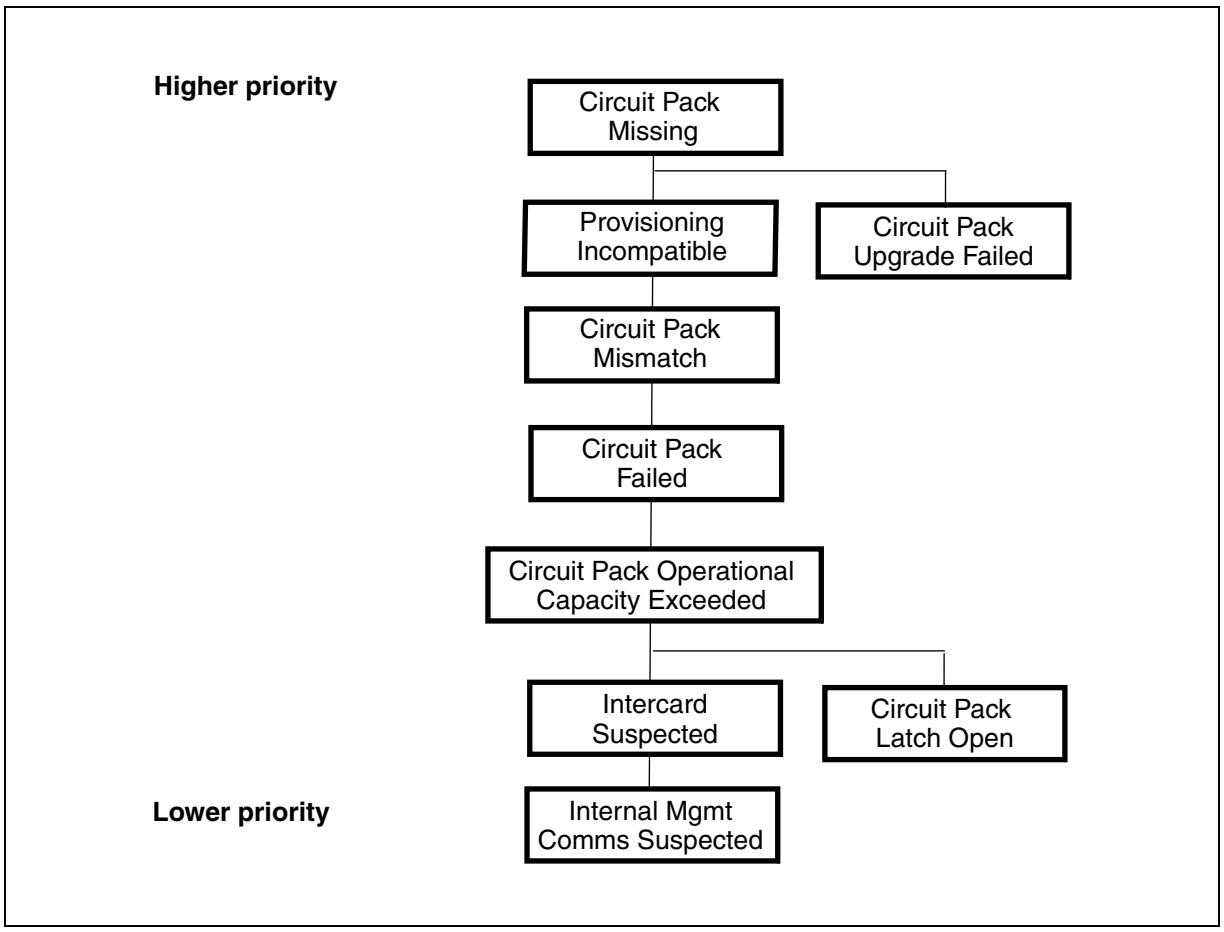
Alarm hierarchies

The following alarm hierarchy diagrams are made to be as generic and simple as possible. Therefore, not every alarm or circumstance shown applies to all modules.

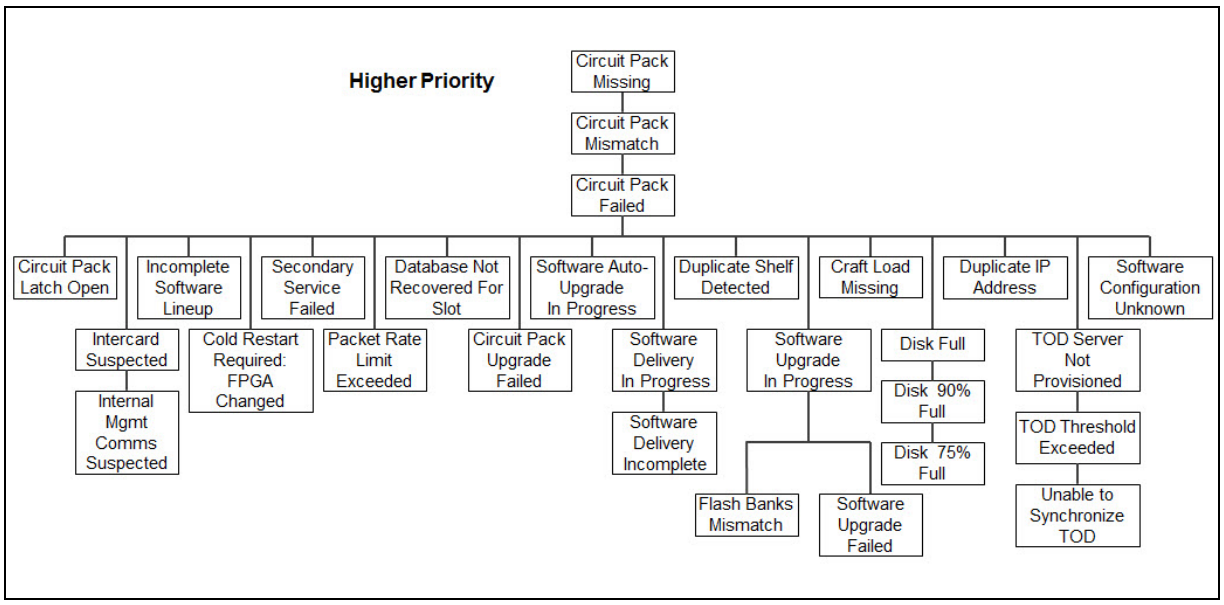
Overall alarm hierarchy



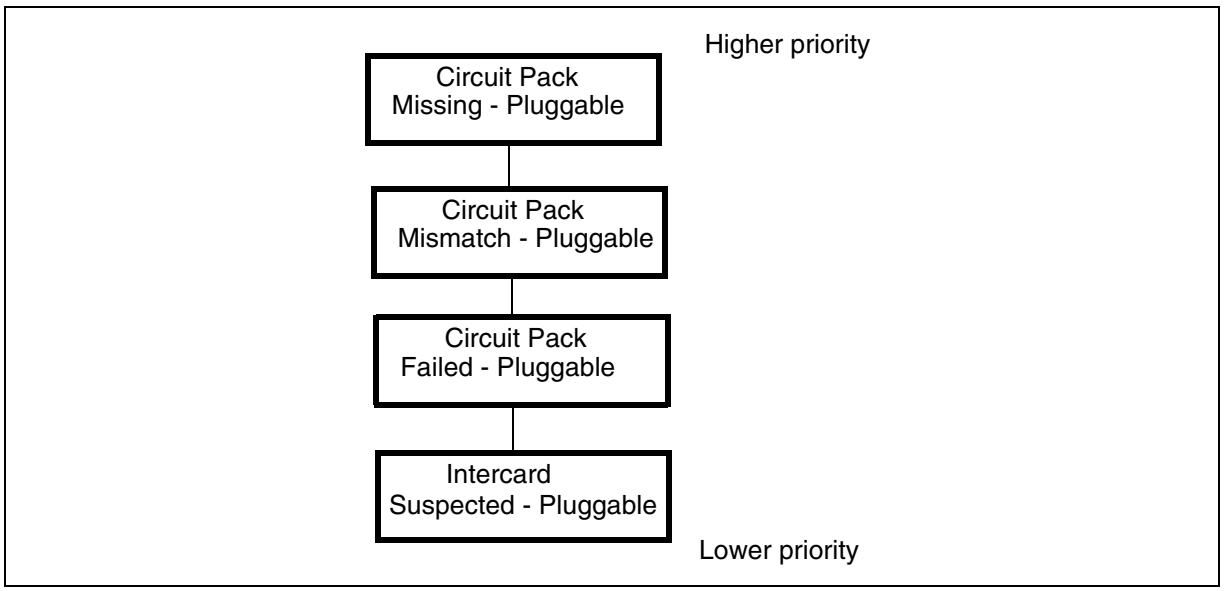
Equipment alarm hierarchy (modules)



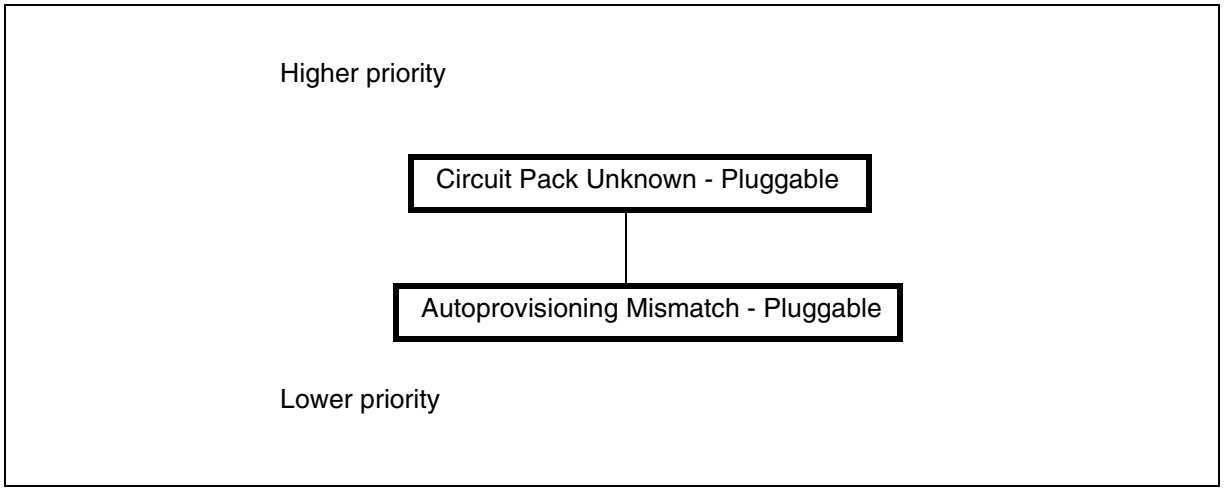
CTM alarm hierarchy



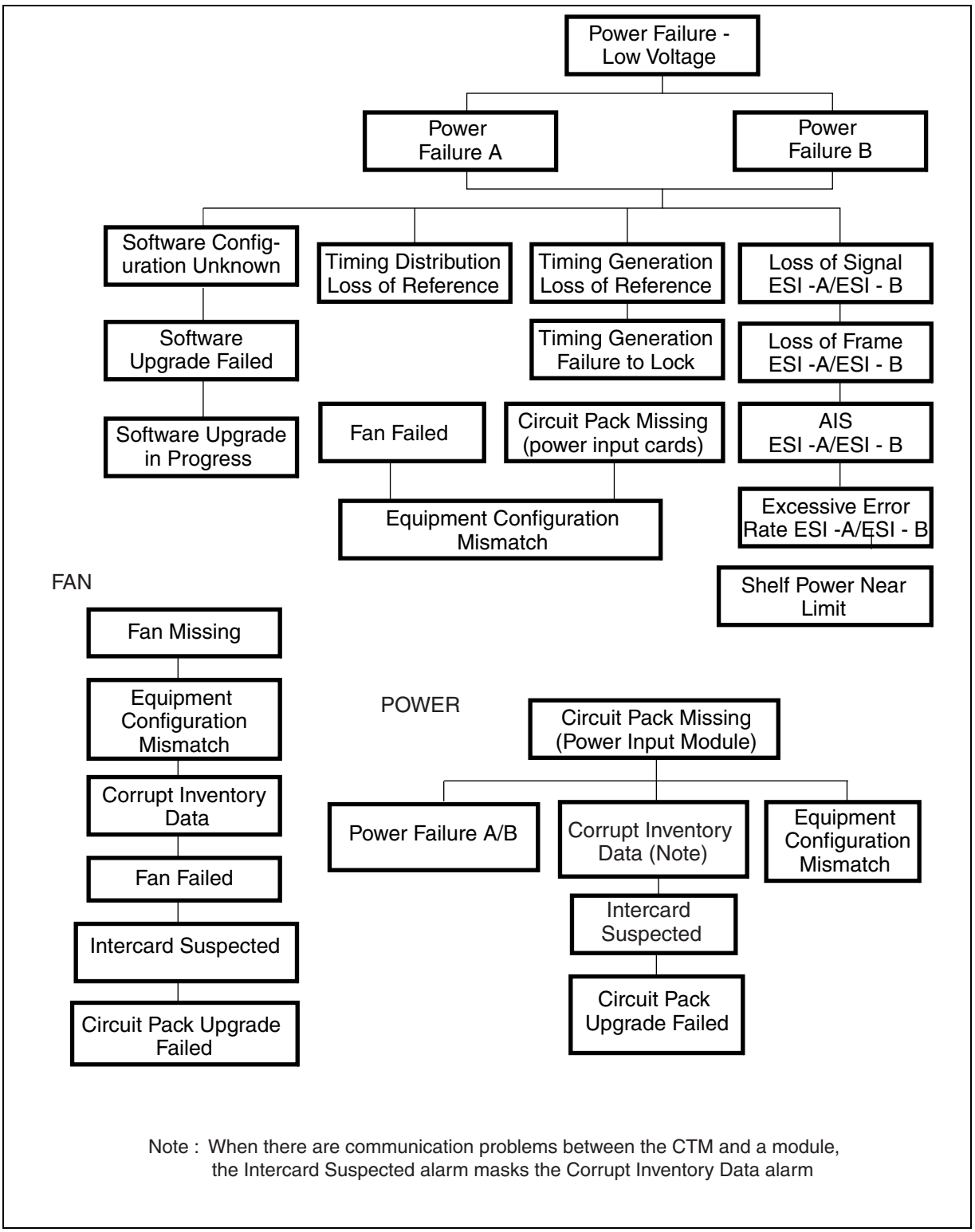
Equipment alarm hierarchy (provisioned pluggable transceivers)



Equipment alarm hierarchy (unprovisioned pluggable transceivers)

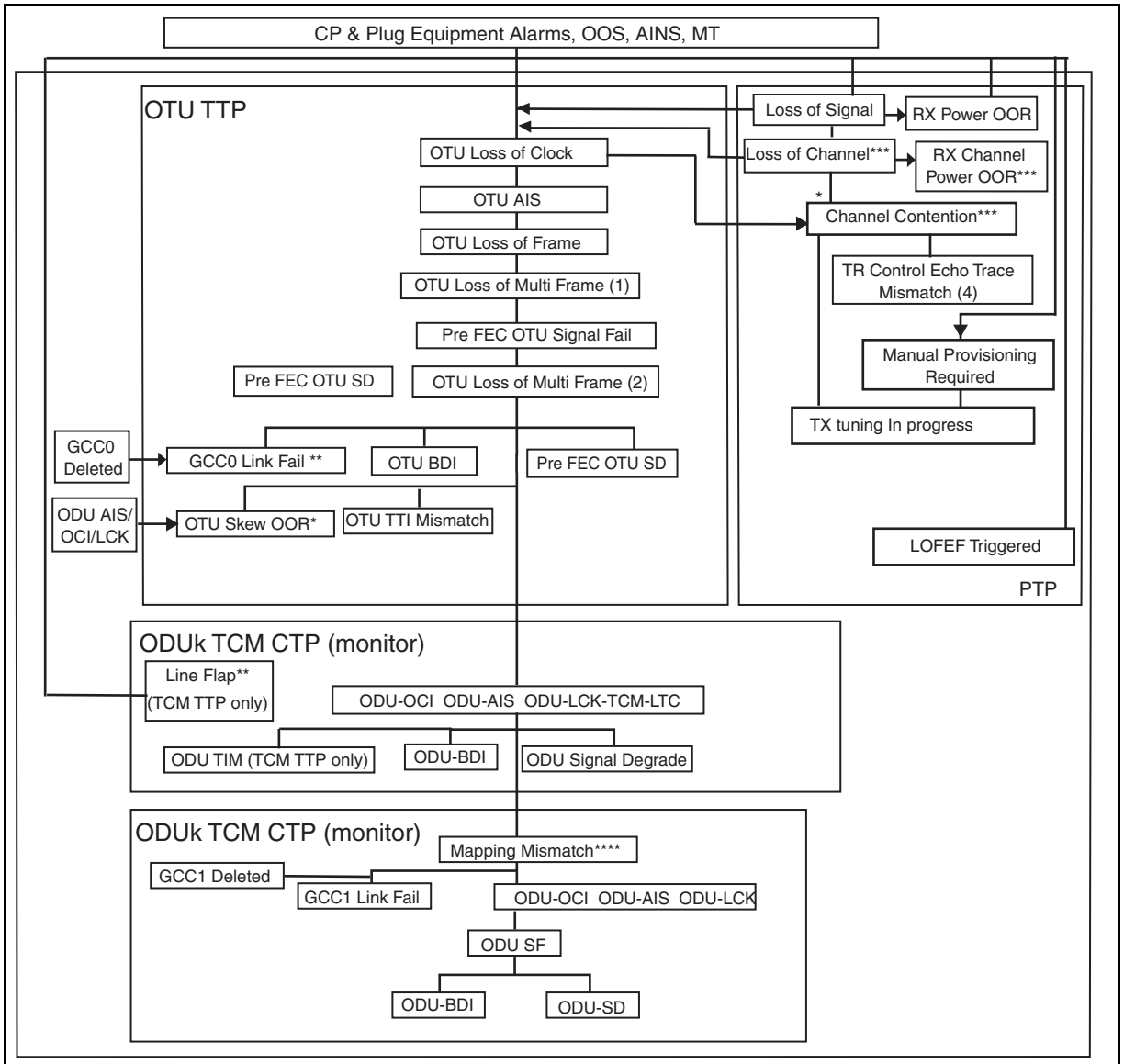


Shelf equipment alarm hierarchy



Note : When there are communication problems between the CTM and a module, the Intercard Suspected alarm masks the Corrupt Inventory Data alarm

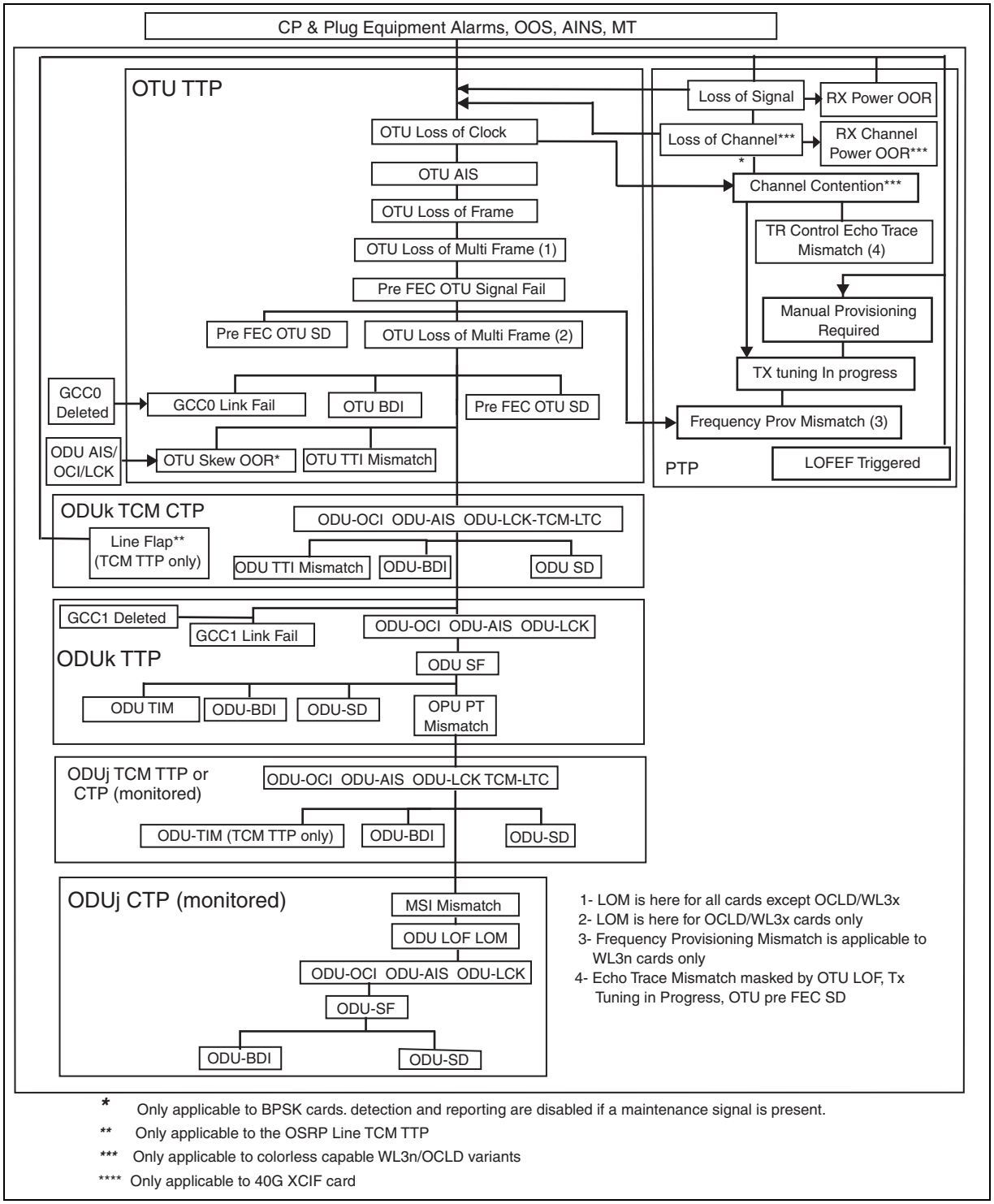
ODUk CTP OTN facility alarm hierarchy - faceplate to fabric direction (RX)



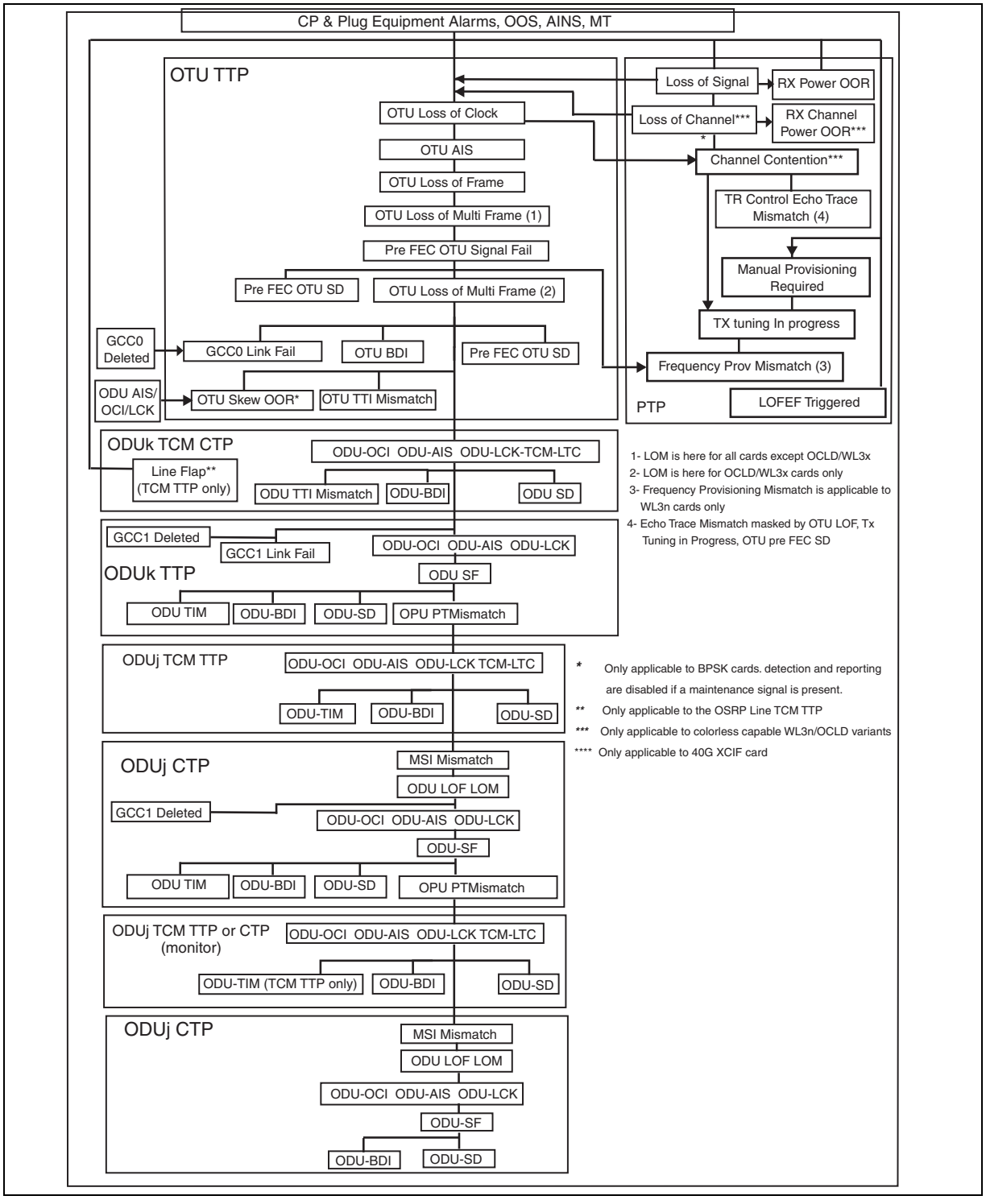
1- LOM is here for all cards except OCLD/WL3x
2- LOM is here for OCLD/WL3x cards only
3- Frequency Provisioning Mismatch is applicable to WL3n cards only
4- Echo Trace Mismatch masked by OTU LOF, Tx Tuning in Progress, OTU pre FEC SD

* Only applicable to BPSK cards. detection and reporting are disabled if a maintenance signal is present.
** Only applicable to the OSRP Line TCM TTP
*** Only applicable to colorless capable WL3n/OCLD variants
**** Only applicable to 40G XCIF card

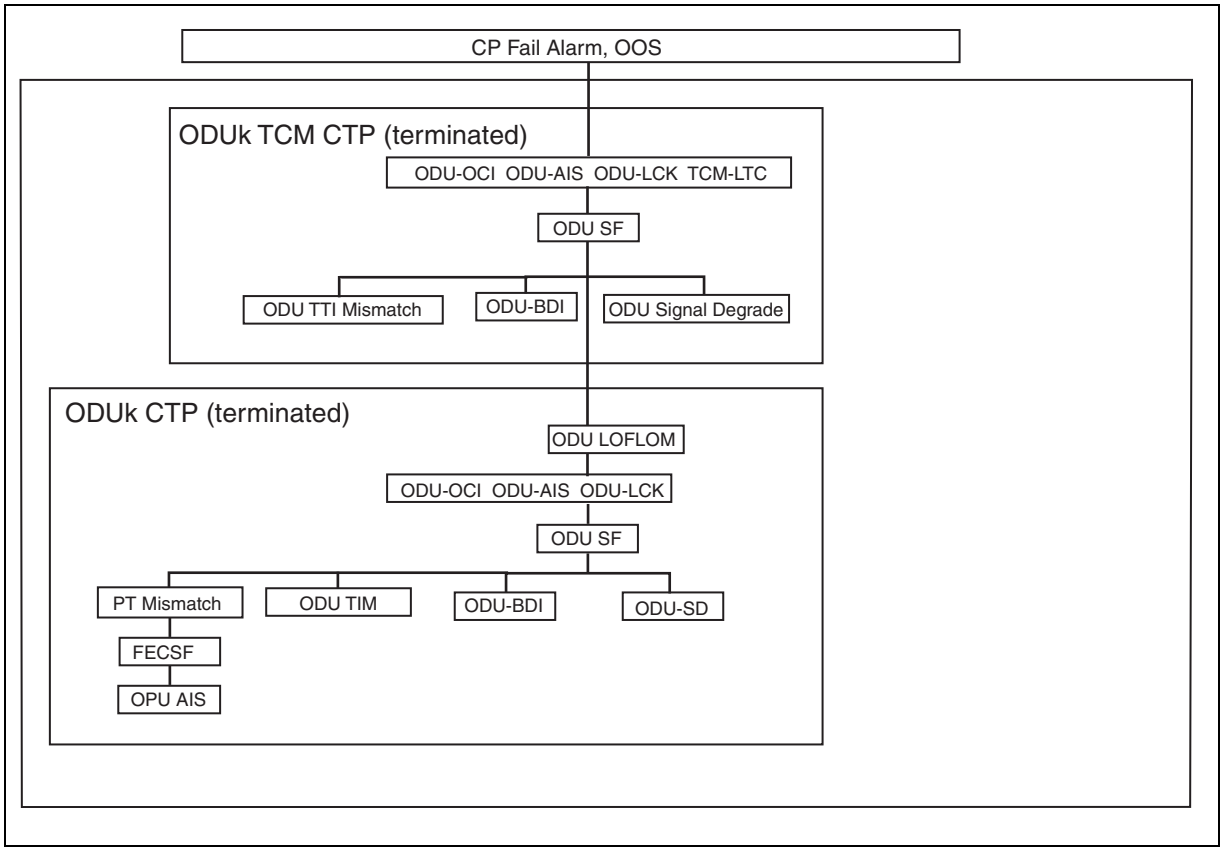
ODUj CTP OTN facility alarm hierarchy - faceplate to fabric direction (RX)



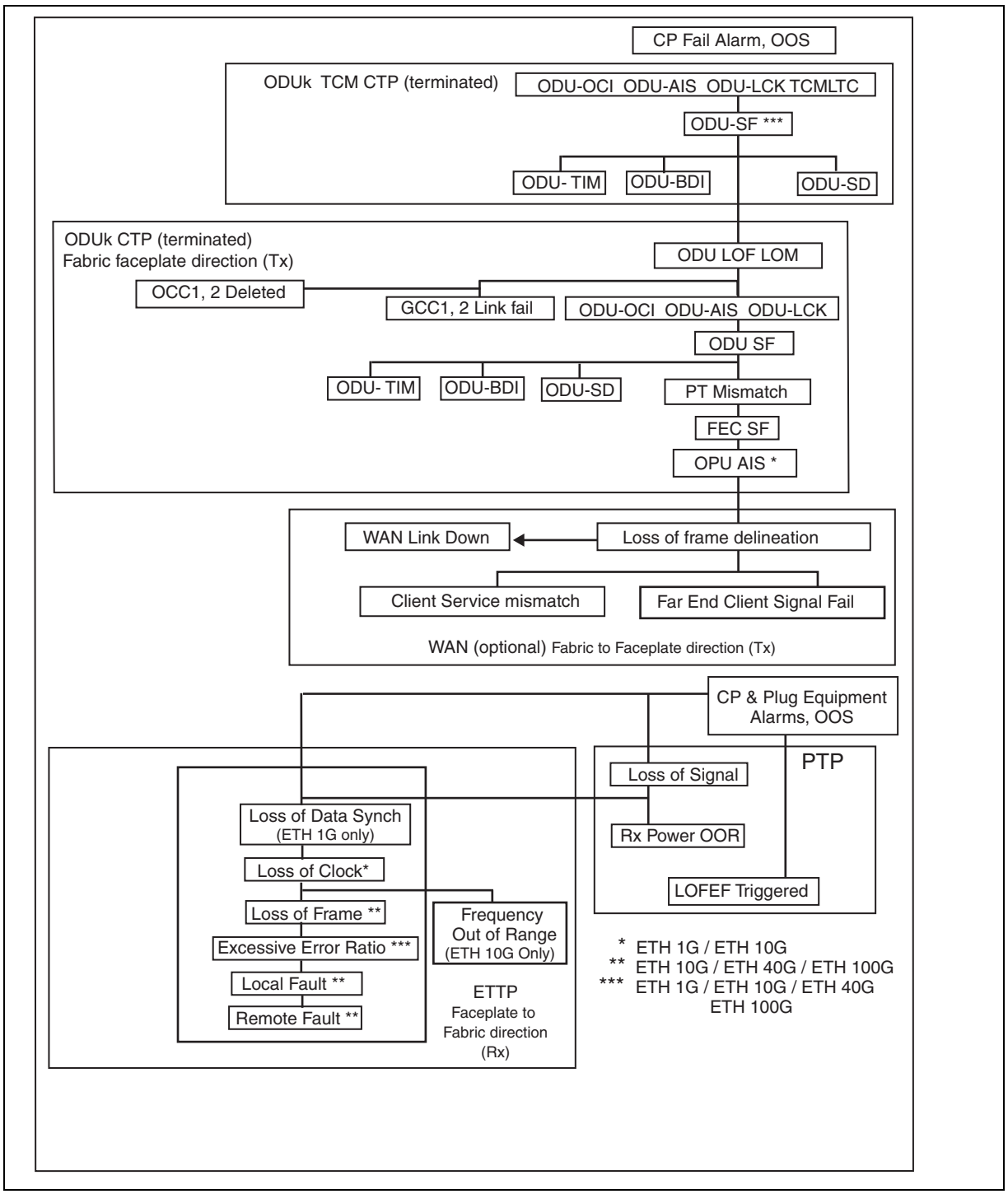
ODUi CTP OTN facility alarm hierarchy - faceplate to fabric direction (RX)



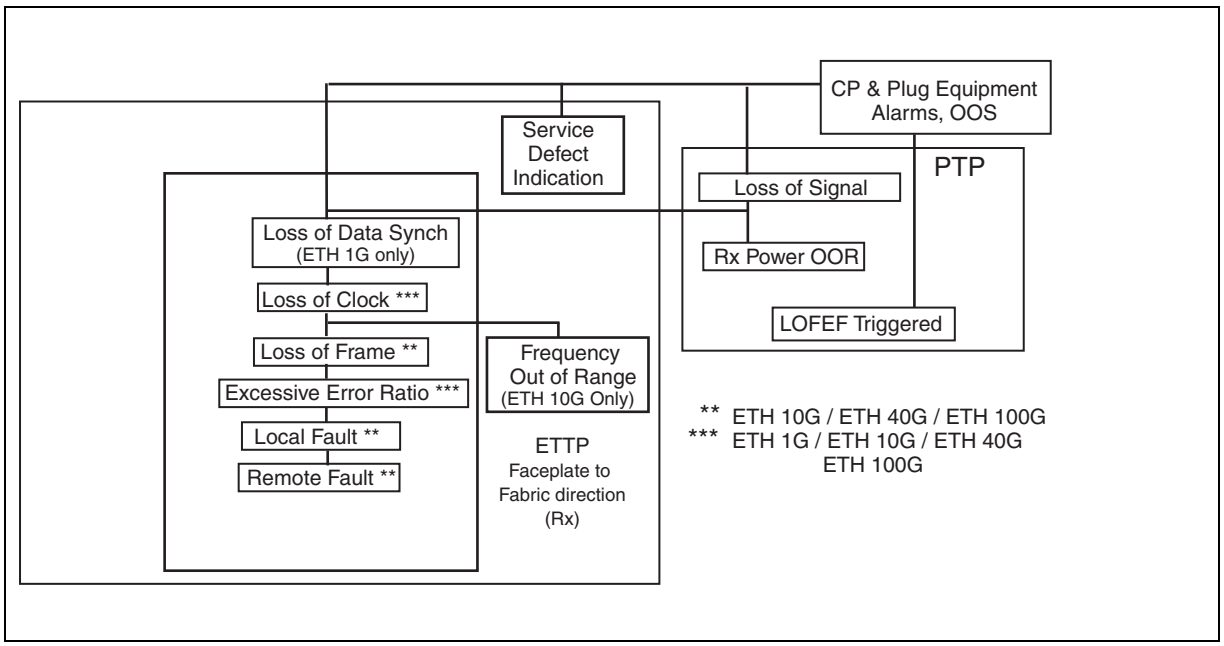
OTN facility alarm hierarchy - fabric to faceplate direction (TX)



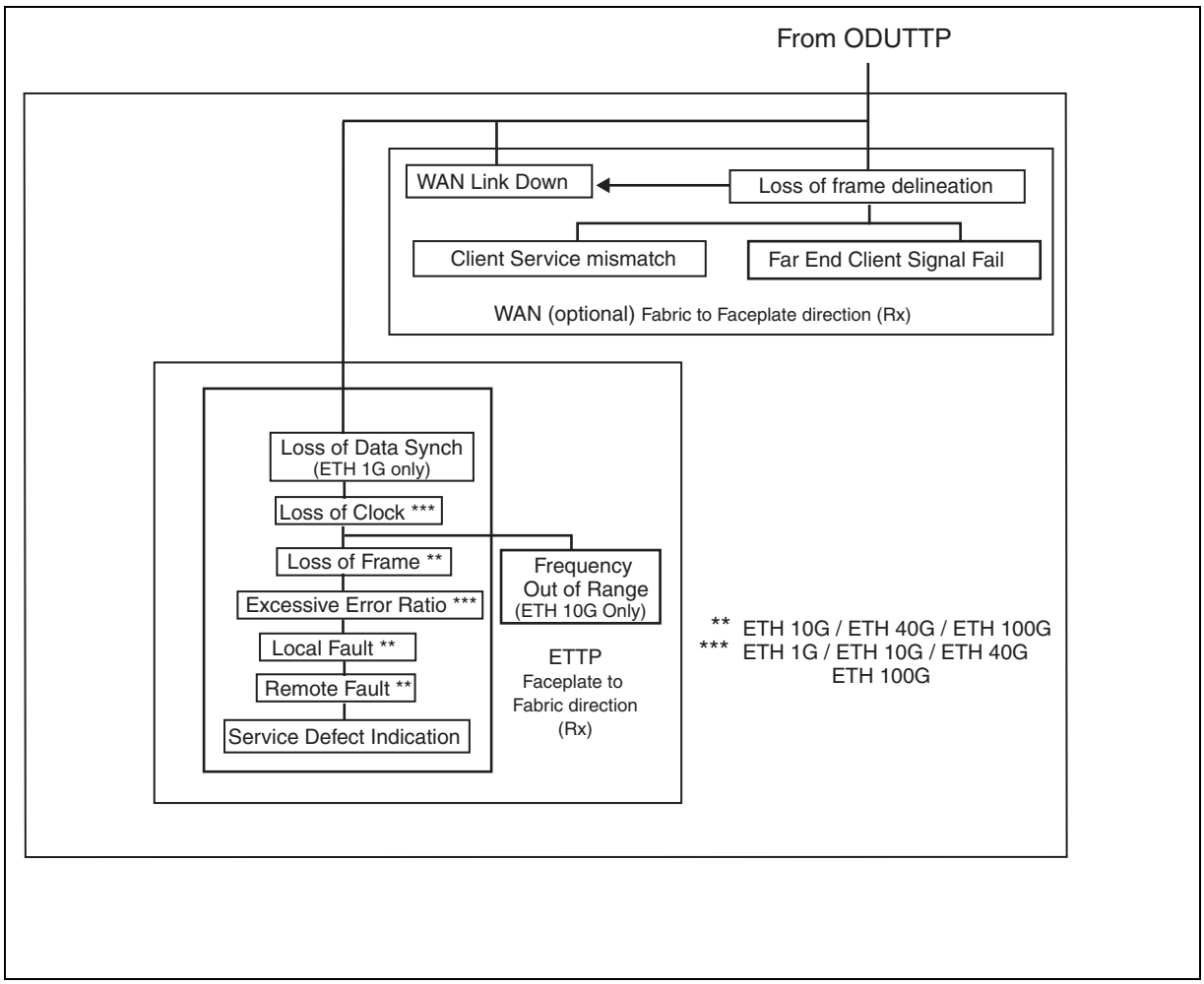
ETTP facility alarm hierarchy - monitored



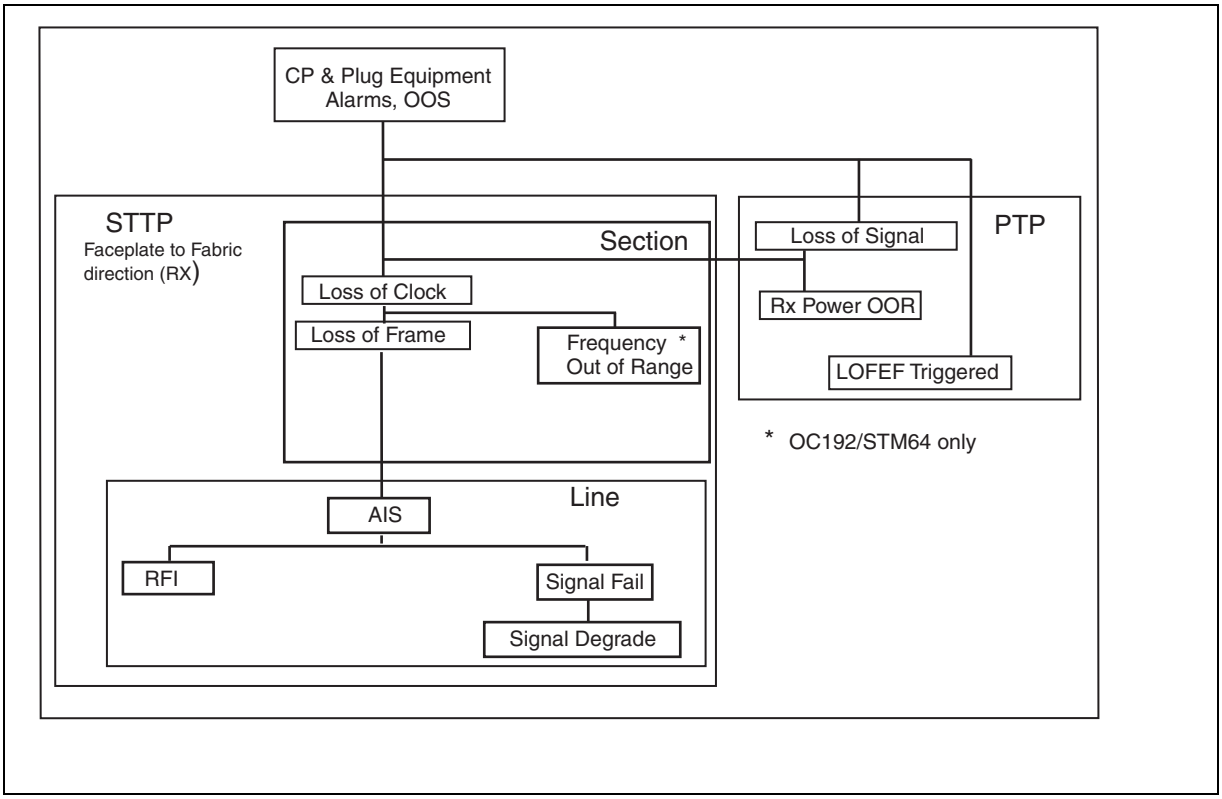
ETTP facility alarm hierarchy - terminated



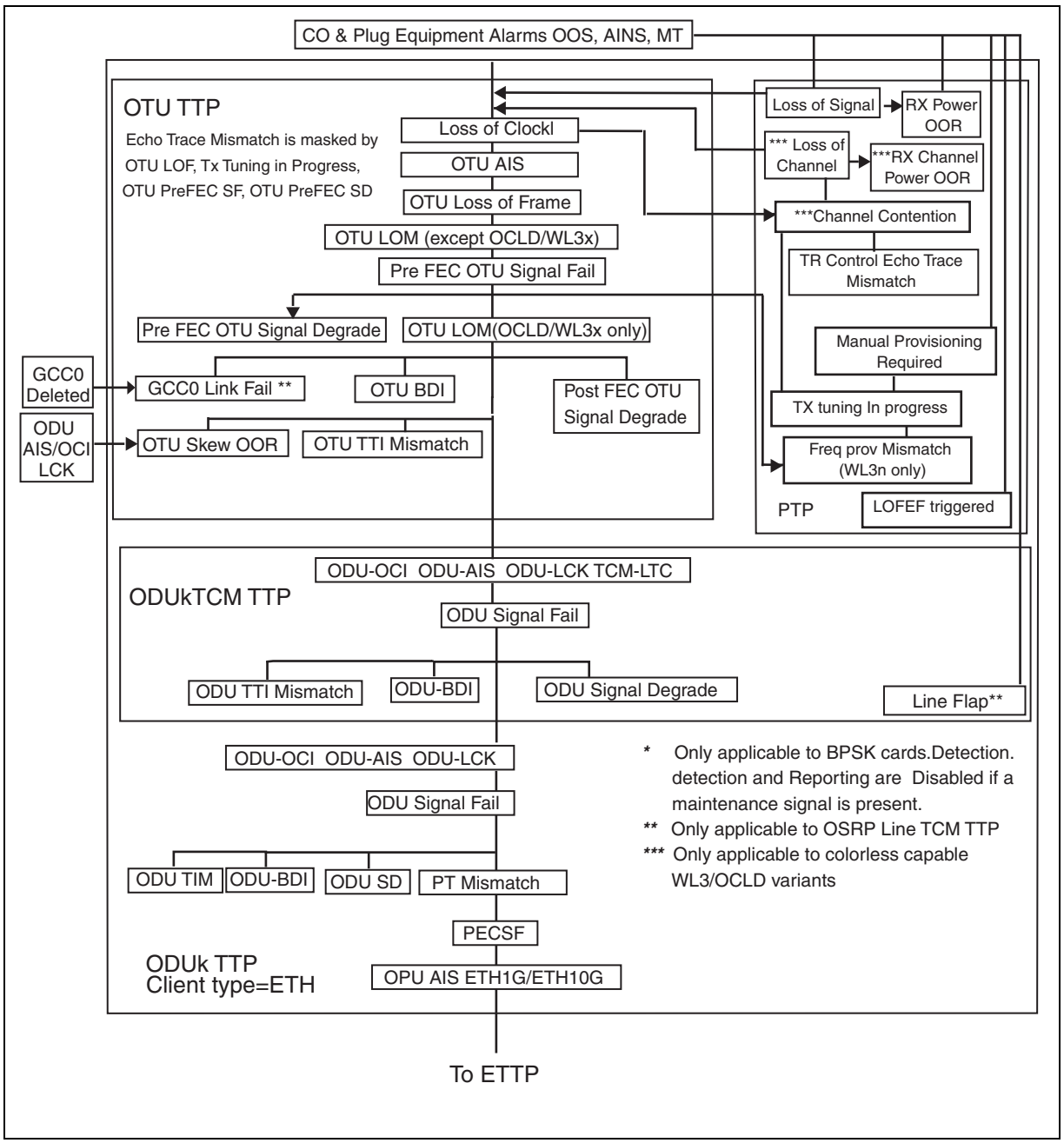
ETTP facility alarm hierarchy



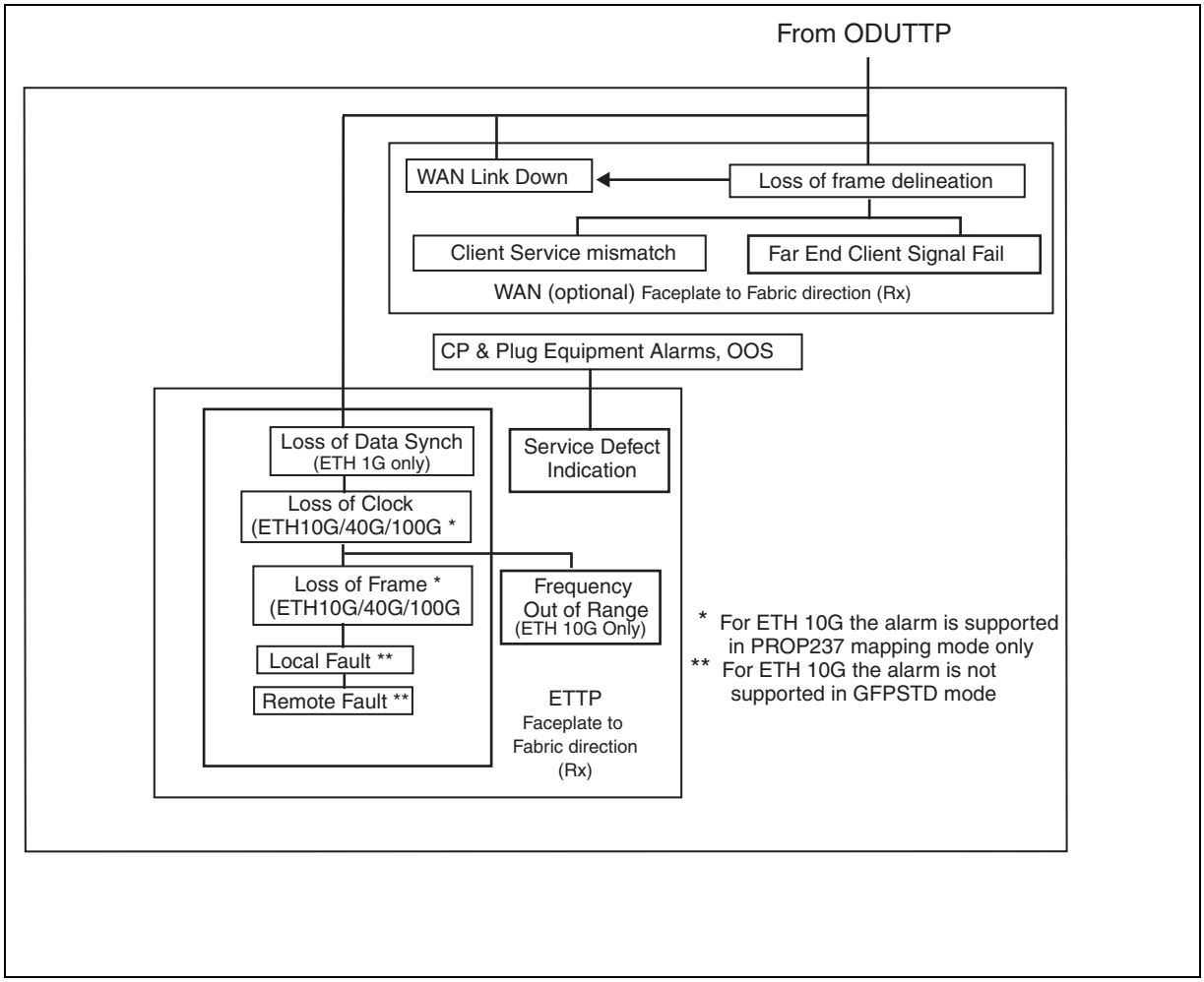
STTP facility alarm hierarchy



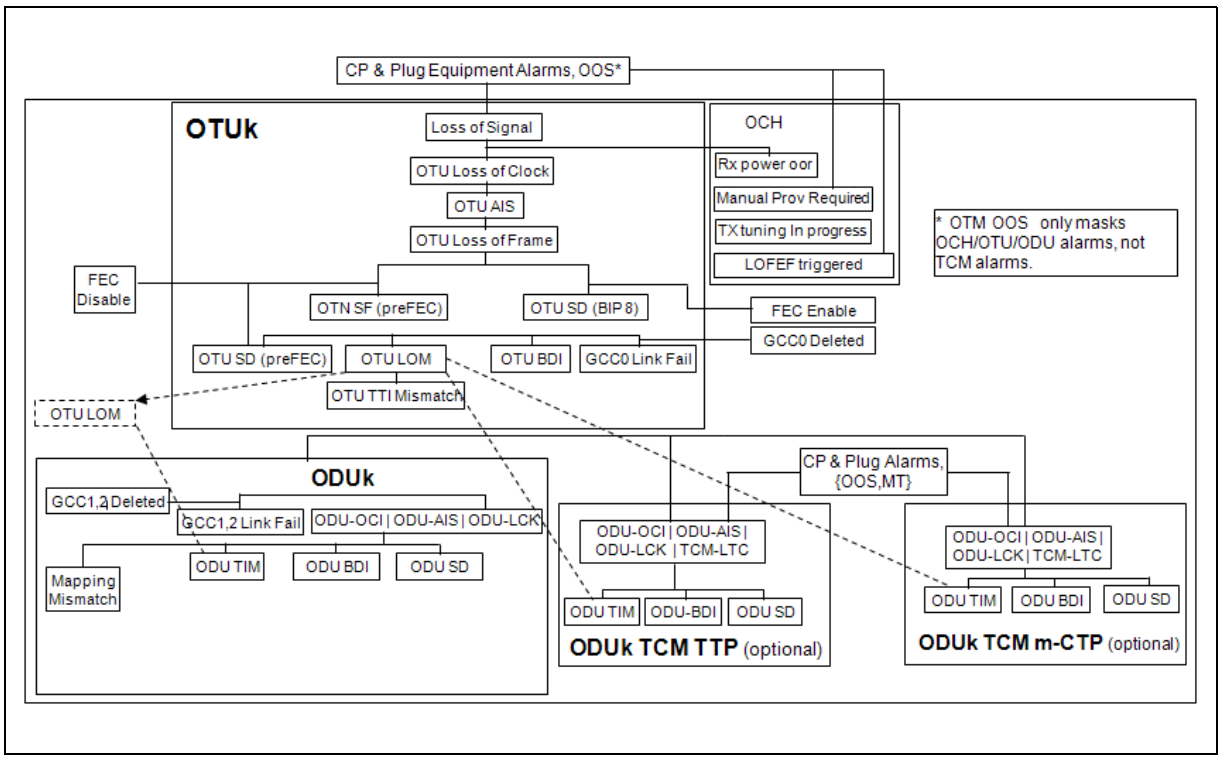
PKT facility alarm hierarchy - faceplate to fabric direction (RX)



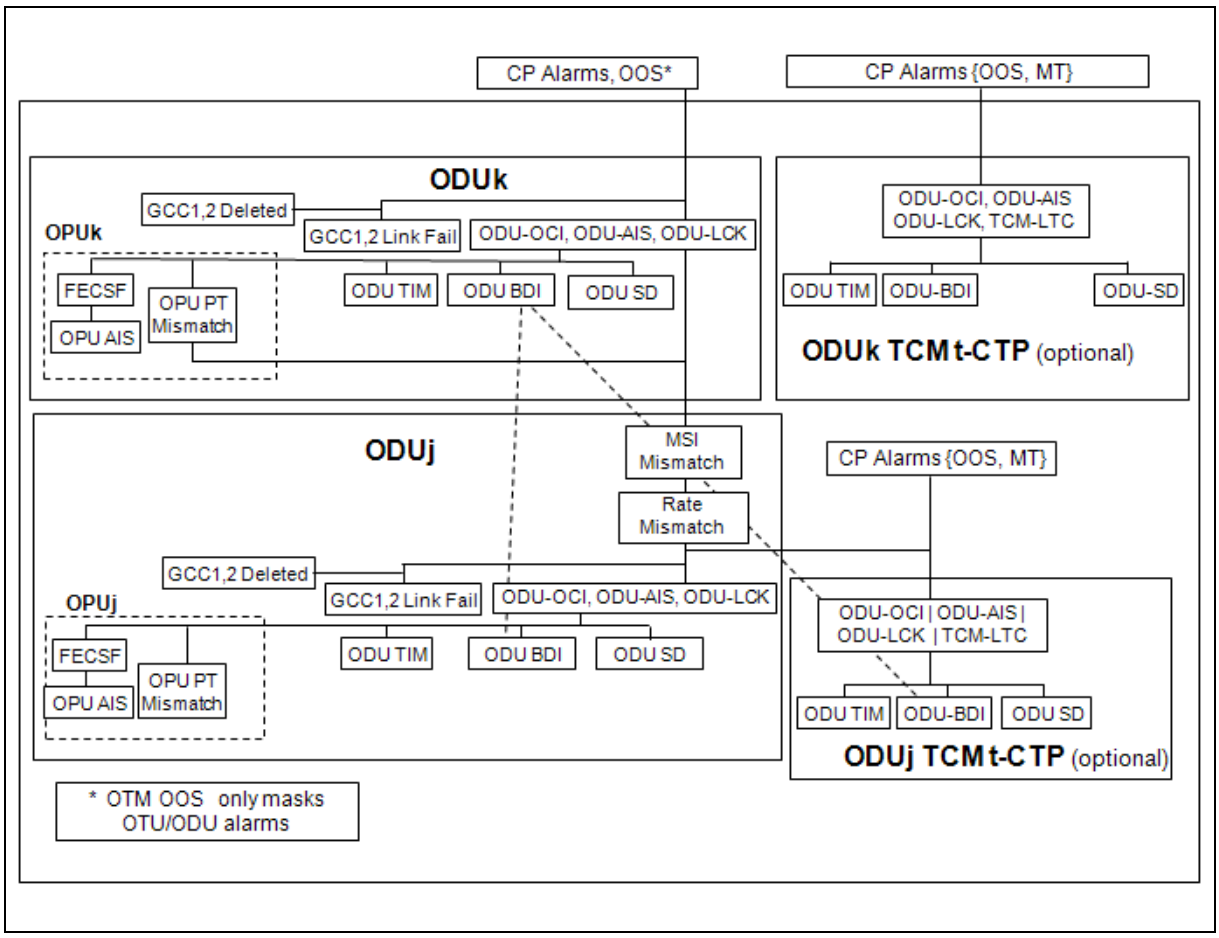
METTP facility alarm hierarchy



TCM facility alarm hierarchy - faceplate to backplane direction

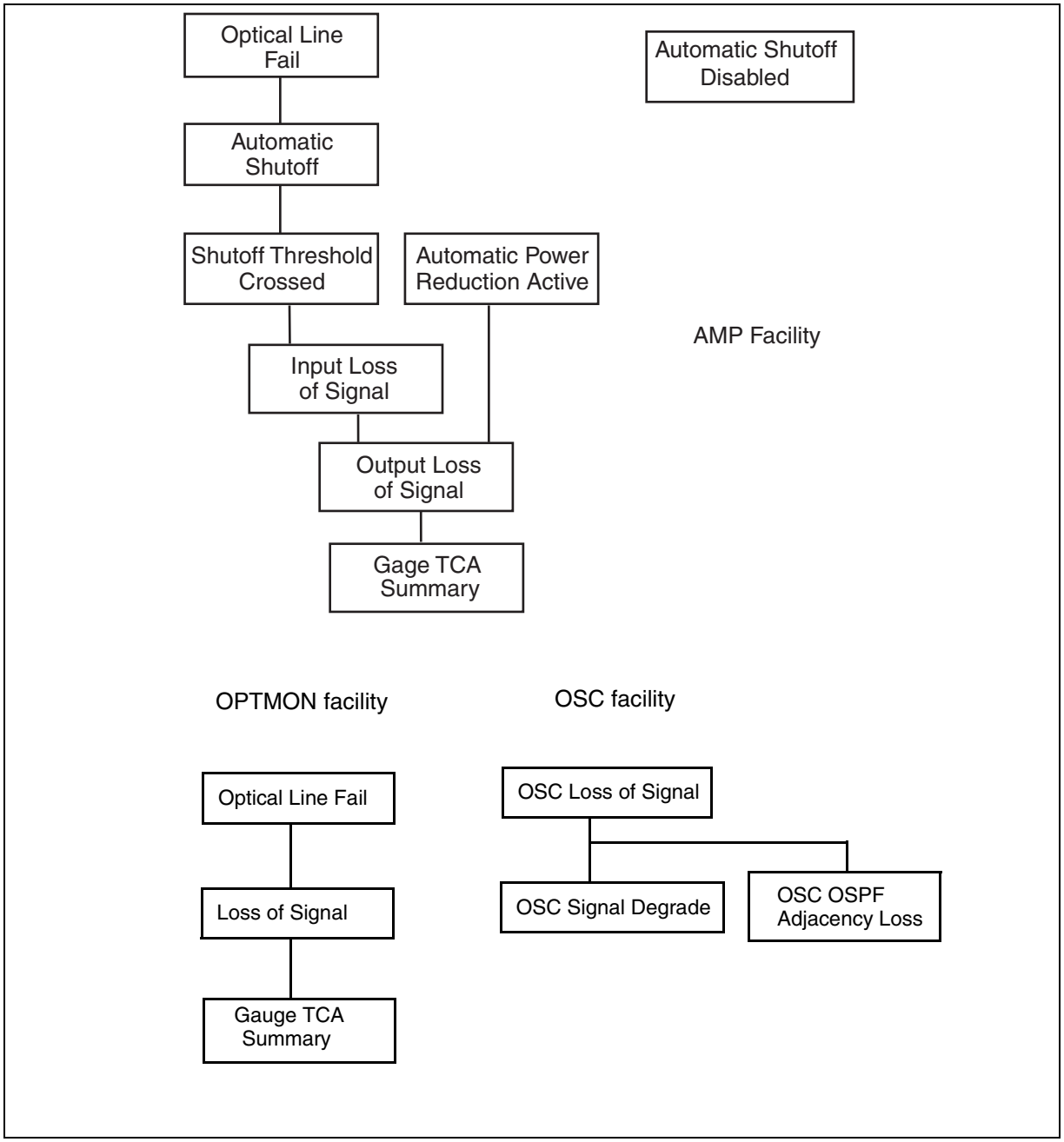


TCM facility alarm hierarchy - backplane to faceplate direction



Photonic optical signal facilities alarm hierarchy

Photonic facility alarms are masked by upstream facility failures.



Alarm clearing procedures—A to H

ATTENTION

The alarm clearing procedures are presented in two chapters, "Alarm clearing procedures—A to H" (this chapter) and Alarm clearing procedures—I to Z (in Part 2 of this document). The complete "List of alarms" is included in both chapters. The numbers in brackets after the alarm names are the alarm IDs.

This release of 6500 Packet-Optical Platform (6500) supports PKT/OTN I/F and Photonic modules. The combination of services is also supported.

For more information on the services (and the modules related to each service) offered in this release, refer to the *6500 - T_Series Shelves- Guide*, 323-1851-103.

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 in this document. Refer to the "List of alarms" on page 4-5 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
APS	Automatic Protection Switching
BDI	Backward Defect Indication
CDC	Colorless Directionless Contentionless

CFP2	C form-factor pluggable
CHMON	Channel Monitoring
CMF	Client Management Frame
CP	Circuit Pack
CPE	Customer Premise Equipment
CTM	Control timing module
CTMX	Control timing extender module
DCN	Data Communications Network
DIP	Dual In-line Package
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
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
NNS	Network Name Server
NSA	Non-Service-Affecting
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
OTN	Optical Transport Network
OTU	Optical Channel Transport Unit
PEC	Product Engineering Code
PIM	Power Input Module
PSI	Payload Structure Identifier
RLA	ROADM with Line Amplifier
ROADM	Re-configurable Optical Add-Drop Multiplexer
SA	Service-Affecting
SD	Signal Degrade
SETS	Synchronization Equipment Timing Source
SLAT	System Lineup and Test
SFP+	Small Form Factor Pluggable
SNCP	Subnetwork Connection Protection

SONET	Synchronous Optical Network
SPLI	Service Photonic Layer Interoperability
SPPC	Section Peak Power Controller
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
VC	Virtual Container
VCG	Virtual Concatenation Group
VCS	Virtual Circuit Segment
VT	Virtual Tributary
WAN	Wide Area Network
WSS w/OPM	Wavelength Selective Switch with Optical Power Monitor
WT	Wavelength Translator
XFP	10G transceiver form factor pluggable

Associated procedures

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

All procedures assume that you have logged into the network element. Refer to the “Interface login and logout” procedures in chapter 1 of *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 A to H are included in this chapter. Additionally, non-hyperlinked references to procedures beginning with I to Z (included in Part 2 of this document) are provided here.

D

E

F

G

H

I

ILAN-OUT Port Failure, see Part 2 of this document
Incomplete Software Lineup, see Part 2 of this document
Input Loss of Signal, see Part 2 of this document
Integrated Test Set Configured, see Part 2 of this document
Integrated Test Set Data Save In Progress, see Part 2 of this document
Intercard Suspected, see Part 2 of this document
Intercard Suspected - Pluggable, see Part 2 of this document
Internal Database Synch in Progress, see Part 2 of this document
Internal Mgmt Comms Suspected, see Part 2 of this document
Intrusion Attempt, see Part 2 of this document
Invalid Site Topology, see Part 2 of this document

L

LACP Failed, see Part 2 of this document
LAN alarms, see Part 2 of this document
Line Flapping, see Part 2 of this document
LINE/MS DCC OSPF Adjacency Loss, see Part 2 of this document
Link Down, see Part 2 of this document
Lockout Active, see Part 2 of this document
Log Collection In Progress, see Part 2 of this document
Log Save In Progress, see Part 2 of this document
Loopback Active, see Part 2 of this document
Loopback Active - Facility, see Part 2 of this document
Loopback Active - Terminal, see Part 2 of this document
Loopback Traffic Detected, see Part 2 of this document
Loss of Alignment - VCAT, see Part 2 of this document
Loss of Channel, see Part 2 of this document
Loss of Clock, see Part 2 of this document
Loss of Control Infrastructure, see Part 2 of this document
Loss of Data Synch, see Part 2 of this document
Loss of Extra Traffic, see Part 2 of this document
Loss Of Frame (OTUTTP, ETTP, STTP), see Part 2 of this document
Loss of Frame Delineation, see Part 2 of this document
Loss Of Multiframe (OTUTTP), see Part 2 of this document

Loss of Signal (OPTMON, VOA), see Part 2 of this document

Loss of Switch Fabric Redundancy, see Part 2 of this document

Low Optical Return Loss at Input, see Part 2 of this document

Low Optical Return Loss at Output, see Part 2 of this document

Low Order Bandwidth Near Limit, see Part 2 of this document

Low Received Span Loss, see Part 2 of this document

M

MAC Status Defect, see Part 2 of this document

Manual Area Address Dropped, see Part 2 of this document

Manual Switch Active, see Part 2 of this document

Member Shelf Mismatch, see Part 2 of this document

Member Shelf Unknown, see Part 2 of this document

Member Shelf Unreachable, see Part 2 of this document

Minimum Gain, see Part 2 of this document

MSI Mismatch (ODUCTP), see Part 2 of this document

N

Number of Level 1 NEs Exceeded, see Part 2 of this document

O

OCH Link Data Retrieval In Progress, see Part 2 of this document

OCH Link Data Save In Progress, see Part 2 of this document

ODU AIS (ODUTTP, ODUCTP), see Part 2 of this document

ODU BDI (ODUTTP, ODUCTP), see Part 2 of this document

ODU LCK (ODUTTP, ODUCTP), see Part 2 of this document

ODU Loss of Frame and Multiframe (ODUTTP, ODUCTP), see Part 2 of this document

ODU OCI (ODUTTP, ODUCTP), see Part 2 of this document

ODU Signal Degrade (ODUTTP, ODUCTP, TCM), see Part 2 of this document

ODU Signal Fail (ODUTTP, ODUCTP), see Part 2 of this document

ODU/OTU Trace Identifier Mismatch, see Part 2 of this document

Optical Line Fail, see Part 2 of this document

Optimization Scanning in Progress, see Part 2 of this document

OPU AIS (ODUTCTP, ETTP, STTP), see Part 2 of this document

OPU Payload Type Mismatch, see Part 2 of this document

P

Provisioning Incompatible - Pluggable, see Part 2 of this document

R

Redundant Database Synch Failed, see Part 2 of this document

Redundant Database Synch Failed - CP, see Part 2 of this document

Redundant Database Synch in Progress, see Part 2 of this document

Redundant Release Synch Failed, see Part 2 of this document

Redundant Release Synch in Progress, see Part 2 of this document

Release Server Mismatch, see Part 2 of this document

Release Server URL Fail, see Part 2 of this document

Remote Defect Indication, see Part 2 of this document

Remote Fault (ETTP), see Part 2 of this document

Remote Node Unreachable, see Part 2 of this document

Remote Port OOS, see Part 2 of this document

Remote Port Unreachable, see Part 2 of this document

RFI (STTP), see Part 2 of this document

Ring Protection Exerciser Fail, see Part 2 of this document

Rollover in Progress, see Part 2 of this document

Root Directory Has Reached Maximum File Entry Limit, see Part 2 of this document

Rx Channel Power Out of Range, see Part 2 of this document

Rx Power Out of Range, see Part 2 of this document

S

Secondary RADIUS Accounting Server Unavailable, see Part 2 of this document

Secondary RADIUS Server Unavailable, see Part 2 of this document

Secondary Service Failed, see Part 2 of this document

Secondary SETS Locking to Primary, see Part 2 of this document

SECTION/RS DCC OSPF Adjacency Loss, see OSPF Adjacency Loss alarms in Part 2 of this document

Service Defect Indication, see Part 2 of this document

Shelf Bandwidth Near Limit, see Part 2 of this document

Shelf Data Missing, see Part 2 of this document

Shelf Power Near Limit, see Part 2 of this document

Shutoff Threshold Crossed, see Part 2 of this document

Signal Degrade (STTP), see “Error alarms (STTP)” on page 4-173

Signal Fail (STTP), see “Error alarms (STTP)” on page 4-173

Signal Fail (STTP), see Part 2 of this document

Slot Sequence Provisioning Incomplete, see Part 2 of this document

SNC Datapath Fault, see Part 2 of this document

SNC Takeover Failed, see Part 2 of this document

SNC Unavailable, see Part 2 of this document

SNMP Proxy Config Failed on Member, see Part 2 of this document

SNMP Proxy Trap Config Failed on Member, see Part 2 of this document

SNMP Proxy Config Failed on Primary, see Part 2 of this document

Software Auto-Upgrade in Progress, see Part 2 of this document

Software Configuration Unknown, see Part 2 of this document

Software Delivery Incomplete, see Part 2 of this document

Software Delivery In Progress, see Part 2 of this document

Software Mismatch, see Part 2 of this document

Software Upgrade Failed, see Part 2 of this document

Software Upgrade in Progress, see Part 2 of this document

Span Protection Exerciser Fail on page 5-393

Synchronization Protection alarms, see Part 2 of this document

T

TCM Loss of Tandem Connection, see Part 2 of this document

Telemetry Loss of Signal, see Part 2 of this document

Test Access in Progress alarms, see Part 2 of this document

Threshold AIS ESO-A/ESO-B, see Part 2 of this document

Time Out, see Part 2 of this document

Timing Distribution Forced Switch - n Ref, see Part 2 of this document

Timing Distribution Lockout - n Ref, see Part 2 of this document

Timing Distribution Loss of Reference - n Ref, see Part 2 of this document

Timing Generation Entry to Freerun, see Part 2 of this document

Timing Generation Entry to Holdover, see Part 2 of this document

Timing Generation Failure To Lock, see Part 2 of this document

Timing Generation Forced Switch - n Ref, see Part 2 of this document

Timing Generation Lockout - n Ref, see Part 2 of this document

Timing Generation Loss of Reference - n Ref, see Part 2 of this document
TOD Server Not Provisioned, see Part 2 of this document
Topology Build Failed, see Part 2 of this document
Transport Data Recovery Failed, see Part 2 of this document
TR Control Disabled, see Part 2 of this document
TR Control Echo Trace Mismatch, see Part 2 of this document
TR Control Initialization in Progress, see Part 2 of this document
TR Control IS Optimization in Progress, see Part 2 of this document
Tx Manual Provisioning Required, see Part 2 of this document
Tx Partial Loss of Capacity - LCAS, see Part 2 of this document
Tx Power Out of Range, see Part 2 of this document
Tx Tuning in Progress, see Part 2 of this document

U

Unable to Synchronize TOD, see Part 2 of this document
Unassigned Channel Detected, see Part 2 of this document
Unequipped, see Part 2 of this document
Unpaired SSH Key, see Part 2 of this document

V

VOA Output LOS, see Part 2 of this document

W

WAYSIDE 1/2 Port Failure, see Part 2 of this document

Procedure 4-1
1+1 APS alarms

Protection Channel Match Fail

Alarm ID: 1747

Probable cause

This alarm is raised when:

- the received channel ID on the protection interface module is not as expected. This is normally because of a failure in the interface module.
- the automatic protection switching (APS) communications protocol between the two optical interfaces is not working because the optical fiber is not connected to the correct slot at either end
- the protection engine does not receive APS bytes from the far-end
- the protection engine receives invalid APS bytes from the far-end

This alarm is only raised on the OTN 1+1 line-side protection configurations.

Impact

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

Protection Switch Byte Fail

Alarm ID: 1391

Probable cause

This alarm is raised when the received channel protection switching control bytes (APS bytes) on the protection interface module are not valid codes. This is normally because of a failure in the interface module or crossed fibers.

This alarm is raised on OTN 1+1 line-side protected configurations.

Impact

Major, 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 - 6500-T Series Shelves*, 323-1851-201.6
- have the optical fiber connection information (that is, how the optical modules on each network element connect to other network elements

Procedure 4-1 (continued)
1+1 APS alarms

Step	Action
1	Identify the interface module raising the alarm. Refer to the Procedure 2-12, "Identifying the module, pluggable module/port, or facility that has raised an alarm" on page 2-31.
2	Identify the protection provisioning on the module raising the alarm. Ensure that the protection scheme is OTN 1+1 line-side. Refer to the "Retrieving protection parameters" procedure in Part 1 of *Configuration - Provisioning and Operating*, 323-1851-311. If the protection is not OTN 1+1 line-side, contact your next level of support or your Ciena support group.
3	Identify the protection provisioning on the far-end. Ensure that the protection scheme is OTN 1+1 line-side. If the same alarm appears at the other end, two fibers have been swapped. If a different alarm condition exists at the far-end, investigate the alarm to identify and localize the fault.
4	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.

If the original alarm was	**Then** go to
Protection Channel Match Fail	step 5
Protection Switch Byte Fail	step 7

5	Verify that the optical fibers/cables are connected to the correct ports at each node. The working port of the protection pair at the near-end must be fibered to the working port of the protection pair at the remote end. The protection port of the protection pair at the near-end must be fibered to the protection port of the protection pair at the remote end. Use TTI to identify fiber connectivity. Refer to the "Retrieving and editing trail trace messages" procedure in Part 1 of *Configuration - Provisioning and Operating*, 323-1851-311.

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

7	Replace the interface module raising the alarm. Refer to the equipment replacement procedures in *Fault Management - Module Replacement for T-Series*, 323-1851-546. Select the appropriate procedure from the "Module replacement procedures list" table. Wait 30 seconds.

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

Procedure 4-1 (continued)
1+1 APS alarms

Step	Action
9	Use the optical fiber connection information to determine the network element and interface module on the far-end of the optical fiber link.
10	Replace the remote interface module. Refer to the equipment replacement procedures in *Fault Management - Module Replacement for T-Series*, 323-1851-546. Select the appropriate procedure from the “Module replacement procedures list” table.
11	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 4-2
Adjacency Discovery Unreliable

Alarm ID: 1072

Probable cause

This alarm is raised when a remote shelf that the SPLI feature is tracking has not communicated (UDP) with the SPLI application for more than 10 minutes. This can occur:

- if the remote shelf has changed their SiteID or TID
- if the remote shelf is isolated from the network
- if the remote shelf is constantly restarting

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 a network plan or other documents that allow you to determine the SPLI connectivity
- observe all safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - General Information, 323-1851-201.0*

Step	Action
1	Determine which shelves are unreliable using the **SPLI** tab in the **Node Information** application. Find the nodes and shelves with a status of Unreliable. Refer to the “Displaying node information” procedure in *Administration and Security*, 323-1851-301, for more information about the **Node Information** application.
2	Verify whether the TID or siteID has changed on those nodes. If changes have been made, change the TID or siteID of those nodes back to the original ones if necessary.
3	If changes have not been made, verify that comms are working correctly by logging into the network element.
4	Click the **Refresh** button in the **SPLI** tab of the **Node Information** window to retrieve the latest statuses.

Procedure 4-2 (continued)
Adjacency Discovery Unreliable

Step	Action
5	If SPLI is not matching all the TID-shelves that are listed as unreliable, click on the **Delete** button. This will remove all the unreliable entries from the table.

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

7	Contact your next level of support or your Ciena support group.

—end—

Procedure 4-3
Adjacency Far End Not Discovered

Alarm ID: 538

Probable cause

This alarm is raised against an ADJ-LINE facility or the MPO ADJ facility when the adjacency cannot be automatically discovered from the far-end. Possible reasons for this far-end adjacency not being discovered include:

- the two adjacency end points have not been fibered
- the two adjacency end points have been fibered but some other problem exists with the fiber or connection
- there is a comms provisioning error, where the TID-level comms circuit is incorrectly provisioned or not provisioned at one or both ends of the alarmed span
- an upstream network element has undergone a restart operation. The alarm will clear once the restart completes
- fibers at the Line AMP NE are swapped (misconnected/crossed)
- the ADJ-LINE Expected Far End Address is incorrectly provisioned
- the appropriate OSC is not provisioned in the OTS or in the OTS Slot Sequence or is not functioning correctly
- the TIDC/IP is not provisioned

In the case of a line adjacency, the discovered provisioned expected far-end address is the Photonics module at the other end of the fiber span.

For CDC connection validation, this alarm is raised against the CCMD16x12 or AMP4 MPO adjacency facility if there is a provisioned (or derived) adjacency and no discovered adjacency. This alarm is not supported for adjacency facilities that have FEA pointing to themselves. (for example, MPO loopback connector on the port).

The alarm is masked by:

- local Circuit Pack Missing or Circuit Pack Mismatch
- remote Circuit Pack Missing or Circuit Pack Mismatch
- if there is no ADJ EFEA

Impact

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

Procedure 4-3 (continued)
Adjacency Far End Not Discovered

Prerequisites

To perform this procedure, you must:

- use an account with at least a level 3 UPC
- observe all safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - 6500-T Series Shelves*, 323-1851-201.6
- have a fiber cleaning kit (for a CDC configuration, an MPO cleaning kit is needed. See the “Cleaning connectors” chapter in *Installation - 6500-T Series Shelves*, 323-1851-201.6)
- have the engineering documentation package (EDP) for shelf details

Step	Action
1	Verify and correct the adjacency provisioning information as required. Refer to the “Editing facility parameters” procedure in Part 1 of *Configuration - Provisioning and Operating*, 323-1851-311.
2	If applicable, check the OSC facility states and confirm provisioning of the OSC in the OTS or in the Slot Sequence.
3	**If** the original alarm has / **Then** cleared / the procedure is complete not cleared / go to step 4

Procedure 4-3 (continued)
Adjacency Far End Not Discovered

Step	Action	
4	**If** this adjacency	**Then**
	is fibered, but a fiber break, reflective event, or disconnect is suspected	go to step 5
	was provisioned for future use, and you do not want this alarm to be displayed in the active alarm list	disable this alarm so that it no longer appears in the active alarms list. Refer to the Procedures for alarm provisioning and alarm profiles in chapter 2 of this document.
	was provisioned for future use and you want this alarm to be displayed in the active alarms list for informational purposes	no action is required. The procedure is complete.
	requires fibering	fiber the adjacency end points. Refer to the EDP. For logical port mappings for CCMD8x16 ports and WSS MPO ports connected to FIM, refer to “Connecting or disconnecting fiber-optic cables to or from IMs or FIMs” procedure in *Installation - 6500-T Series Shelves*, 323-1851-201.6.
5	Clear any alarms that indicate a fiber break or disconnect, such as: • Automatic Power Reduction Active • Automatic Shutoff • Input Loss of Signal • Loss of Signal (OPTMON) • Optical Line Fail	
6	Verify the fibers at the Line AMP NE or MPO Adjacency facility for any reversed fiber connections and correct if necessary.	
7	Verify that the provisioned values for ADJ-LINE Expected Far End Address Format or Expected Far End Address are correct.	
8	Edit the provisioned values as appropriate to correct the expected values. Refer to the “Editing facility parameters” procedure in Part 1 of *Configuration - Provisioning and Operating*, 323-1851-311. For CDC MPOs, edit the TID slot sequence to change the ADJ EFEA of the MPO. Refer to the “Editing TID slot sequences” procedure in Part 2 of *Configuration - Provisioning and Operating,* 323-1851-311.	

Procedure 4-3 (continued)
Adjacency Far End Not Discovered

Step	Action
9	Check for and clean any dirty fibers. Refer to the “Cleaning connectors” chapter in *Installation - 6500-T Series Shelves*, 323-1851-201.6.
10	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 4-4
Adjacency Mismatch

Alarm ID: 539

Probable cause

This alarm is raised against an ADJ-LINE facility when the **Expected far-end address** parameter of the line adjacency is manually provisioned, but does not match the discovered address (**Actual Far End Address**) listed for the ADJ-LINE facility.

If the provisioned information is correct, mis-fibering can be the cause for this alarm.

For CDC configurations, an MPO miscabling error or miscabling between FIM3 and RLA module where the Adjacency Expected Far End Address does not match the Adjacency Actual Far End Address and is not NULL, will cause the “Adjacency Mismatch” alarm to be raised on the Adjacencies at both ends of the MPO cable.

For CDC connection validation, this alarm is raised against the FIM/RLA/CCMD16x12/AMP4 MPO adjacency facility when a non-empty provisioned adjacency does not match discovered ADJ.

This alarm will also raise if:

- after removing the modules from the TID slot sequence, you leave the MPO cables connected to the removed module.
- mis-fibering of the FIM3 and RLA
- a Colored Line system is connected to a Photonic Colorless Line system.

  Note: This alarm can be raised momentarily when adding or deleting channels on CDC. The alarm is raised due to temporary mismatch between the provisioned and discovered wavelength and persists for the duration of the OTM tuning to the provisioned wavelength.

This alarm is expected on network elements adjacent to network elements undergoing a TID consolidation reconfiguration. These alarms clear after the inter-shelf adjacencies are updated with the **Node name**.

In the case of a line adjacency, the discovered far-end address is the photonics module at the other end of the fiber span.

Procedure 4-4 (continued)
Adjacency Mismatch

This alarm is also raised against an ADJ-TX or ADJ-RX facility when either the ADJ-TX or ADJ-RX facility has a discovered type that does not match the transmitter or receiver type. The alarm is raised when you provision a far-end address on a colorless CCMD to point to a transmitter that is not supported on a colorless line.

Normally when the ADJ-TX or ADJ-RX facility has Auto Discovered set to Auto, any change to the discovered type will be automatically populated to the transmitter or receiver type. However, if the change happens while the ADJ-TX or the ADJ-RX is managed by DOC (DOC Care is True), a switch module exists, or if the “Synch Provisioned” parameter is false, this auto-population is not possible and causes a mismatch.

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
- know the correct far-end address for the alarmed adjacency

Step	Action	
1	**If** this alarm is raised against	**Then** go to
	an ADJ-LINE facility	step 2
	an ADJ-TX or ADJ-RX facility	step 7
2	Ensure that a Colored Line system is not connected to a Photonic Colorless Line system.	
3	Using the network planning diagram, verify if the **Expected far-end address** adjacency parameter is correct. Refer to the “Retrieving protection parameters” procedure in Part 1 of *Configuration - Provisioning and Operating*, 323-1851-311.	
4	**If** the actual far-end address is	**Then**
	correct	go to step 5
	incorrect	verify that the line-side fiber is correctly connected. Go to step 6.

Procedure 4-4 (continued)
Adjacency Mismatch

Step	Action
5	Edit the **Expected far-end address** and **Expected far-end address format** adjacency parameters so that they match the **Actual far-end address** and **Actual far-end address Format** listed for the ADJ-LINE facility. Refer to the "Editing facility parameters" procedure in Part 1 of *Configuration - Provisioning and Operating*, 323-1851-311.
6	If the alarm does not clear, contact your next level of support or your Ciena support group. This procedure is complete.
7	Using the network planning diagram, verify that the actual far-end address parameter is correct.
8	**If** the actual far-end address is — **Then** go to correct — step 9 incorrect — step 11
9	Verify that the transmitter module (that the ADJ actual far-end address points to) is provisioned correctly. Correct the provisioning on the transmitter module in order for it to match the ADJ Tx/Rx transmitter/receiver type.
10	If the alarm does not clear, contact your next level of support or your Ciena support group. This procedure is complete.
11	If the actual far-end address is NULL, provision the correct expected far-end address between the transmitter module and the CMDADJ-TX port. Otherwise, clear the SPLI match that is discovered by setting the expected far-end address to NULL at the CMD ADJ-TX and transmitting module (if it supports ADJ provisioning). Then reprovision with the correct expected far-end address.
12	Ensure that the transmitter (that the ADJ actual far-end address points to) is supported on a colorless line system.
13	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 4-5
All Provisioned RADIUS Accounting Servers Unavailable

Alarm ID: 1518

Probable cause

This alarm is raised when no response is received from any provisioned RADIUS accounting server during a user-provisioned timeout.

This alarm is also raised when the RADIUS accounting server provisioning on the network element is incorrect.

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: • 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 *Administration and Security*, 323-1851-301.
5	Check the status of the RADIUS accounting server. Ensure the status is ON.

Procedure 4-5 (continued)
All Provisioned RADIUS Accounting Servers 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 4-6
All Provisioned RADIUS Servers Unavailable

Alarm ID: 582

Probable cause

This alarm is raised when:

- all requests to the primary and secondary RADIUS servers of a CTM time out
- all requests to a RADIUS server of a CTM time out and only one RADIUS server has been provisioned (primary or secondary)

If the All Provisioned RADIUS servers Unavailable alarm is raised and only a single RADIUS server is provisioned (primary or secondary), provisioning the second RADIUS server will cause the All Provisioned RADIUS servers Unavailable alarm to clear and either the Primary RADIUS Server Unavailable or Secondary RADIUS Server Unavailable alarm to be raised for the original RADIUS server.

The alarm is not raised due to server time out.

If the alternate method for security is Challenge/Response, the user can log in using the challenge response generated by Site Manger. The shared secret is required to generate the correct response. If the alternate method for security is Local, the user can log in using a local user ID and password.

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	Ensure the primary and secondary RADIUS servers of the CTM are enabled and have a valid IP address. Refer to the “Provisioning the primary or secondary RADIUS server” procedure in *Administration and Security*, 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 4-7
Automatic Power Reduction Active

Alarm ID: 542

Probable cause

The APR alarm is raised against the input or Line A output port of an AMP facility. The APR condition is caused by a reflection somewhere downstream from the AMP facility. This reflection can be caused by:

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

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

> ***Note:*** This alarm indicates a condition on the output port of an amplifier; however, the alarm is raised against the input port of the corresponding RLA or AMP4 modules. Therefore, ensure you troubleshoot the appropriate port. See the block diagrams of the amplifiers in the *6500 - T_Series Shelves- Guide*, 323-1851-103.

Procedure 4-7 (continued)
Automatic Power Reduction Active

ATTENTION

As of Release 10.2, the MuxAmp configuration disables the Automatic Power Reduction (APR) function. Certain C-band amplifier modules used in a MuxAmp configuration with one or more wavelengths in the IEC 60825-1 Class 1M range (such as those from a WL3n source) may have a Class 1 Hazard level label but should have a Class 1M Hazard Level label because APR is disabled.

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

The following C-band amplifier modules may have a Hazard Level 1 warning label.

– NTK720BA, AMP4 C-Band pluggable module

– NTK722AA, RLA 20x1 C-Band w/Upgrade 1xSFP module

For more information and the procedure to apply the Level 1M label on these modules, see the chapter on observing product and personnel safety guidelines in *Installation - 6500-T Series Shelves*, 323-1851-201.6.

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 safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - 6500-T Series Shelves*, 323-1851-201.6
- have the engineering documentation package (EDP)
- have a fiber cleaning kit
- have a replacement module

Procedure 4-7 (continued)
Automatic Power Reduction Active

Step	Action
1	**If** this alarm / **Then** was raised as a result of maintenance or SLAT that has not been completed — no action is required. The alarm will clear when the maintenance activity or SLAT is completed. The procedure is complete. is unexpected — go to step 2
2	Confirm that the amplifier's provisioning matches what is defined in the EDP. The amplifier's provisioning can be checked by using the Configuration->Equipment and Facility Provisioning screen in Site Manager. Edit the power level values as required. Refer to the “Retrieving protection parameters” procedure in Part 1 of *Configuration - Provisioning and Operating*, 323-1851-311.
3	**If** the original alarm has / **Then** cleared — the procedure is complete not cleared — go to step 4
4	**If** the alarmed amplifier is / **Then** go to Port 8 (Line A) — step 5 otherwise — step 9
5	Ensure that all LC/SC connectors located after the amplifier output are properly mated. Verify this on both ends of the connector-mating receptacles.
6	**If** the original alarm has / **Then** cleared — the procedure is complete not cleared — go to step 7
7	Ensure that the termination plugs are present and are mated properly on unused ports.
8	**If** the original alarm has / **Then** cleared — the procedure is complete not cleared — go to step 9

Procedure 4-7 (continued)
Automatic Power Reduction Active

Step	Action

9

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

CAUTION
Risk of damage to modules
Never disconnect an optical fiber that is connected to an active or powered up optical amplifier. To disconnect or reconnect an optical fiber, make sure the optical amplifier is out of service (OOS), then disconnect or reconnect the fiber.

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

Place the alarmed AMP facility out of service (OOS) using the Edit button in the Configuration->Equipment and Facility Provisioning screen of Site Manager. For further instructions refer to the “Changing the primary state of a facility” procedure in Part 1 of *Configuration - Provisioning and Operating*, 323-1851-311.

10

CAUTION
Risk of traffic loss
Only disconnect the output fiber of the alarmed optical amplifier. It is not necessary to disconnect any other output fibers, which could affect service.

Disconnecting the Line B out fiber will impact traffic in both directions, as this triggers Automatic Laser Shut Off (ALSO).

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

Procedure 4-7 (continued)
Automatic Power Reduction Active

Step	Action
11	Place the AMP facility back in-service (IS) using the Edit button in the Configuration->Equipment and Facility Provisioning screen of Site Manager. For further instructions refer to the “Changing the primary state of a facility” procedure in Part 1 of *Configuration - Provisioning and Operating*, 323-1851-311.
12	**If** the original alarm has / **Then** cleared / the procedure is complete not cleared / go to step 13
13	You may have to clean a specific connector or connectors that may not be immediately connected to the alarmed amplifier output. For information on isolating connector losses, complete Procedure 2-16, “Locating a reflective event”.
14	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 4-8
Automatic Shutoff

Alarm ID: 590

Probable cause

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

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

DANGER

Risk of radiation exposure

If light is used to test the broken fiber (for example, with a light source), 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.

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	Complete the Optical Line Fail alarm clearing procedure in Part 2 of this document.
2	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 4-9
Automatic Shutoff Compromised

Alarm ID: 1775

Probable cause

This alarm is raised when the Rx/Tx fibers of the OSC on an RLA circuit pack are crossed at one or both ends of a photonic span.

The alarm is also raised when the Tx power on the SFP is below the threshold or if the transmitter is disabled.

Impact

Major, service-affecting (M, SA) alarm

Prerequisites

To perform this procedure, you must:

- observe all safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - 6500-T Series Shelves*, 323-1851-201.6
- have the engineering documentation package (EDP)
- have a fiber cleaning kit

Step	Action
1	Ensure that the OSC fibers are correctly connected at both ends of their spans.
2	If the alarm does not clear, ensure that the transmitter is enabled. Check for and clean any dirty fibers. Refer to the “Cleaning connectors” chapter in *Installation - General Information*, 323-1851-201.6.
3	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 4-10
Automatic Shutoff Disabled

Alarm ID: 1035

Probable cause

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

- recovery from ALSO in certain configurations
- check for ORL at SLAT Time
- during the nodal continuity testing
- initial turn up and recovery on a stretched span (for example, without OSC)

CAUTION

Risk of laser radiation exposure

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

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

Impact

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

Prerequisites

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

Procedure 4-10 (continued)
Automatic Shutoff Disabled

Step	Action
1	Make sure that the maintenance work has been completed.
2	Immediately after the maintenance work has been completed, enable Auto Shutoff: • Select Facilities -> AMP. • Set the ALSO Disabled parameter to False in the AMP facility. This action clears the Automatic Shutoff Disabled alarm.
3	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 4-11
Auto Protection Switch Acknowledge Time Out

Alarm IDs: 1395

Probable cause

This alarm is raised for 1+1 OTN protection groups if an expected reverse request is not received by the tail end of a switch within 50 ms.

This alarm can be raised if a local 6500 1+1 OTN protection group is set to bidirectional mode and the far-end is operating in unidirectional mode.

Impact

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

Prerequisites

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

Step	Action
1	Identify the module raising the alarm. Refer to the Procedure 2-12, "Identifying the module, pluggable module/port, or facility that has raised an alarm" on page 2-31.
2	Ensure the fibering of the network is done properly. If not, make changes to correct the problem. If the alarm does not clear, continue with the next step.
3	From your company records, determine the correct switch mode for the link.

If the correct mode is	**Then** go to
unidirectional	step 4
bidirectional	step 5

4	At the local network element, change the switch mode of the optical interface pair identified in step 1. Refer to the "Changing the protection parameters for a pair of facilities or equipment" procedure in Part 2 of *Configuration - Provisioning and Operating*, 323-1851-311. Go to step 7. ***Note:*** Changing the protection switch mode for one of the optical interface modules in a pair automatically changes the protection switch mode for the other module in the pair.
5	Use the optical fiber/cable connection information to identify the network element and optical interface modules that are on the remote end of the link.

Procedure 4-11 (continued)
Auto Protection Switch Acknowledge Time Out

Step	Action
6	Log into the remote network element and change the mode of the optical interface modules to bidirectional.
7	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 4-12
Autoprovisioning Mismatch

Alarm ID: 60

Probable cause

This alarm is raised when a module is installed in an unprovisioned slot that does not support that module. For example, a photonic module inserted in a slot reserved by an OTS for a different EQPT type. There is no effect on shelf operations.

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

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 - 6500-T Series Shelves*, 323-1851-201.6
- if necessary, obtain a replacement module or a filler card

Step	Action
1	Identify the module raising the alarm. Refer to the Procedure 2-12, “Identifying the module, pluggable module/port, or facility that has raised an alarm” on page 2-31.
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 whether the slot is reserved by an OTS for a different equipment type.
4	**If** / **Then** go to the alarmed slot is reserved by an OTS for a different equipment type — step 5 otherwise — step 6
5	You can edit the OTS instance using the OTS Management application to release the slot. Then go to step 8. If you do not want to edit the OTS instance, go to step 9.

Procedure 4-12 (continued)
Autoprovisioning Mismatch

Step	Action	
6	**If**	**Then** go to
	the module in the alarmed slot is a spare module you want to store in that slot	step 7
	otherwise	step 9
7	Disable auto equipping for the alarmed slot. Refer to the “Enabling/disabling slot-based automatic equipping” procedure in *Administration and Security*, 323-1851-301.	
8	Reseat the module in the same slot. Refer to the equipment replacement procedures in *Fault Management - Module Replacement for T-Series*, 323-1851-546. Go to step 10.	
9	Remove the module in the alarmed slot and replace it with a module that is supported in the slot (refer to the *6500 - T_Series Shelves- Guide*, 323-1851-103), a module of the correct equipment type, or a filler card. Refer to the equipment replacement procedures in *Fault Management - Module Replacement for T-Series*, 323-1851-546.	
10	If the alarm does not clear, contact your next level of support or your Ciena support group.	

—end—

Procedure 4-13
Autoprovisioning Mismatch - Pluggable

Alarm ID: 343

Probable cause

This alarm is raised when an SFP+/CFP2/CFP2-ACO/QSFP+/QSFP28 installed in an unprovisioned port of a module is not supported for that module.

When auto equipping is disabled, this alarm is not raised.

Impact

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

Prerequisites

To perform this procedure, you must:

- observe all safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - 6500-T Series Shelves*, 323-1851-201.6
- obtain a supported replacement SFP+/CFP2/CFP2-ACO/QSFP+/QSFP28 for the corresponding module (refer to the *6500 - T_Series Shelves- Guide*, 323-1851-103)

Step	Action
1	Identify the module raising the alarm. Refer to the Procedure 2-12, “Identifying the module, pluggable module/port, or facility that has raised an alarm” on page 2-31. The **Unit** field in the **Active Alarms** application specifies the module, shelf ID, module slot, and SFP+/CFP2/CFP2-ACO/QSFP+/QSFP28 port using the following format: < module>-<shelf-id>-slot#-SFP+/CFP2/CFP2-ACO/QSFP+/QSFP28 port# **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.
2	Replace the SFP+/CFP2/CFP2-ACO/QSFP+/QSFP28 you identified in step 1 with a supported SFP+/CFP2/CFP2-ACO/QSFP+/QSFP28. Refer to the “Replacing an SFP/SFP+/CFP2/CFP2-ACO/QSFP+/QSFP28 module” procedure in *Fault Management - Module Replacement for T-Series*, 323-1851-546.

Procedure 4-13 (continued)
Autoprovisioning Mismatch

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

—end—

Procedure 4-14
AutoRoute Configuration Mismatch

Alarm ID: 1262

Probable cause

This alarm is raised when:

- the Autoroute OTS parameter values are not provisioned consistently in the channel access OTS instances at a site and/or within a domain.
- a mismatch is detected among the channel access OTS instances at site. The detection is limited by the connectivity among the shelves at the site. For example, the availability of TR records from the other shelves.

The alarm is raised against the OTS instances where the Autoroute parameter value is Enable.

Impact

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

Prerequisites

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

Step	Action
1	Use the Site Manager “OTS Management” or “Photonic Configuration” applications to set the OTS Autoroute value to the same value in all the OTSs within the node and within each of the optical domains that this node participate. Refer to the “Editing an OTS instance in the OTS Management application” procedure in Part 2 of *Configuration - Provisioning and Operating*, 323-1851-311. The OTS Autoroute parameter is only applicable to Channel Access OTS types (for example; ROADM). It is not applicable to other OTS types such as AMP and DGE.
2	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 4-15
Backplane ID Module 1/2 Failed

Alarm IDs: 679, 680

Use this procedure to clear the following alarms:

- Backplane ID Module 1 Failed
- Backplane ID Module 2 Failed

Probable cause

This alarm is raised when the shelf identifier unit 1 or unit 2 on the backplane has failed, is missing, has invalid data, or cannot be read.

The “Backplane ID Module 2 Failed” alarm is also raised when the shelf identifier unit 2 on the backplane detects a Mismatch between SID1 and SID2.

Impact

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

Prerequisites

To perform this procedure, you must have an electrostatic device (ESD) ground strap.

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	Perform a manual CTM protection switch. Refer to the “Operating a protection switch” procedure in Part 2 of *Configuration - Provisioning and Operating*, 323-1851-311.
3	**If** the alarm is / **Then** go to cleared / step 4 not cleared / step 5
4	Perform a protection switch to switch back to the originally active CTM (if needed). This procedure is complete.
5	Cold restart the Standby CTM. Wait five minutes for the CTM to restart.
6	If the alarm has not cleared, perform another manual CTM protection switch. Refer to the “Operating a protection switch” procedure in Part 2 of *Configuration - Provisioning and Operating*, 323-1851-311.
7	Cold restart the standby CTM and wait five minutes.

Procedure 4-15 (continued)
Backplane ID Module 1/2 Failed

Step	Action
8	If the alarm has not cleared, re-seat or cold restart the standby CTM and wait five minutes. Refer to the equipment replacement procedures in *Fault Management - Module Replacement for T-Series*, 323-1851-546.
9	**If** the alarm is / **Then** cleared / This procedure is complete. not cleared / go to step 10
10	Reseat the active CTM. This will cause an automatic CTM protection switch. Wait five minutes for the CTM to restart. Refer to Procedure 2-11, "Restarting an interface module or the CTM" on page 2-27".
11	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 4-16
Bandwidth Oversubscribed

Alarm IDs: 1767

Probable cause

This alarm is raised when a Holding Priority Bandwidth on an OSRP link is reduced below zero relative to the Maximum Available Bandwidth on the link. This can occur during SNC Preemption or a Reserved Home Path Bandwidth on the link or if an OSRP line is removed/deleted from the OSRP link where the available link bandwidth would become negative.

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	Change the Holding Priority Bandwidth on a link to zero or greater than zero by adding more lines to the link to increase the available bandwidth or reduce the bandwidth usage by re-grooming/rerouting some SNCs on the link to a different path or different Home Path. Refer to the OSRP provisioning procedures in chapter 1 of *Configuration - Control Plane*, 323-1851-330.
2	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 4-17
BW Lockout Configured

Alarm IDs: 1771

Probable cause

This alarm is raised when a bandwidth lockout is applied against both ends of an OSRP line intended for maintenance activities. The alarm will be cleared if either end of the line becomes bandwidth unlocked.

Impact

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

Prerequisites

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

Step	Action
1	Select the required network element in the navigation tree.
2	From the Configuration menu, select **Control Plane**: **OSRP Provisioning**.
3	Select the Lines tab.
4	Select the required shelf, containing link identifier, common line identifier, neighboring node, neighboring link identifier, and neighboring common line identifier from the drop-down lists.
5	Click **Retrieve**.
6	Select the OSRP line you want to edit from the OSRP line table.
7	Click Edit to open the Edit OSRP Line dialog box.
8	Disable (uncheck) OSRP bandwidth lockout by unchecking the Bandwidth lock out check box.
9	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 4-18
Cable Trace Compromised

Alarm ID: 1850

Probable cause

This alarm is raised against the Fiber Interconnect Modules (FIM1/FIM3), CCMD16X12, CCMD8x4, AMP4, or ROADM with Line Amp (RLA), if connection discovery is hampered due to hardware malfunction.

This alarm is raised against the FIM1/ FIM3, if there is an issue with the Smart Connect Module (SCM) of FIM. The alarm is raised against the CCMD16X12, CCMD8x4, AMP4, or RLA if there is an issue with the Transmit Optical Sub Assembly (TOSA) functionality.

Impact

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

Step	Action
1	Identify the module raising the alarm. Refer to Procedure 2-12, "Identifying the module, pluggable module/port, or facility that has raised an alarm" on page 2-31.

CAUTION
Risk of traffic loss
Replacement of the FIM1, FIM3, CCMD16x12, CCMD8x4, AMP4 or RLA is service affecting. If the alarm is unexpected, contact your next level of support or your Ciena support group before replacing the module or module.

2	Replace the module raising the alarm. Refer to the appropriate replacement procedure in *Fault Management - Module Replacement for T-Series*, 323-1851-546.
3	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 4-19
Channel Contention

Alarm ID: 1870

Probable cause

This alarm is raised against the PTP facility of a 2x100G PKT/OTN WL3n I/F or 5x100G WL3n CFP2-ACO PKT/OTN IF modules.

Impact

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

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 - 6500-T Series Shelves*, 323-1851-201.6
- 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 module
- use an account with at least a level 3 UPC

Step	Action
1	Identify the facility in “Channel Contention”. Refer to Procedure 2-12, “Identifying the module, pluggable module/port, or facility that has raised an alarm” on page 2-31.
2	**If** / **Then** go to the reported Echo Trace value is not “unknown” or the wavelength is already in use on the network — step 5 otherwise — step 3
3	Check the following provisioning information is correct on the card: • Modulation Format matches the other end of the link. • ENM is matching the other end of the link. • Differential coding matches the other end of the link. • If the upstream Tx is turned on, the channel is equalized by DOC. If all the provisioning information above is correct and the alarm is still active, then disable Channel Contention Detection.

Procedure 4-19 (continued)
Channel Contention

Step	Action
4	**If** the original alarm is / **Then** cleared / the procedure is complete not cleared / go to step 8
5	Reprovision the facility wavelength to an available wavelength/frequency. Refer to the “Retrieving equipment and facility details” and “Editing facility parameters” procedures in Part 1 of *Configuration - Provisioning and Operating*, 323-1851-311.
6	**If** the original alarm is / **Then** cleared / the procedure is complete not cleared / go to step 7
7	If the alarm is not clear and the facility wavelength is not already in use on the network, disable Channel Contention Detection. Refer to the “Retrieving equipment and facility details” and “Editing facility parameters” procedures in Part 1 of *Configuration - Provisioning and Operating*, 323-1851-311.
8	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 4-20
Channel Controller: Failure Detected

Alarm ID: 709

Probable cause

This alarm is raised against an RLA when the RLA is unable to function properly. Conditions that can cause this alarm include:

- the RLA has failed
- there is a loss of signal on one of the channels carried by the RLA
- the OPM is not provisioned against RLA monitor ports (there is an adjacency provisioning error)
- the RLA provisioning data is invalid
- the fibers to the RLA monitor ports are crossed or connected to a wrong OSC port

Note: Use optical terminators on unused input faceplate connectors of the installed RLA. 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.

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 engineering documentation package (EDP) containing shelf details
- have a replacement module if required
- have a fiber cleaning kit
- have an electrostatic device (ESD) ground strap

Step	Action	
1	Check for and clear any active "Circuit Pack Failed" alarm if they are raised against the RLA module.	
2	**If** the original alarm has	**Then**
	cleared	the procedure is complete
	not cleared	go to step 3

Procedure 4-20 (continued)
Channel Controller: Failure Detected

Step	Action
3	Check for and clear any of the following adjacency alarms: • Adjacency Mismatch • Adjacency Far End Not Discovered
4	**If** the original alarm has / **Then** cleared — the procedure is complete not cleared — go to step 5
5	Check for and clear any of the following alarms on all network elements before clearing the Channel Controller: Failure Detected alarm: • Automatic Power Reduction Active • Automatic Shutoff • Input Loss of Signal • Loss of Signal • Optical Line Fail • Output Loss of Signal • Shutoff Threshold Crossed • Channel Controller: Unexpected Loss Detected
6	**If** the original alarm has / **Then** cleared — the procedure is complete not cleared — go to step 7
7	Verify the adjacency of the RLA monitor port to ensure that the **Expected far-end address** field has the correct RLA module port listed, and that the corresponding **Adjacency type** field has the correct adjacency type listed (OPM). Refer to the “Retrieving protection parameters” procedure in Part 1 of *Configuration - Provisioning and Operating*, 323-1851-311.
8	**If** the original alarm has / **Then** cleared — the procedure is complete not cleared — go to step 9

Procedure 4-20 (continued)
Channel Controller: Failure Detected

Step	Action
9	Verify the derived OPM to RLA adjacency. Check the OPM adjacency of the OPM monitor port to ensure that the **Expected far-end address** field has the correct RLA port listed, and that the corresponding **Adjacency type** field has the correct adjacency type listed. Refer to the "Retrieving protection parameters" procedure in Part 1 of *Configuration - Provisioning and Operating*, 323-1851-311.
10	**If** the original alarm has / **Then** cleared / the procedure is complete not cleared / go to step 11
11	Verify that the CHC facilities associated with the RLA have the correct **Switch Selector** provisioned. Correct any discrepancies. Refer to the "Retrieving equipment and facility details" and "Editing facility parameters" procedures in Part 1 of *Configuration - Provisioning and Operating*, 323-1851-311.
12	**If** the original alarm has / **Then** cleared / the procedure is complete not cleared / go to step 13
13	Check the **Secondary State** of the CHC facilities associated with the RLA. Refer to the "Retrieving equipment and facility details" procedure in Part 1 of *Configuration - Provisioning and Operating*, 323-1851-311. If only certain (not all) CHC facilities indicate a FAF condition (facility failure), this can indicate a problem with the channel(s) added from a CCMD16x12 module.
14	**If** the original alarm has / **Then** cleared / the procedure is complete not cleared / go to step 15
15	Check the shelf-to-shelf association. The **Associated OTS** field should list the adjacent OTS (TID-shelf-instance), and the **Actual Associated OTS** should match the **Associated OTS**. Refer to the "Retrieving OTS Management details" procedure in Part 2 of *Configuration - Provisioning and Operating*, 323-1851-311.
16	**If** the / **Then** **Associated OTS** shows the incorrect adjacent OTS / correct the **Associated OTS** field **Actual Associated OTS** is not the same as the **Associated OTS** / verify the inter-shelf communications
17	If necessary, repeat step 15 and step 16 on each adjacent shelf.

Procedure 4-20 (continued)
Channel Controller: Failure Detected

Step	Action

18 **If** the original alarm has **Then**

cleared	the procedure is complete
not cleared	go to step 19

19

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

Verify that all RLA to OPM fibers are connected to the correct ports and that the fiber is clean. Refer to the cleaning connectors procedures in *Installation - 6500-T Series Shelves*, 323-1851-201.6.

20 **If** the original alarm has **Then**

cleared	the procedure is complete
not cleared	go to step 21

21 Perform a warm restart on the RLA. Refer to Procedure 2-11, "Restarting an interface module or the CTM" on page 2-27.

22 **If** the original alarm has **Then**

cleared	the procedure is complete
not cleared	go to step 23

23

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

Perform a cold restart on the RLA module. Refer to Procedure 2-11, "Restarting an interface module or the CTM" on page 2-27.

24 **If** the original alarm has **Then**

cleared	the procedure is complete
not cleared	go to step 25

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

—end—

Procedure 4-21
Channel Controller: Unexpected Loss Detected

Alarm ID: 877

Probable cause

This alarm is raised against an RLA when the RLA is unable to function properly. Conditions that can cause this alarm include:

- the RLA has failed
- the difference between the expected loss and the measured loss is greater than 6 dB
- there is a loss of signal on one of the channels carried by the RLA
- incorrect channel wavelength provisioning
- the OPM is not provisioned against RLA monitor ports (there is an adjacency provisioning error)
- the RLA provisioned data is invalid
- the fibers to the RLA monitor ports are crossed or connected to an incorrect OSC port
- the transmitter power at the CCMD16x12 ingress port is not within +/- 3 dBm of the provisioned Max/Typical Launch Power for that Tx adjacency. The alarm is raised on managed channels that have this unexpected power level, or on inactive channels that are being manually pre-checked with this unexpected power level. This condition only applies to the CCMD16x12 module.
- there is a fiber break between a CCMD16x12 common out port and the corresponding RLA switch input port.

  Note: Use optical terminators on unused input faceplate connectors of installed RLA modules. 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.

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
- have the engineering documentation package (EDP) containing shelf details

Procedure 4-21 (continued)
Channel Controller: Unexpected Loss Detected

- have a replacement module if required
- have a fiber cleaning kit
- have an electrostatic device (ESD) ground strap

Step	Action
1	At the RLA site, check the CHC facility status against the affected RLA. Note that in Site Manager you can click the switch selector column to sort the channels by port.
2	Check for channels with a secondary state of SGEO. Refer to the “Primary and secondary states” section in Part 1 of *Configuration - Provisioning and Operating*, 323-1851-311.
3	Verify whether all channels from a particular port, or just a subset are affected. If all channels on a switch port are SGEO, then there is a problem with the fiber connection between the RLA switch input port and the connected equipment (CCMD16x12). Investigate the potential fiber issue.
4	**If** the original alarm has / **Then** cleared / the procedure is complete not cleared / go to step 5
5	**If** a passthrough channel / **Then** go to is affected / step 29 is not affected / go to step 6
6	Verify the facility and equipment secondary state of the connected equipment. Refer to the “Primary and secondary states” section in Part 1 of *Configuration - Provisioning and Operating*, 323-1851-311.
7	If secondary states such as Supporting entity outage, FAF, Auto in-service, or SGEO exist, verify the failure.
8	Check for and clear any active module Failed alarm raised against the RLA.
9	**If** the original alarm has / **Then** cleared / the procedure is complete not cleared / go to step 10
10	Check for and clear any of the following adjacency alarms: • Adjacency Mismatch • Adjacency Far End Not Discovered

Procedure 4-21 (continued)
Channel Controller: Unexpected Loss Detected

Step	Action

11 **If** the original alarm has **Then**

cleared	the procedure is complete
not cleared	go to step 12

12 Check for and clear any of the following alarms on all network elements before clearing the Channel Controller: Failure Detected alarm:

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

13 **If** the original alarm has **Then**

cleared	the procedure is complete
not cleared	go to step 14

14 Check the wavelength provisioning of the line cards to make sure that it matches the wavelength of the CMD port the card is connected to. Refer to the “Retrieving equipment and facility details” procedure in Part 1 of *Configuration - Provisioning and Operating*, 323-1851-311.

15 **If** the original alarm has **Then**

cleared	the procedure is complete
not cleared	go to step 16

16 Verify the RLA adjacency of the LIM monitor port to ensure that the **Expected far-end address** field has the correct WSS OPM module port listed, and that the corresponding **Adjacency type** field has the correct adjacency type listed (OPM). Refer to the “Editing facility parameters” procedure in Part 1 of *Configuration - Provisioning and Operating*, 323-1851-311.

Refer to the “ADJ/ADJ-LINE/ADJ-TX/ADJ-RX/ADJ-FIBER facility parameters” table in Part 1 of *Configuration - Provisioning and Operating*, 323-1851-311.

17 **If** the original alarm has **Then**

cleared	the procedure is complete
not cleared	go to step 18

Procedure 4-21 (continued)
Channel Controller: Unexpected Loss Detected

Step	Action
18	Verify the derived OPM to RLA adjacency. Check the OPM adjacency of the RLA monitor port to ensure that the **Expected far-end address** field has the correct RLA module port listed, and that the corresponding **Adjacency type** field has the correct adjacency type listed. Refer to the "Retrieving protection parameters" procedure in Part 1 of *Configuration - Provisioning and Operating*, 323-1851-311.
19	**If** the original alarm has / **Then** cleared / the procedure is complete not cleared / go to step 20
20	Check the shelf-to-shelf association. The **Associated OTS** field should list the adjacent OTS (TID-shelf-instance), and the **Actual Associated OTS** should be the same as the **Associated OTS**. Refer to the "Retrieving OTS Management details" procedure in Part 2 of *Configuration - Provisioning and Operating*, 323-1851-311.
21	**If** the / **Then** **Associated OTS** shows the incorrect adjacent OTS / correct the **Associated OTS** field **Actual Associated OTS** is not the same as the **Associated OTS** / verify the inter-shelf communications
22	If necessary, repeat step 20 and step 21 on each adjacent shelf.
23	**If** the original alarm has / **Then** cleared / the procedure is complete not cleared / go to step 24
24	Verify that all RLA fibers are connected to the correct ports. Refer to the EDP. Verify that the fiber is clean. Refer to "Cleaning connectors" procedure in *Installation - 6500-T Series Shelves*, 323-1851-201.6.
25	**If** the original alarm has / **Then** cleared / the procedure is complete not cleared / go to step 26
26	Using the **Domain Optical Controller (DOC)** application, check for channels that have a channel condition of "Pre-Check Fail" or "Fault Detected". From the Site Manager window, click on **Configuration - Domain Optical Controller (DOC)** window and verify channel condition. If these channel conditions are the cause of this alarm, the DOC Action: Fault Detected alarm will be raised.

Procedure 4-21 (continued)
Channel Controller: Unexpected Loss Detected

Step	Action

27 Check the DOC logs to determine which channel has the unexpected ingress power. (From the Site Manager window, click on Configuration - Domain Optical Controller (DOC) window and then select DOC Logs button in Site Manger.) For this channel, verify (and if necessary, adjust) the power level at the source.

28

If the original alarm has	**Then**
cleared	the procedure is complete
not cleared	go to step 29

29 Perform a warm restart on the RLA. Refer to Procedure 2-11, "Restarting an interface module or the CTM" on page 2-27.

30

If the original alarm has	**Then**
cleared	the procedure is complete
not cleared	go to step 31

31

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

Perform a cold restart on the RLA. Refer to Procedure 2-11, "Restarting an interface module or the CTM" on page 2-27.

32

If the original alarm has	**Then**
cleared	the procedure is complete
not cleared	go to step 33

33

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.

If a subset (or single) channel on a particular switch port are SGEO, and the channel is not locally added at that node, then this may indicate a RLA hardware fault. Replace the RLA. Refer to the "Replacing a RLA 20x1 C-Band w/Upgrade 1xSFP module" procedure in *Fault Management - Module Replacement for T-Series*, 323-1851-546.

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

—end—

Procedure 4-22
Channel Degrade

Alarm ID: 1283, 1952

Probable cause

This alarm is raised when the RLA facility ‘Derived Input Power’ is less than the value of ‘Reference Input Power Profile’ minus the ‘Minor or Major Degrade Threshold’.

> ***Note:*** The Channel Degrade alarm has a 0.5 dB hysteresis that is considered before clearing the alarm. The delta between the CHC facility Derived Input Power and its Reference Input Power Profile must be less than 0.5 dB to clear the alarm.

The Minor Degrade Threshold defaults to 3 dB and can be user-provisioned between 0 to 30 dB using the Site Manager Node Information application and the Systems settings.

> ***Note:*** Major Degrade Threshold must be greater than the Minor Degrade Threshold. An attempt to edit major degrade threshold lower than minor degrade threshold, will be blocked by the system

For a CDC configuration, the minor degrade alarm is raised when the derived input power is greater than 3 dB below the reference input power.

The Major Degrade Threshold defaults to 6 dB and can be user-provisioned between 0 to 30 dB. A description of the function follows.

The “Reference Input Power Profile” parameter displays a referenced or baselined value for the Derived Input Power parameter. This power profile helps determine how the channel power changes over time. The power profile is system reset after a capacity change (a channel add or delete) or can be user reset using the “Reset Power Profile” button in the Equipment and Facility Provisioning application or can be user reset using the Reset TCA Baselines button in the DOC application.

If a channel is found to be below its previously stored value by more than a threshold, a minor degrade alarm is raised and the Channel Fault Status (CFS) is updated for that channel.

Note the following system behavior due to a change in “Derived Input Power”:

- up to 3 dB low in derived input power results in no alarms or CFS change. Re-optimize the channels.

- 3 to 6 dB low in derived input power results in the Channel Degrade (minor, NSA) alarm, the CFS set to “Degrade Minor”, the channel dropped from the control list, hold channel at current pixel setting
- 6 dB low in derived input power results in the Channel Degrade (minor, NSA) alarm, the CFS set to “Degrade Major”, the channel dropped from control list, hold channel at current pixel setting

On a CHC facility of a RLA if the ‘Derived Input Power’ of a channel is less than the value of ‘Reference Input Power Profile’ minus the ‘Minor/Major Degrade Threshold’, then the ‘Channel Degrade’ minor, NSA alarm is raised. This triggers the freezing of the pixel of the affected channel on the RLA. The Channel Fault Status (CFS) in the DOC application displays ‘Degrade Minor’ when the Minor degrade condition exists on the affected channel.

Note that one Channel Degrade alarm is raised per affected channel, which means more than one ‘Channel Degrade’ alarm can be raised against the same RLA equipment.

It is strongly recommended that the Minor Degrade and Major Degrade Thresholds remain at their default values.

Any drop in power that occurs prior to the RLA input could lead to the degrade condition.

Note: Use optical terminators on unused input faceplate connectors of installed RLA. 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.

Impact

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

Prerequisites

To perform this procedure, you must:

- have the optical fiber/cable connection information (that is, how the modules 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 safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - 6500-T Series Shelves*, 323-1851-201.6

Procedure 4-22 (continued)
Channel Degrade

Step	Action
1	Identify the module raising the alarm. Refer to the Procedure 2-12, "Identifying the module, pluggable module/port, or facility that has raised an alarm" on page 2-31.
2	If there are any Photonic alarms active, troubleshoot those alarms in the system first before trying to troubleshoot this alarm.
3	If no Photonic alarm is active, try to identify and fix any potential drop in power along the channel path all the way to the head-end service module.

4

If the original alarm has	**Then**
cleared	the procedure is complete
not cleared	go to step 5

Note: If the CHC facility 'Reset Power Profile' button is used to reset the power profile, it will affect the channels that were selected before clicking the button. If the DOC reset TCA Baseline button is used, it will affect the whole domain Power Profile.

5 If the fiber degrade is a known issue to the system and you want to clear the alarm, update the input power profile of the affected RLA facility on the RLA by clicking on the "Reset Power Profile" button in the equipment and facilities screen after selecting one or more affected channels.

6

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

ATTENTION
Clicking the Reset TCA Baselines Button from the DOC facility not only resets the 'Reference Input Power Profile' of each and every CHC facility of that domain but also resets the 'TCA Baselines' of the applicable facilities of the whole domain.

7 If the fiber degrades in the DOC domain is a known issue to the system and you want to clear the alarms of the whole domain rapidly, click the 'Reset TCA Baselines' button from the DOC facility. The reset TCA Baseline command will reset all Channel Degrade alarms in that domain. If the Channel Degrade alarm(s) cleared, then the procedure is complete.

8

If the alarm is raised against	**Then** go to
CDC configurations	step 9
otherwise	step 10

Procedure 4-22 (continued)
Channel Degrade

Step	Action
9	Click the “Reset Power Profile” button in the Equipment and Facility Provisioning application.
10	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 4-23
Channel Opacity Error

Alarm ID: 1433

Probable cause

This alarm is raised when a RLA pixel of a ROADM OTS is incorrectly set to Opaque (the CHC facility Opaque parameter is set to Yes), while a DOC-managed channel is meant to be using it.

The alarm is raised against the CHC facility at the shelf where the problem is detected.

For CDC configurations, this alarm is raised for RLA facilities when the pixel is set to OPAQUE. The RLA can be configured as part of ROADM OTS or as a CDC upgrade RLA. For a CHC facility on a CDC upgrade, this alarm is raised when there is a CRS provisioned on the facility but the CHC opacity is set to Opaque, regardless if the channel is DOC-managed.

Impact

Major, Service-affecting (M, SA) alarm

Prerequisites

To perform this procedure, you must observe all safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - 6500-T Series Shelves*, 323-1851-201.6.

Step	Action
1	Ensure that the CHC facility against which the alarm is raised, is used by a DOC-managed channel.
2	Change the RLA Opaque setting to No. Refer to the “Editing facility parameters” procedures in Part 1 of *Configuration - Provisioning and Operating*, 323-1851-311.
3	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 4-24
Circuit Pack Failed

Alarm IDs: 56, 1963

Probable cause

This alarm is raised in the following situations:

- the trouble detection circuits of a module detect a failure
- the CTM/CTMX detects a major failure on another module
- a power failure on the standby CTM/CTMX
- a newly active CTM/CTMX raises the alarm against the mate CTM/CTMX after a CTM/CTMX protection switch is caused by a power outage on the previously active CTM/CTMX

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

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

Impact

Critical, service-affecting (C, SA) alarm for:

- a working module in a 1+1 APS linear configuration with protection module faulty/unavailable
- a module in an unprotected configuration with switch modules

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

- an inactive or protected module in a 1+1 APS linear configuration
- a module without switch modules
- a working module with a protection module available or for protection module with a working module available

Photonic services

Critical, service-affecting (C, SA) alarm

Procedure 4-24 (continued)
Circuit Pack Failed

Prerequisites

To perform this procedure, you must:

- observe all safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - 6500-T Series Shelves*, 323-1851-201.6
- have a replacement module for the failed module
- have an electrostatic device (ESD) ground strap

Step	Action
1	Perform a DGN-EQPT command. If the alarm does not clear, continue to the next step.
2	Determine the time since the “Circuit Pack Failed” alarm was raised. Design expert data is automatically saved after a “Circuit Pack Failed” condition. This will take five minutes for the interface modules and 10 minutes for the CTM/CTMX. It is recommended that modules are not replaced during this time after the “Circuit Pack Failed” alarm has raised. The design expert data will not be captured if you do not wait.
3	Identify the module raising the alarm. Refer to the Procedure 2-12, “Identifying the module, pluggable module/port, or facility that has raised an alarm” on page 2-31. If the failure is against the CTM/CTMX, it may not be possible to log into the network element to determine the active alarms.
4	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf. ***Note:*** Do not re-seat the modules when the alarm is active.
5	Replace the faulty module. Refer to the equipment replacement procedures in *Fault Management - Module Replacement for T-Series*, 323-1851-546.
6	Retrieve all alarms and ensure the system is restored to its original state. **If** the original alarm has — **Then** go to cleared — step 7 not cleared — step 9
7	Select **Shelf Level View** from the **Configuration** menu.
8	Ensure that the new module is displayed.
9	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Table 4-1
Circuit Pack Failed alarm severities

Module configuration	Inactive/protected or active without cross-connects	Active or unprotected with cross-connects
2x100G WaveLogic 3n C-Band PKT/OTN I/F	m, NSA	C, SA
2x100G CFP2 PKT/OTN I/F	m, NSA	C, SA
20x10G SFP+ PKT/OTN I/F	m, NSA	C, SA
40x10G SFP+ PKT/OTN IF	m, NSA	C, SA
5x100G WL3n CFP2-ACO PKT/OTN I/F	m, NSA	C, SA
5x100G/12x40G QSFP28/QSFP+ PKT/OTN I/F (NTK762EA)	m, NSA	C, SA
Switch Module (SM)	m, NSA	C, SA
CCMD16x12	m, NSA	C, SA
CCMD8X4	m, NSA	C, SA
RLA	m, NSA	C, SA
CTM	m, NSA	NA
CTMX	m, NSA	C, SA
OTDR4	m, NSA	C, SA
MFC	m, NSA	C, SA
AMP4	m, NSA	C, SA
Note: The severity of the “Circuit Pack Fail” alarm for the CTM is not affected by the presence/absence of switch modules.		

Procedure 4-25
Circuit Pack Failed - Pluggable

Alarm ID: 340

Probable cause

This alarm is raised when a provisioned SFP+/CFP2/CFP2-ACO/QSFP+/ QSFP28 fails.

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 safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - 6500-T Series Shelves*, 323-1851-201.6
- have an optical power meter with the same optical connectors as the network element
- obtain a supported replacement SFP+/CFP2/CFP2-ACO/QSFP+/ QSFP28 for the corresponding module (refer to the *6500 - T_Series Shelves- Guide*, 323-1851-103)

Step	Action
1	Identify the module raising the alarm. Refer to the Procedure 2-12, “Identifying the module, pluggable module/port, or facility that has raised an alarm” on page 2-31. The **Unit** field in the **Active Alarms** application specifies the module, shelf ID, module slot, and SFP+/CFP2/CFP2-ACO/ QSFP+/QSFP28 port using the following format: <module>-<shelf-id>-slot#-SFP+/CFP2/CFP2-ACO/QSFP+/QSFP28 port#
2	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf. ***Note:*** Do not re-seat the modules when the alarm is active.
3	Replace the SFP+/CFP2/CFP2-ACO/QSFP+/QSFP28 you identified in step 1 with a supported SFP+/CFP2/CFP2-ACO/QSFP+/QSFP28. Refer to the “Replacing an SFP/SFP+/CFP2/CFP2-ACO/QSFP+/QSFP28 module” procedures in *Fault Management - Module Replacement for T-Series*, 323-1851-546.
4	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 4-26
Circuit Pack Latch Open

Alarm ID: 100, 1973

Probable cause

This alarm is raised when the bottom/lower locking lever on the module is not fully closed and the module is inserted into a slot, or the latch on the module is broken.

Impact

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

Prerequisites

To perform this procedure, you must observe all safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - 6500-T Series Shelves*, 323-1851-201.6.

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 module raising the alarm. Refer to the Procedure 2-12, “Identifying the module, pluggable module/port, or facility that has raised an alarm” on page 2-31.
3	Ensure that the module raising the alarm is pushed all the way into its slot, until the locking levers touch their latches.
4	Lock the module into its slot by pushing the upper locking lever down and the lower lever up at the same time.

ATTENTION
Do not force the locking levers. If the levers do not close correctly, gently re-insert the module. If the module cannot be re-inserted, remove the module and go to step 5.

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

—end—

Procedure 4-27
Circuit Pack Mismatch

Alarm ID: 36

Probable cause

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

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

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

For passive modules (such as FIM3), this alarm is raised when the module connected to the Access Panel External slot port does not match the provisioned module.

The alarm clears if the module in the specified slot is manually put out-of-service.

Impact

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

Critical, service-affecting (C, SA) alarm if active 1+1 APS or unprotected with switch modules
Minor, non-service-affecting (m, NSA) alarm if inactive 1+1 APS protected or without switch modules

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

For multi-port modules with ports configured with different protection schemes, the module assumes the highest alarm severity.

Photonic services

Critical, service-affecting (C, SA) alarm

Procedure 4-27 (continued)
Circuit Pack Mismatch

Prerequisites

To perform this procedure, you must observe all safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - 6500-T Series Shelves*, 323-1851-201.6.

Step	Action
1	Use one of the following options to view the shelf inventory: • select **Inventory** from the **Configuration** menu • select **Equipment & Facility Provisioning** from the **Configuration** menu
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 the shelf inventory using one of the following methods: • If using the **Shelf Inventory** application, compare the slot assignments and physical PECs listed with the actual modules in the shelf until you identify the mismatched module. • If using the **Shelf Level View** application, check if there is an "X" on an equipment graphic. The X indicates a circuit pack/module is physically present in the shelf, but the equipment provisioned for the circuit pack/module does not match what is present in the shelf. Mismatched modules can be the same type, but have different PECs. In these cases, ensure PECs match. Refer to the Probable cause section for this alarm. If you are not on site, use one of the following methods to identify any mismatches between the physical PEC and provisioned PEC by comparing the: • **Phys. PEC** and the **Prov. PEC** in the **Circuit Pack Details** tab in the **Shelf Level View** application • **Provisioned PEC** in the **Equipment & Facility Provisioning** application and the **Physical PEC** in the **Shelf Inventory** application A mismatch can indicate a PEC provisioning error or an incorrect module is installed.

Procedure 4-27 (continued)
Circuit Pack Mismatch

4	**If** you have	**Then** go to
	identified the mismatched	step 5
	not identified the mismatched	step 8

5 Replace the mismatched module with an appropriate module. Refer to the equipment replacement procedures in *Fault Management - Module Replacement for T-Series*, 323-1851-546.

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

7 Identify the module raising the alarm. Refer to the Procedure 2-12, "Identifying the module, pluggable module/port, or facility that has raised an alarm" on page 2-31.

8 Replace the module you identified in step 7. Refer to the equipment replacement procedures in *Fault Management - Module Replacement for T-Series*, 323-1851-546. Select the appropriate procedure from the "Module replacement procedures list" table.

If the alarm clears, the module you identified in step 7 is damaged.

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

—end—

Table 4-2
Circuit Pack Mismatch alarm severities

Modules/Configuration	Inactive	Active
2x100G WaveLogic 3n C-Band PKT/OTN I/F	m, NSA	C, SA
2x100G CFP2 PKT/OTN I/F	m, NSA	C, SA
20x10G SFP+ PKT/OTN I/F	m, NSA	C, SA
(1+2) 100G PKT/OTN IF	m, NSA	C, SA
100G PKT/OTN WL3n IF	m, NSA	C, SA
40x10G SFP+ PKT/OTN IF	m, NSA	C, SA
5x100G WL3n CFP2-ACO PKT/OTN I/F	m, NSA	C, SA
5x100G/12x40G QSFP28/QSFP+ PKT/OTN I/F (NTK762EA)	m, NSA	C, SA
OTDR4	m, NSA	C, SA
CTM	m, NSA	C, SA

Table 4-2
Circuit Pack Mismatch alarm severities (continued)

Modules/Configuration	Inactive	Active
MFC	m, NSA	C, SA
AMP4	m, NSA	C, SA
CCMD8X4	m, NSA	C, SA
CCMD16X12	m, NSA	C, SA
RLA (ROADM Line Amplifier)	m, NSA	C, SA
SM	m, NSA	C, SA

Procedure 4-28
Circuit Pack Mismatch - Pluggable

Alarm ID: 342

Probable cause

This alarm is raised when the installed SFP+/CFP2/CFP2-ACO/QSFP+/ QSFP28, is different from Provisioned PEC on the circuit pack.

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 safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - 6500-T Series Shelves*, 323-1851-201.6
- obtain a supported SFP+/CFP2/CFP2-ACO/QSFP+/QSFP28 for the corresponding circuit pack (refer to the *6500 - T_Series Shelves- Guide*, 323-1851-103)

Step	Action
1	Identify the circuit pack raising the alarm. Refer to the Procedure 2-12, “Identifying the module, pluggable module/port, or facility that has raised an alarm” on page 2-31. The **Unit** field in the **Active Alarms** application specifies the circuit pack, shelf ID, circuit pack slot, and SFP+/CFP2/ CFP2-ACO/QSFP+/QSFP28 port using the following format: <circuit pack>-<shelf-id>-slot#-SFP+/CFP2/CFP2-ACO/QSFP+/QSFP28 port#
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 SFP+/CFP2/CFP2-ACO/QSFP+/QSFP28 you identified in step 1 with a supported SFP+/CFP2/CFP2-ACO/QSFP+/QSFP28. Refer to the equipment replacement procedures in *Fault Management - Module Replacement for T-Series*, 323-1851-546.
4	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 4-29
Circuit Pack Missing

Alarm ID: 35, 681

Probable cause

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

- no circuit pack is in the designated slot
- circuit pack failure makes the circuit pack undetectable
- the access panel or PIM has been removed from the system. This alarm masks any existing alarm on that unit. For example, the Circuit Pack Missing alarm masks the Power Failure - B alarm.

  When both the A and B power feeds to one or more zones that supply power to a circuit pack have failed, the associated “Power Failure A/B” alarm must be cleared first in order to clear this alarm. Refer to the alarm clearing procedures in Part 2 of this document.

  Note: A Circuit Pack Missing alarm against an access panel masks/clears certain BITSIN and comms alarms (for example, the ILAN port, COLAN) raised against the access panel before its removal.

- a provisioned passive module (such as FIM3) is disconnected from the shelf Access Panel External Slot port.

If you change the state of the circuit pack raising this alarm to OOS, this alarm clears and the “Slot Empty” alarm is raised.

Impact

Minor, non-service-affecting (m, NSA) alarm for a protected module

Critical, service-affecting (C, SA) alarm for an active 1+1 APS or unprotected with switch modules

Minor, non-service-affecting (m, NSA) alarm for an inactive 1+1 APS, protected 1+1 APS, or without switch modules

Alarms with Critical, service-affecting severity are raised when both circuit packs in a protection group are pulled out of their slots. In this case, a m, NSA alarm and a C, SA alarm are raised.

For multi-port circuit packs with ports configured with different protection schemes, the circuit pack assumes the highest alarm severity.

Photonic services

Critical, service-affecting (C, SA) alarm

Prerequisites

To perform this procedure, you must:

- observe all safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - 6500-T Series Shelves*, 323-1851-201.6
- obtain replacement circuit packs

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 Procedure 2-12, “Identifying the module, pluggable module/port, or facility that has raised an alarm” on page 2-31.
3	**If** / **Then** go to an equipment connected to External Slots is reported missing — step 6 any other circuit pack is reported missing — step 4
4	**If** / **Then** the slot is empty — insert a circuit pack of the correct type into the slot. Go to step 5. a circuit pack of the correct type is in the slot — go to step 7.
5	Wait 30 seconds and retrieve all alarms to determine if the original alarm has cleared. **If** the original alarm has / **Then** cleared — the procedure is complete not cleared — go to step 7
6	Verify that the cable between the shelf External Slot Inventory port and the external peripheral is connected and is not damaged. For a CDC configuration, verify that the LAN cable is connected to the FIM3 and is not damaged. Go to step 11.

Procedure 4-29 (continued)
Circuit Pack Missing

Step	Action

7 **If** the circuit pack

	Then go to
is still carrying traffic and providing all services	the next step
is not carrying traffic and providing all services	step 11

8 Initiate a switch to the backup CTM/CTMX. Refer to the "Operating a protection switch" procedure in *Part 2 of Configuration - Provisioning and Operating*, 323-1851-311. After the system recovers, check if the alarm has cleared.

If the original alarm has	**Then** go to
cleared	step 9
not cleared	step 11

9 Reseat the previously active CTM/CTMX. Refer to the "Reseating a module" procedure in *Fault Management - Module Replacement for T-Series*, 323-1851-546. When the CTM/CTMX has finished booting, initiate a switch back to the originally active CTM/CTMX. After the system recovers, check if the alarm has cleared.

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

10 Initiate a switch back to the backup CTM/CTMX. Replace the original CTM/CTMX. Refer to the "Replacing a Control and Timing Module (CTM/CTMX)" procedure in *Fault Management - Module Replacement for T-Series*, 323-1851-546. Initiate a switch back to the newly inserted CTM/CTMX. After the system recovers, check if the alarm has cleared.

If the original alarm has	**Then**
cleared	the procedure is complete
not cleared	go to step 11

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

—end—

Table 4-3
Circuit Pack Missing alarm severities

Module/configuration	Inactive	Active
Access Panel	NA	m, NSA
CTM	m, NSA	C, SA
CTMX	m, NSA	C, SA
SM	m, NSA	C, SA
2x100G WL3n PKT/OTN IM	m, NSA	C, SA
2x100G CFP2 PKT/OTN IM	m, NSA	C, SA
20x10G SFP+ PKT/OTN IM	m, NSA	C, SA
RLA	m, NSA	C, SA
40x10G SFP+ PKT/OTN IF	m, NSA	C, SA
5x100G WL3n CFP2-ACO PKT/OTN I/F	m, NSA	C, SA
5x100G/12x40G QSFP28/QSFP+ PKT/OTN I/F (NTK762EA)	m, NSA	C, SA
OTDR4	m, NSA	C, SA
MFC	m, NSA	C, SA
AMP4	m, NSA	C, SA
CCMD8X4	m, NSA	C, SA
CCMD16x12	m, NSA	C, SA
FIM3	m, NSA	C, SA

Procedure 4-30
Circuit Pack Missing - Pluggable

Alarm ID: 339

Probable cause

This alarm is raised when a provisioned SFP+/CFP2/CFP2-ACO/QSFP+/QSFP28 is not physically installed in the circuit pack.

Impact

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

Prerequisites

To perform this procedure, you must:

- observe all safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - 6500-T Series Shelves*, 323-1851-201.6
- obtain a supported SFP+/CFP2/CFP2-ACO/QSFP+/QSFP28 for the corresponding circuit pack (refer to the *6500 - T_Series Shelves- Guide*, 323-1851-103)

Step	Action
1	Identify the circuit pack raising the alarm. Refer to the Procedure 2-12, “Identifying the module, pluggable module/port, or facility that has raised an alarm” on page 2-31. The **Unit** field in the **Active Alarms** application specifies the circuit pack, shelf ID, circuit pack slot, and SFP+/CFP2/CFP2-ACO/QSFP+/QSFP28 port using the following format: <circuit pack>-<shelf-id>-slot#-SFP+/CFP2/CFP2-ACO/QSFP+/QSFP28 port#
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 SFP+/CFP2/CFP2-ACO/QSFP+/QSFP28 module in the port you identified in step 1. Refer to the “Replacing an SFP+/CFP2/CFP2-ACO/QSFP+/QSFP28 module” procedure in *Fault Management - Module Replacement for T-Series*, 323-1851-546.
4	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 4-31
Circuit Pack Operational Capability Exceeded

Alarm ID: 1064

Probable cause

This alarm is raised against a 2x100G WL3n I/F module when equipment specifications are exceeded. This alarm indicates that at least one of the measurements, reach or PMD (Polarization Mode Dispersion) DGD (differential group delay), exceeded the specifications of the circuit pack. For information on operational specifications, refer to the *6500 - T_Series Shelves- Guide,* 323-1851-103.

If the client is not connected yet, the severity of the alarm is NSA since it does not impact client traffic. However, it still can impact line traffic. Line signal conditioning will be applied if the condition which caused this alarm to be raised was present during optical signal acquisition (for example, after connecting fiber, or after card insertion or cold restart operation). It is possible for this alarm to be raised without impacting traffic, if traffic was already running prior to the condition being detected. Actions must be taken to clear this alarm as soon as possible.

You can confirm the presence of signal conditioning in the PM screen where the OTU-SEFS PM count would be incrementing.

The alarm is latched even if all measurements, reach or PMD DGD do not exceed the specifications of the circuit pack and does not get re-evaluated until either a cold restart of the circuit pack or a line fault condition toggles (for example, a fiber pull and reinsertion).

Impact

Critical, service-affecting (C, SA) alarm
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 - 6500-T Series Shelves*, 323-1851-201.6
- obtain a replacement circuit pack suitable for the configuration

Procedure 4-31 (continued)
Circuit Pack Operational Capability Exceeded

Step	Action
1	Identify the circuit pack raising the alarm. Refer to the Procedure 2-12, "Identifying the module, pluggable module/port, or facility that has raised an alarm" on page 2-31.
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 that the circuit pack is connected to the correct optical link using ODU/OTU TTI. There should be no "ODU/OTU Trace Identifier Mismatch" alarm.
4	**If** the circuit pack — **Then** go to is connected to the correct optical link — step 6 is connected to the wrong optical link — step 5
5	Disconnect the existing fiber connections and re-connect the circuit pack to the correct optical link. **If** the alarm — **Then** clears — the procedure is complete does not clear — go to step 6
6	Contact your next level of support to find out and order the suitable circuit pack for the configuration. ***Note:*** If the condition which triggered the "Circuit Pack Operational Capability Exceeded" alarm is not present anymore, this latched alarm could be cleared by either cold restarting the circuit pack against which the alarm is raised (Refer to Procedure 2-11, "Restarting an interface module or the CTM" on page 2-27.) or by toggling the line in the transponder receive direction. Both actions to clear the alarm are service impacting.
7	Replace the circuit pack with a circuit pack suitable for the configuration. Refer to 'Replacing a PKT/OTN I/F module" procedure in *Fault Management - Module Replacement for T-Series*, 323-1851-546.
8	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 4-32
Circuit Pack Unknown

Alarm ID: 58, 1974

Probable cause

This alarm is raised in the following situations:

- when the on-board processor of a circuit pack cannot communicate with the CTM after you insert the circuit pack into the shelf
- when an unknown circuit pack is inserted into an unprovisioned slot
- when both the A and B power feeds to the zone powering a circuit pack have failed “Power Failure A/B” alarm have to be cleared first in order to clear this alarm. Refer to the alarm clearing procedures in Part 2 of this document.
- when external equipment connected to an External Slot inventory port on the access panel is unknown

ATTENTION

A circuit pack in the wrong slot only occurs if the circuit pack keying is removed. Circuit packs are keyed to fit into specific slots. Do not remove the circuit pack keying for any reason.

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 - 6500-T Series Shelves*, 323-1851-201.6.

Step	Action
1	Identify the circuit pack raising the alarm. Refer to the Procedure 2-12, “Identifying the module, pluggable module/port, or facility that has raised an alarm” on page 2-31.

If the circuit pack is	**Then** go to
a newly inserted or manually provisioned switch module	step 2
not a switch module	step 4

Procedure 4-32 (continued)
Circuit Pack Unknown

Step	Action
2	Perform protection switch of the CTM. Refer to “Operating a protection switch” procedure in Part 2 of *Configuration - Provisioning and Operating*. 323-1851-311. Do not insert any circuit packs while the CTM is performing a protection switch.
3	**If** the original alarm has / **Then** cleared — 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	Ensure that the circuit pack reporting the alarm is supported for the software release running on the shelf. You can check this against the hardware baseline report. **If** the circuit pack is / **Then** not supported by the software release — the circuit pack cannot be equipped in the shelf. Remove it. Go to step 6. supported by the software release — go to step 7
6	Wait 30 seconds, and retrieve all alarms. **If** the original alarm has / **Then** cleared — the procedure is complete not cleared — go to step 7
7	Compare the circuit pack raising the alarm with the supported circuit packs for each slot on the shelf. Refer to the *6500 - T_Series Shelves- Guide,* 323-1851-103. **If** the circuit pack raising the alarm is in / **Then** an unsupported slot — go to step 8 a supported slot — the circuit pack may be damaged. Go to step 9.
8	Replace the circuit pack raising the alarm with a circuit pack supported in that slot. Refer to the equipment replacement procedures in *Fault Management - Module Replacement for T-Series*, 323-1851-546. Select the appropriate procedure from the “Module replacement procedures list” table. Go to step 10.

Procedure 4-32 (continued)
Circuit Pack Unknown

Step	Action
9	Replace the circuit pack with an identical circuit pack. Refer to the equipment replacement procedures in *Fault Management - Module Replacement for T-Series*, 323-1851-546. Select the appropriate procedure from the “Module replacement procedures list” table.
10	Wait 30 seconds and retrieve all alarms.

If the original alarm	**Then**
is cleared	the procedure is complete. If you replaced a circuit pack in step 9, the circuit pack you replaced is damaged.
is not cleared	contact your next level of support or your Ciena support group

—end—

Procedure 4-33
Circuit Pack Unknown - Pluggable

Alarm ID: 341

Probable cause

This alarm is raised when an unrecognized SFP+/CFP2/CFP2-ACO/QSFP+/QSFP28 is installed in an unprovisioned port.

The Circuit Pack Unknown - Pluggable alarm cannot be disabled. Use the following steps to clear the alarm.

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 safety requirements described in the "Observing product and personnel safety guidelines" chapter in *Installation - 6500-T Series Shelves*, 323-1851-201.6
- obtain a supported SFP+/CFP2/CFP2-ACO/QSFP+/QSFP28 for the corresponding circuit pack (refer to the *6500 - T_Series Shelves- Guide*, 323-1851-103)

Step	Action
1	Identify the circuit pack raising the alarm. Refer to the Procedure 2-12, "Identifying the module, pluggable module/port, or facility that has raised an alarm" on page 2-31. The **Unit** field in the **Active Alarms** application specifies the circuit pack, shelf ID, circuit pack slot, and SFP+/CFP2/CFP2-ACO/QSFP+/QSFP28 port using the following format: <circuit pack>-<shelf-id>-slot#-SFP+/CFP2/CFP2-ACO/QSFP+/QSFP28 port#
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 SFP+/CFP2/CFP2-ACO/QSFP+/QSFP28 you identified in step 1 with a supported SFP+/CFP2/CFP2-ACO/QSFP+/QSFP28. Refer to the "Replacing an SFP/SFP+/CFP2/CFP2-ACO/QSFP+/QSFP28 module" procedure in *Fault Management - Module Replacement for T-Series*, 323-1851-546.
4	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 4-34
Circuit Pack Upgrade Failed

Alarm ID: 124, 1958

Probable cause

This alarm is raised against a circuit pack when the upgrade process of the circuit pack fails.

This alarm can also be raised after a CTM/CTMX replacement, when the inserted CTM is running a different software release than the active release on the network element.

> ***Note:*** In some cases, a "Circuit Pack Missing" or "Circuit Pack Unknown" alarm is simultaneously active with a "Circuit Pack Upgrade Failed" alarm for a particular slot. This condition can be cleared either by performing a minimal delivery of the corresponding software release, or by configuring a software release server for the network element. Refer to the "Transferring a software load to a network element" procedure in chapter 8 of *Administration and Security*, 323-1851-301.

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.
- use an account with at least a level 3 UPC

Step	Action
1	Check the upgrade state of all the circuit packs from Site Manager. Refer to the "Upgrading a software load" procedure in chapter 9 of *Administration and Security*, 323-1851-301. If a circuit pack upgrade has failed, the system attempts to auto-upgrade it.

Procedure 4-34 (continued)
Circuit Pack Upgrade Failed

Step	Action

ATTENTION
Do not attempt to clear any alarms during the upgrade.

2

If the original alarm has	**Then**
cleared	the procedure is complete
not cleared	go to step 3

3

If	**Then** go to
the alarm is raised after a CTM/CTMX replacement	step 4
otherwise	step 6

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 Refer to the “Replacing the switch module” procedure in *Fault Management - Module Replacement for T-Series,* 323-1851-546, to clear this alarm.

Go to step 9.

6 Reseat the circuit pack raising the alarm. Refer to the “Reseating a module” procedure in *Fault Management - Module Replacement for T-Series,* 323-1851-546. Select the appropriate procedure from the “Module replacement procedures list” table.

7

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

8 Replace the circuit pack. Refer to the replacement procedures in *Fault Management - Module Replacement for T-Series,* 323-1851-546. Select the appropriate procedure from the “Module replacement procedures list” table.

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

—end—

Procedure 4-35
Client Service Mismatch

Alarm ID: 696

Probable cause

This alarm is raised against a WAN facility of a 20x10G SFP+ PKT/OTN I/F, 2x100G CFP2 I/F or 2x100G WL3n I/F module.

The alarm is raised when the GFP UPI Tx byte provisioned on the remote circuit pack does not match the GFP UPI expected Byte on the local circuit pack. When this alarm is active, traffic from the far-end is lost.

The alarm point is identified at the generic framing procedure (GFP) level to indicate a provisioning mismatch between the near-end and far-end facility provisioning. For example, one end is configured to preserve the preamble and the other is configured to discard the preamble. The GFP user payload identifier (UPI) byte is used for this purpose.

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 network connection information (that is, how the optical modules on each network element connect to other network elements)
- observe all safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - 6500-T Series Shelves*, 323-1851-201.6

Step	Action
1	Trace the switch module information to determine the corresponding facility of the far-end circuit pack.
2	Ensure that the nodal switch modules are provisioned correctly.
3	Determine if the client facility provisioned at the corresponding far-end circuit pack matches the near-end. Correct any mismatches. Refer to the “Retrieving equipment and facility details” and “Editing facility parameters” procedures in Part 1 of *Configuration - Provisioning and Operating*, 323-1851-311.

Procedure 4-35 (continued)
Client Service Mismatch

Step	Action
4	Determine if the corresponding far-end facility parameters match the parameters at the end reporting the Client Service Mismatch alarm. Correct any mismatches. Refer to the “Retrieving equipment and facility details” and “Editing facility parameters” procedures in Part 1 of *Configuration - Provisioning and Operating*, 323-1851-311.
5	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 4-36
Cold Restart Required: FPGA Changed

Alarm ID: 646

Probable cause

This alarm is raised when a new functionality is introduced on a circuit pack that requires FPGA Loads. The circuit pack must be restarted to be loaded with the new feature. This alarm is also raised when a circuit pack loses its FPGA load from within the file system, and the FPGA load maintained on the circuit pack is older than the required load for this release.

If this alarm is raised as part of a network element software upgrade, refer to the appropriate Software Upgrade Procedure listed in the “Software Upgrade Procedures” section of the *6500 - T_Series Shelves- Guide*, 323-1851-103.

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 4-36 (continued)
Cold Restart Required: FPGA Changed

Step	Action
1	**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. Perform a cold restart on the circuit pack raising the alarm. Refer to Procedure 2-11, "Restarting an interface module or the CTM" on page 2-27.
2	If the alarm does not clear after the circuit pack restart, contact your next level of support or your Ciena support group.

—end—

Procedure 4-37
Configuration Mismatch

Alarm ID: 1415

Probable cause

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

Impact

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

Note: Shelf function is not affected by this alarm.

Requirements

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

Step	Action
1	Launch the OSRP Provisioning application and click on Links Tab to determine if both ends of the OSRP link have the same admin weight and bundle id assigned.
2	If different, provision the OSRP link to have the same admin weight and bundle id assigned. Refer to the “Editing an OSRP link” procedure in *Configuration - Control Plane*, 323-1851-330.
3	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 4-38
Configuration Mismatch - Adv BW Limit

Alarm ID: 1416

Probable cause

This alarm is raised when there is a configuration mismatch due to advertised bandwidth (Adv BW) limit being different on adjacent OSRP links.

Impact

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

Requirements

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

Step	Action
1	Identify the Advertisement BW limit on each side of the link. Refer to the "Editing an OSRP link" procedure in *Configuration - Control Plane*, 323-1851-330.
2	Ensure that both ends have the same Advertisement BW limit.
3	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 4-39
Configuration Mismatch - BW Lockout

Alarm ID: 1770

Probable cause

This alarm is raised when a bandwidth lockout is enabled on one end of an OSRP line and disabled on the other end.

If you apply a bandwidth lockout for maintenance activities to one end of the line, it is required to apply a bandwidth lockout on the other end of the line to clear the alarm.

The alarm also clears when the bandwidth lockout on both sides are matching (enabled or disabled).

It can take up to 30 seconds for this alarm to raise if one end of the OSRP line is configured and the other end is not.

Impact

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

Prerequisites

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

Step	Action
1	Disable the bandwidth lockout on the OSRP line or enable the bandwidth lockout at the other end of the OSRP line. Refer to the “Editing an OSRP line” procedure in *Configuration - Control Plane*, 323-1851-330.
2	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 4-40
Configuration Mismatch - BW Threshold

Alarm ID: 1768

Probable cause

This alarm is raised when there is a Bandwidth Threshold mismatch configuration on both ends of an OSRP link.

The alarm clears when you provision the same Bandwidth threshold value on both sides of the link.

Impact

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

Prerequisites

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

Step	Action
1	Identify which Bandwidth Threshold is misconfigured (which side of the link is misconfigured). Refer to “Retrieving OSRP provisioning information” procedure in *Configuration - Control Plane*, 323-1851-330.
2	Provision both ends of the OSRP link with the same Bandwidth Thresholds. Refer to the “Editing an OSRP line” procedure in *Configuration - Control Plane*, 323-1851-330.
3	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 4-41
Configuration Mismatch - Common ID

Alarm ID: 1411

Probable cause

This alarm is raised when the Common Line ID field of the OSRP line on either side is different.

Impact

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

Requirements

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

Step	Action
1	Identify the common id value of the OSRP line at the node raising the alarm. See the “Editing an OSRP link” procedure in *Configuration - Control Plane*, 323-1851-330.
2	Verify common id value of the node at the other ends of the OSRP line and compare it to the values found in step 1.
3	If the common id values on both ends of the OSRP line are not the same, change the values to be the same. Refer to the “Editing an OSRP link” procedure in *Configuration - Control Plane*, 323-1851-330.
4	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 4-42
Configuration Mismatch - Link ID

Alarm ID: 1420

Probable cause

This alarm is raised when in a link aggregation one end of the aggregation contains OSRP lines that are part of a different OSRP link.

Impact

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

Requirements

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

Step	Action
1	Identify the OSRP lines in a link aggregation on each side of the link. See the "Adding an OSRP link" procedure in *Configuration - Control Plane*, 323-1851-330.
2	Ensure all OSRP lines in a link aggregation on each side is part of only one OSRP link.
3	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 4-43
Configuration Mismatch - Node

Alarm ID: 1421

Probable cause

This alarm is raised when there is a configuration mismatch due to mismatch in aggregated OSRP line node IDs between adjacent OSRP links. The alarm raises when in a link aggregation at one end of the aggregation reports OSRP lines that are part of a different node.

Impact

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

Requirements

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

Step	Action
1	Identify the OSRP lines in a link aggregation on each side of the link. See the "Adding an OSRP link" procedure in *Configuration - Control Plane*, 323-1851-330.
2	Ensure that all OSRP lines in a link aggregation on each side are part of the same node.
3	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 4-44
Configuration Mismatch - OVPN ID

Alarm ID: 1769, 1866

Probable cause

This alarm is raised when the Optical Virtual Private Network Identifier (OVPN ID) on both ends of the OSRP link do not match.

The alarm clears when you provision the same OVPN ID on both sides of the link.

Impact

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

Prerequisites

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

Step	Action
1	Ensure that there are no Sub-Network Connections (SNCs) on the link. Refer to “Deleting a sub-network connection” procedure in *Configuration - Control Plane*, 323-1851-330.
2	Provision both ends of the link with the same OVPN ID. Refer to the “Editing an OSRP link” procedure in *Configuration - Control Plane*, 323-1851-330.
3	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 4-45
Configuration Mismatch - Primary State

Alarm ID: 1410

Probable cause

This alarm is raised when the administrative state of the ends of the OSRPLINE is mismatched with the remote end.

Impact

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

Requirements

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

Step	Action
1	Identify the administrative state of the OSRPLINE on each side of the link. See the “Adding an OSRP link” procedure in *Configuration - Control Plane*, 323-1851-330.
2	Ensure the administrative state of the OSRPLINE on each side is the same.
3	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 4-46
Control Plane Operations Blocked

Alarm ID: 1776

Probable cause

This alarm is raised on a DOC to indicate that the control plane cannot restore or create new SNCs because DOC Auto add channels and/or DOC Auto delete channels parameters are set to disable when the corresponding OTS facility is control plane enabled (CPS is provisioned to Enable).

Impact

Warning

Prerequisites

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

Step	Action	
1	**If** the OTS is supposed to be control plane	**Then** go to
	enabled	step 2
	disabled	step 3
2	Update the DOC facility attributes DOC Auto add channels and DOC Auto delete channels parameters to enable as follows: • From the Site Manager menu, select the DOC instance **(Configuration->Photonic Services->Domain Optical Controller (DOC)**. The Domain Optical Controller (DOC) window opens. • Select the required shelf from the Shelf pull-down menu, as required. (ALL is the default.) • Click on the **Start Monitoring** or **Refresh** button. • Select the required DOC instance from the summary table. • Select the **Settings** tab. • Click on the **Edit** button. The Edit DOC dialog is displayed. • Use the pull down menus to change the DOC values Auto add channels and Auto delete channels to “Enabled”. Go to step 4.	

Procedure 4-46 (continued)
Control Plane Operations Blocked

Step	Action
3	Update the CPS attribute of the OTS facility to Disable as follows: • From the Site Manager menu, select the OTS **(Configuration->Photonic Services->OTS management** or **Photonic Configuration Management)**. • From the OTS window, click the row with the desired OTS to highlight it and then click the **Edit** or **Edit OTS** button. The Edit OTS window opens. • From the Edit OTS window, click the **CPS** drop-down box and select “Disable”. Refer to the “Editing an OTS instance in the OTS Management application” procedure in Part 2 of *Configuration - Provisioning and Operating* 323-1851-311 for more information.
4	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 4-47
Control Plane System Mismatch

Alarm ID: 1773

Probable cause

This alarm is raised on a shelf when each OTS provisioned on that shelf that has a CPS value provisioned to Disable, but the domain to which the OTS belongs has at least one OTS within the domain with CPS provisioned to Enable.

This indicates that the CPS values for each OTS within a domain is not consistent. The event is only raised against the OTS with CPS provisioned to Disable. The alarm clears when you provision the CPS parameter on each ROADM OTS within a domain to the same value.

Impact

Warning

Requirements

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

Step	Action
1	Set the CPS parameter on each ROADM OTS within a domain to the same value.
2	Select **OTS management** or **Photonic Configuration Management** from **Configuration->Photonic Services**.
3	In the OTS Management or Photonic Configuration Management window, select the required shelf from the Shelf drop-down list.
4	Select the OTS that you want to edit and click the **Edit** or **Edit OTS** button. The Edit OTS window opens — If the intention for the L0 Control Plane software is to have visibility of the optical domain managed by the OTS, each OTS in the same domain must set the CPS value Enable. — If the intention for the L0 Control Plane software is not to have visibility of the optical domain managed by the OTS, each OTS in the same domain must set the CPS value to Disable. Refer to the “Editing an OTS instance in the OTS Management application” procedure in Part 2 of *Configuration - Provisioning and Operating,* 323-1851-311 for more information.
5	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 4-48
Co-Routed SNC Degraded

Alarm ID: 1827

Probable cause

This alarm is raised when some (but not all) of the terminating Subnetwork Connection (SNC) members are 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.

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	Follow the “SNC Unavailable” alarm clearing procedure in part 2 of this document. This alarm is cleared when all terminating Subnetwork. Connection (SNC) members have finished creating and starting state.
2	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 4-49
Co-Routed SNC Unavailable

Alarm ID: 1826

Probable cause

This alarm is raised when all the terminating Subnetwork Connection (SNC) members are 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.

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	Follow the “SNC Unavailable” alarm clearing procedure in part 2 of this document. This alarm is cleared when any terminating Subnetwork Connection (SNC) member has finished creating and starting state.
2	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 4-50
Corrupt Inventory Data

Alarm ID: 656

Probable cause

The alarm is raised against the cooling fan module, Fiber Interconnect Modules (FIM1/FIM3), access panel and PIM which is:

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

Impact

Critical, service-affecting (C, SA) alarm if active on fans (when at least one other fan related alarm is present)
Major, non-service-affecting (M, NSA) alarm if active on a PIM or fan (when no other fan-related alarm is present)
Minor, non-service-affecting (m, NSA) alarm if active on the access panel or PIM

Prerequisites

To perform this procedure, you must observe all safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - 6500-T Series Shelves*, 323-1851-201.6.

Step	Action

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

1 Verify that the alarmed unit is fully inserted.

Procedure 4-50 (continued)
Corrupt Inventory Data

Step	Action
2	Reseat the alarmed unit. Refer to the “Reseating a module” procedure in *Fault Management - Module Replacement for T-Series*, 323-1851-546.
3	**If** the original alarm has / **Then** cleared / the procedure is complete not cleared / go to step 4
4	Replace the alarmed unit. Refer to the equipment replacement procedures in *Fault Management - Module Replacement for T-Series*, 323-1851-546. The Circuit Pack Missing alarm is raised for that unit and the Corrupt Inventory Data for that unit clears.
5	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 4-51
Craft Load Missing

Alarm ID: 627

Probable cause

This alarm is raised when the CTM does not contain a craft (that is, NE Java Webstart Site Manager) load. The craft load is loaded when the CTM is upgraded.

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	Deliver the software load to the network element. Refer to the “Transferring a software load to a network element” 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 4-52
Craft Load Unpacking Aborted - Low Disk Space

Alarm ID: 1156

Probable cause

This alarm is raised when the CTM is running low in disk space, such that NE Java Webstart Site Manager cannot be installed in the NE.

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	Free disk space by deleting unused releases in the NE with DLT-RELEASE. Refer to the “Deleting a software load” procedure in *Administration and Security*, 323-1851-301. When there is sufficient free disk space after (DLT-RELEASE), the NE Java Webstart Site Manager will be installed automatically. After installation, the alarm will be clear.
2	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 4-53
Cross-connection Mismatch

Alarm ID: 863

Probable cause

For CDC configurations, this alarm is raised when redundant slot sequences are provisioned. Note that redundant slot sequences are not supported. The alarm clears when you deprovision the slot sequences.

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	Perform a database restore of a known good database. Refer to the backup and restore procedures in chapter 6 of *Administration and Security*, 323-1851-301, for more information.
2	If the problem has not been resolved after a successful database restore, contact your Ciena support group.

—end—

Procedure 4-54
Dark Fiber Loss Measurement Disabled

Alarm ID: 1825

Probable cause

This event is raised when the “Dark Fiber Loss Measurement” system parameter is set to 'Off' on a shelf with photonic equipment provisioned.

Impact

Warning

Prerequisites

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

Step	Action
1	Open the Node Information Site Manager application and select the System tab. Click **Edit** then set the “Dark Fiber Loss Measurement” system parameter to On. Refer to the “Editing the nodal system parameters” procedure in *Administration and Security*, 323-1851-301. ***Note:*** If “Shelf Sync” is set to “No”, the “Dark Fiber Loss Measurement” system parameter can be changed from either primary shelf or member shelf. If “Shelf Sync” is set to “Yes”, the “Dark Fiber Loss Measurement” system parameter can only be changed from primary shelf and the change will be broadcasted to all its member shelves.
2	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 4-55
Database Auto Save in Progress

Alarm ID: 1047

Probable cause

This alarm is raised when an automatic database backup is initiated.

Note: This alarm is disabled by default.

Impact

Warning

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

—end—

Procedure 4-56
Database Integrity Fail

Alarm ID: 8

Probable cause

This alarm is raised when there is a possibility that provisioning data on the CTM is in a corrupted state.

Impact

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

Step	Action
1	Contact your next level of support or your Ciena support group.

—end—

Procedure 4-57
Database Restore in Progress

Alarm ID: 143

Probable cause

This alarm is raised when the provisioning data is being restored to a standalone shelf or to one or multiple shelves in a consolidated TID.

Impact

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

Prerequisites

To perform this procedure, you must

- be able to connect to the CTM
- use an account with at least a level 3 UPC

Step	Action
1	Wait until the currently ongoing database restore successfully completes. Refer to the “Restoring provisioning data” procedure in *Administration and Security*, 323-1851-301. To clear the alarm and abort the database restore action, click **Cancel** in the **Backup and Restore** application. Canceling recovers the system and cleans up any backup files left in invalid states.
2	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 4-58
Database Save Failed

Alarm ID: 1263

Probable cause

This alarm is raised when the CTM detects that a save command sent to the CTM fails.

Impact

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

Prerequisites

To perform this procedure, you must

- be able to connect to the CTM
- use an account with at least a level 3 UPC

Step	Action
1	Select your next step. **If** you want to / **Then** go to clear the alarm by canceling the action — step 2 clear the alarm and retry the action — step 3
2	Click **Cancel** in the **Backup and Restore** application. Refer to the “Restoring provisioning data” procedure in *Administration and Security*, 323-1851-301 for more information. Canceling cleans up any backup files left in invalid states.
3	This alarm can be cleared if you try to backup or restore the provisioning data again. The alarm clears if the backup or restore action is successful. Refer to the “Restoring provisioning data” procedure in *Administration and Security*, 323-1851-301 for more information.

Procedure 4-58 (continued)
Database Save Failed

Step	Action
4	If the alarm does not clear, check the network element to determine whether a condition exists that can prevent a save. These conditions include: • a “Software Upgrade in Progress” alarm is active • a database save is already in progress • a “Software Mismatch” alarm is active • the software version on the CTM is different from the other modules • a “Disk Full” alarm is active • a corruption in the network element database is detected (indicated by a Transport Data Recovery Failed alarm) • active alarms are present unless you specify the backup to ignore active alarms Below is a checklist for Database Save specific failure (these failures are popped up in Site Manager when a database save is failed). • Database Save Failed: FTP/SFTP access denied — Ensure the IP address, directory path, userid and password are valid for the remote host • Database Save Failed: Failure transferring file, — Ensure that the remote host has adequate disk space and the correct attributes (permissions) are set for writing to the remote directory. • Database Save Failed: Invalid destination — check URL path, filename, permission • Database Save Failed: Could not connect to destination — Ensure there are no issues with FTP server on the remote host. • Database Save Failed: Could not connect to Source — Ensure there are no issues with FTP server on the remote host. An FTP server can handle up to certain amount of simultaneous FTP sessions (for example 50), so when performing a save, the Maximum Transfer Session parameter should be set to a number that the FTP server can handle.
5	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 4-59
Database Restore Failed

Alarm ID: 1264

Probable cause

This alarm is raised when a restore command fails.

Impact

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

Prerequisites

To perform this procedure, you must

- be able to connect to the CTM
- use an account with at least a level 3 UPC

Step	Action
1	Select your first step. **If** you want to / **Then** go to clear the alarm by canceling the action — step 2 clear the alarm and retry the action — step 3
2	Click **Cancel** in the **Backup and Restore** application. Refer to the "Restoring provisioning data" procedure in *Administration and Security*, 323-1851-301 for more information. Canceling cleans up any backup files left in invalid states.
3	This alarm can also clear if you try to restore the provisioning data again. The alarm clears if the restore action is successful. Refer to the "Restoring provisioning data" procedure in *Administration and Security*, 323-1851-301 for more information.

Procedure 4-59 (continued)
Database Restore Failed

Step	Action
4	If the alarm does not clear, check the network element to determine whether a condition exists that can prevent a restore. These conditions include: • a “Software Upgrade in Progress” alarm is active • a database save is already in progress • a “Software Mismatch” alarm is active • the software version on the CTM is different from the other circuit packs • a “Disk Full” alarm is active • a corruption in the network element database is detected (indicated by a Transport Data Recovery Failed alarm) • active alarms are present unless you specify the backup to ignore active alarms Below is a checklist for Database Restore specific failure (these failures appear in Site Manager when a database restore action fails). • Database Restore Failed: Invalid source — Check the database filename prefix. If the file identifier is used in the database filename then the user must use the **Use filename starting with** checkbox option to match with the database filename prefix. — Check the shelf number in the database filename prefix. If it does not match with the NE shelf number then the user must use the **Use filename with shelf number** checkbox option to match with the database shelf number prefix. • Database Restore Failed: Backup not from this node — This failure indicates the node name saved in the database and the NE node name do not match. Either the database was saved in the different shelf or the current NE node name had been changed after the database save. You can specify the restore to ignore the node name check by uncheck the **Do not restore if data was not backed up from this NE** checkbox. • Database Restore Failed: Mismatched Software Releases — Ensure the database software release is not different from the NE software release. • Database Restore Failed: Software Subsystem — This failure may indicate that the standby CTM is not ready for switch of activity. If the standby CTM is Out-of-Service, place the equipment In-Service and retry the Database Restore operation. For all cases, contact your next level of support or your Ciena support group.

Procedure 4-59 (continued)
Database Restore Failed

Step	Action

- Database Restore Failed: Incompatible S/R options
  - — If database was saved with the communication setting option by checking the **Do not restore if data was not backed up from this NE** check box. Ensure this checkbox is checked on the restore.
  - — If database was saved without checking the **Do not restore if data was not backed up from this NE** check box. Ensure this checkbox is not checked on the restore.
- Database Restore Failed: FTP/SFTP access denied
  - — Ensure the IP address, directory path, userid and password are valid for the remote host
- Database Restore Failed: Could not connect to destination
  - — Ensure there are no issues with FTP server on the remote host.
- Database Restore Failed: Could not connect to Source
  - — Ensure there are no issues with FTP server on the remote host.

  An FTP server can handle up to certain amount of simultaneous FTP sessions (for example 50), so when performing a Restore, the Maximum Transfer Session parameter should be set to a number that the FTP server can handle.

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

—end—

Procedure 4-60
Database Commit Failed

Alarm ID: 1265

Probable cause

This alarm is raised when a Commit command fails.

Impact

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

Prerequisites

To perform this procedure, you must

- be able to connect to the CTM
- use an account with at least a level 3 UPC

Step	Action
1	Select your next step. **If** you want to / **Then** go to clear the alarm by canceling the action — step 2 clear the alarm and retry the action — step 3
2	Click **Cancel** in the **Backup and Restore** application. Refer to the "Restoring provisioning data" procedure in *Administration and Security*, 323-1851-301, for more information. Canceling cleans up any backup files left in invalid states.
3	This alarm can also clear if you try to backup or restore the provisioning data again. The alarm clears if the backup or restore action is successful. Refer to the "Restoring provisioning data" procedure in *Administration and Security*, 323-1851-301, for more information.
4	If the alarm does not clear, check the network element to determine whether a condition exists that can prevent a commit. These conditions include: • a "Software Upgrade in Progress" alarm is active • a database save is already in progress • a "Software Mismatch" alarm is active • the software version on the CTM is different from the other circuit packs • a "Disk Full" alarm is active • a corruption in the network element database is detected (indicated by a Transport Data Recovery Failed alarm) • active alarms are present unless you specify the backup to ignore active alarms

Procedure 4-60 (continued)
Database Commit Failed

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

—end—

Procedure 4-61
Database Save in Progress

Alarm ID: 147

Probable cause

This alarm is raised while a database save is in progress and clears when the save is completed or has failed.

Impact

Warning

Step	Action
1	No action is required. The alarm clears when database save is completed or failed.

—end—

Procedure 4-62
Debug Port in Use

Alarm ID: 1132

Probable cause

This alarm is raised when a user with a UPC 4 or greater logs in to the debug port.

The “Debug Port In Use” alarm is disabled by default and can be enabled using the Site Manager Configuration->Alarms & Controls->Alarm Profiles application.

The alarm severity can also be provisioned.

Impact

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

Step	Action
1	No action is required. The alarm clears when the debug port is no longer in use.
2	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 4-63
Degraded Switch Fabric

Alarm ID: 1875

Probable cause

This alarm is raised when the Switch Fabric capacity is reduced by more than one Switch Module (SM) because multiple SMs are unavailable (for example. taken OOS-MA, failed, or missing).

The alarm can be caused by placing the switch module manually out-of-service, Circuit Pack Fail alarm, or a Circuit Pack Missing alarm.

Impact

Major, service-affecting (M, SA) alarm

Step	Action
1	If any switch module is placed OOS manually, place it in-service and verify if the alarm is cleared.
2	If the alarm is not cleared, select **Active Alarms** from the **Faults** menu to retrieve alarms and clear all active alarms.
3	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 4-64
Delay Measurement Enabled on Slave Node

Alarm ID: 1418

Probable cause

This alarm is raised when latency discovery is enabled on an OSRP slave node.

Impact

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

Step	Action
1	Disable latency discovery on slave node. Refer to the “Editing an OSRP link” procedure in *Configuration - Control Plane*, 323-1851-330. If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 4-65
Delay Measurement Mismatch Capability

Alarm ID: 1417

Probable cause

This alarm is raised when a link is up between master node and the slave node and the user enables latency discovery on master node on that link. Then the master OSRP node will be capable of delay measurements while the salve node is not capable of performing delay announcements.

Impact

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

Step	Action
1	Disable latency discovery flag on master node. Refer to the “Editing an OSRP link” procedure in *Configuration - Control Plane*, 323-1851-330.
2	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 4-66
Disk Full alarms

Use this procedure to clear alarms associated with the CTM disk capacity.

Disk 75 percent Full

Alarm ID: 374

Probable cause

This alarm is raised when the disk is 75% full on the CTM and clears when there is at least 30% free space.

The Disk 75 percent Full alarm is for information only and does not affect the operation of the shelf. It is recommended that you attempt to clear this alarm to prevent possible future problems if the disk becomes too full.

Impact

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

Disk 90 percent Full

Alarm ID: 375

Probable cause

This alarm is raised when the disk is 90% full on the CTM and clears when there is at least 15% free space.

The Disk 90 percent Full alarm is for information only and does not affect the operation on the shelf. It is recommended that you attempt to clear this alarm to prevent possible future problems if the disk becomes too full.

Impact

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

Disk Full

Alarm ID: 146

Probable cause

This alarm is raised when the disk is full on the CTM.

Impact

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

ATTENTION

Any time a Disk Full condition is reached, some applications or operations are blocked. For example, the system blocks upgrades, circuit pack provisioning, and initializations.

Procedure 4-66 (continued)
Disk Full alarms

Prerequisites

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

Step	Action
1	Delete any loads that you do not require on the disk. Refer to the “Deleting a software load” 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 4-67
DOC Action: Channel Add In Progress

Alarm ID: 875

Probable cause

This alarm is raised by DOC as soon as the **Add** channel command enters the EXECUTING state. This alarm is only active at the DOC site where the **Add** command is executing.

This alarm provides a warning to users who want to perform system maintenance or 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.

Step	Action
1	No action is required. Wait for the DOC add to complete (successfully, unsuccessfully, or by the **Stop DOC Action** command). DOC will then clear the alarm.
2	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 4-68
DOC Action: Channel Delete In Progress

Alarm ID: 876

Probable cause

This alarm is raised by the DOC as soon as the **Delete** or **Forced Delete** command enters the EXECUTING state. The EXECUTING state begins after the “Delete: Waiting” state. This alarm is only active at the DOC site where the **Delete** or **Forced Delete** command is executing.

This alarm provides a warning to users who want to perform system maintenance or provisioning.

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	No action is required. Wait for DOC delete to complete (successfully, unsuccessfully, or by the **Stop DOC Action** command). DOC will then clear the alarm.
2	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 4-69
DOC Action Failed: Add

Alarm ID: 576

Probable cause

This alarm is raised when a Channel Add command (automatic or manual) in DOC is requested and fails. Conditions that can cause this failure include:

- maintenance activities, such as module replacement, module restart, and fiber cut occurred during the Channel Add command
- an internal communications issue (for example, the ILAN port is not cabled)
- a provisioning error on the Rx or Tx adjacency
- an associated adjacency or AMP facility is deleted
- the DOC Action: Channel Add was stopped before the addition was completed

This alarm appears only on the affected DOC shelf.

This alarm is cleared if the **Clear DOC Alarms** button is clicked in the **DOC** application. However, this will not clear the underlying problem.

Note: It is recommended that DOC be placed OOS before inserting a standby CTM. If it is not, and the DOC is set to automatically add channels or you manually add a channel during the standby CTM insertion, the DOC Action Failed: Add alarm can be raised after the insertion. In this case, the alarm will clear in approximately five minutes.

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 engineering documentation package (EDP) containing provisioning details

Procedure 4-69 (continued)
DOC Action Failed: Add

Step	Action
1	If maintenance activities, such as module replacement, module restart, or fiber cut occurred during the **Add** channel operation, then this alarm will be active. Ensure that the maintenance activities have completed.
2	Check for and clear any active "DOC Invalid Photonic Domain" alarms using the Procedure 4-76, "DOC Invalid Photonic Domain" on page 4-153 procedure in this document.
3	Check for and clear any of the following alarms on all the network elements that are active within the DOC span of control: • Adjacency Far End Not Discovered • Adjacency Provisioning Error • Automatic Power Reduction Active • Automatic Shutoff • Channel Controller: Unexpected Loss Detected • Circuit Pack Failed • Circuit Pack Mismatch • Circuit Pack Missing • Circuit Pack Unknown • Gauge Threshold Crossing Alert Summary • Optical Line Fail • OSC Loss of Signal • Shutoff Threshold Crossed ***Note:*** If the Optical Line Fail alarm is active, clear this alarm first.

Procedure 4-69 (continued)
DOC Action Failed: Add

Step	Action
4	Clear all other active alarms on the network elements within the DOC span of control. For optimal DOC operation, the system must be alarm free. Use the DOC **Logs** window to view the DOC logs to determine if another network element reported an error. Review the DOC logs from the other network element. Refer to the "Displaying the DOC logs for the summary table" procedure in Part 2 of *Configuration - Provisioning and Operating*, 323-1851-311.
5	Verify, and if necessary, correct the following provisioned data (reference the EDP): • Tx and Rx adjacency parameters (**Adjacency type** and all power-related parameters) • Line adjacency parameter (**Fiber Type**) • AMP optical facility parameters (**Mode**, **Target Gain**, **Target Power**, and **Target Peak Power**)
6	Check the subtending connections to the CCMD16x12. Make sure that the connections, power levels and wavelengths are within specifications.
7	Re-attempt to add the channels.
8	If the alarm does not clear, or clears then returns, or the channels cannot be added, contact your next level of support or your Ciena support group. **—end—**

Procedure 4-70
DOC Action Failed: Delete

Alarm ID: 577

Probable cause

This alarm is raised when a Channel Delete command (automatic or manual) in DOC is requested and fails. Conditions that can cause this failure include:

- maintenance activities, such as module replacement, module restart, and fiber cut occurred during the Channel Delete operation
- an internal communications issue (for example, the ILAN port is not cabled)
- an optical disconnect, such as a fiber break, within the DOC span of control
- a provisioning error on the Rx or Tx adjacency
- an associated adjacency or AMP facility is deleted
- the DOC Action: Channel Delete was stopped before the deletion was completed

This alarm appears only on the affected DOC shelf.

This alarm is cleared if the **Clear DOC Alarms** button is clicked in the **DOC** application. However, this will not clear the underlying problem.

> ***Note:*** It is recommended that DOC be placed OOS before inserting a standby CTM. If it is not, and the DOC is set to automatically delete channels or you manually delete a channel during the standby CTM insertion, the DOC Action Failed: Delete alarm can be raised after the insertion. In this case, the alarm will clear in approximately five minutes.

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 engineering documentation package (EDP) containing provisioning details

Procedure 4-70 (continued)
DOC Action Failed: Delete

Step	Action
1	If maintenance activities, such as module replacement, module restart, or fiber cut occurred during the **Delete** channel operation, then this alarm will be active. Ensure that the maintenance activities have completed.
2	Check for and clear active "DOC Invalid Photonic Domain" alarms using Procedure 4-76, "DOC Invalid Photonic Domain" on page 4-153 procedure in this document.
3	Check for and clear any of the following alarms on all the network elements that are active within the DOC span of control: • Adjacency Far End Not Discovered • Adjacency Provisioning Error • Automatic Power Reduction Active • Automatic Shutoff • Channel Controller: Unexpected Loss Detected • Circuit Pack Failed • Circuit Pack Mismatch • Circuit Pack Missing • Circuit Pack Unknown • Gauge Threshold Crossing Alert Summary • Optical Line Fail • OSC Loss of Signal • Shutoff Threshold Crossed ***Note:*** If the Optical Line Fail alarm is active, clear this alarm first.
4	Clear all other active alarms on the network elements within the DOC span of control. For optimal DOC operation, the system must be alarm free. Use the DOC **Logs** window to view the DOC logs to determine if another network element reported an error. Review the DOC logs from the other network element. Refer to the "Displaying the DOC logs for the summary table" procedure in Part 2 of *Configuration - Provisioning and Operating*, 323-1851-311.

Procedure 4-70 (continued)
DOC Action Failed: Delete

Step	Action
5	Verify, and if necessary, correct the following provisioned data (reference the EDP): • Tx and Rx adjacency parameters (**Adjacency type** and all power-related parameters) • Line adjacency parameter (**Fiber Type**) • AMP optical facility parameters (**Mode**, **Target Gain**, **Target Power**, and **Target Peak Power**)
6	**If** the **Channel Condition** field displays — **Then** go to a condition other than “Partially Deleted” — step 7 “Partially Deleted” — step 10
7	Click the **Clear DOC Alarms** button in the DOC window. This clears the alarm; however, the underlying problem is not cleared.
8	Click the **Re-optimize** button, and wait until the optimization completes.
9	**If** the optimization — **Then** go to fails — Procedure 4-72, “DOC Action Failed: Optimize” on page 4-142 succeeds — step 10
10	Re-attempt the **Delete** operation. **ATTENTION** Any channels that were in the delete queue are returned to their previous state when the deletion fails. These channels must be re-selected for deletion.
11	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 4-71
DOC Action Failed: Monitor

Alarm ID: 549

Probable cause

This alarm is raised when DOC is unable to monitor, and thus unable to determine if the Photonic Domain is optimal. Conditions that can cause this failure include:

- an internal communications issue (for example, the ILAN port is not cabled)
- an optical disconnect, such as a fiber break, within the DOC span of control
- a circuit pack or module within the DOC photonic domain was replaced or restarted

This alarm appears only on the affected DOC shelf.

This alarm is cleared if the DOC Primary Sate is changed to OOS. However, this will not clear the underlying problem.

Note 1: It is recommended that DOC be placed OOS before inserting a standby CTM. If it is not, the DOC Action Failed: Monitor alarm can be raised after the insertion. In this case, the alarm will clear in approximately five minutes.

Note 2: When this alarm is raised, it indicates that DOC cannot determine the optimization state of the system. As a result, DOC maintains the current optimization state. If this alarm resulted from a comms issue, the optimization state displayed in DOC is most likely correct. If this alarm resulted from a system fault, such as a fiber cut, DOC may indicate the system is optimized when it is not. Once the fault is repaired, the system returns to its optimal state.

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 4-71 (continued)
DOC Action Failed: Monitor

Step	Action
1	If maintenance activities, such as module replacement, module restart, or fiber cut occurred while DOC automatic monitoring was running, then this alarm will be active. If this is the case, and the maintenance activities are complete, the alarm should clear autonomously during the next DOC Auto Monitor run. DOC Auto Monitor runs two minutes after the last DOC Auto Monitor operation completes.
2	Check for and clear active "DOC Invalid Photonic Domain" alarms using Procedure 4-76, "DOC Invalid Photonic Domain" on page 4-153 procedure in this document. After the DOC Invalid Photonic Domain alarm clears, the DOC Action Failed: Monitor alarm should clear autonomously during the next DOC Auto Monitor run.
3	**If** the original alarm has — **Then** cleared — the procedure is complete not cleared — go to step 4
4	Check for and clear any of the following alarms on all the network elements that are active within the DOC span of control: • Adjacency Far End Not Discovered • Adjacency Provisioning Error • Automatic Power Reduction Active • Automatic Shutoff • Circuit Pack Failed • Circuit Pack Mismatch • Circuit Pack Missing • Circuit Pack Unknown • Gauge Threshold Crossing Alert Summary • Optical Line Fail • OSC Loss of Signal • Shutoff Threshold Crossed ***Note:*** If the Optical Line Fail alarm is active, clear this alarm first. After the alarms in step 4 clear, the DOC Action Failed: Monitor alarm should clear autonomously during the next DOC Auto Monitor run.

Procedure 4-71 (continued)
DOC Action Failed: Monitor

Step	Action
5	**If** the original alarm has / **Then** cleared / the procedure is complete not cleared / go to step 6
6	Clear all other active alarms on the network elements within the DOC span of control. For optimal DOC operation, the system must be alarm free. Use the DOC **Logs** window to view the DOC logs to determine if another network element reported an error. Review the DOC logs from the other network element. Refer to the "Displaying the DOC logs for the summary table" procedure in Part 2 of *Configuration - Provisioning and Operating*, 323-1851-311. After the other alarms and conditions clear, the DOC Action Failed: Monitor alarm should clear autonomously during the next DOC Auto Monitor run.
7	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 4-72
DOC Action Failed: Optimize

Alarm ID: 550

Probable cause

This alarm is raised when DOC is unable to perform a manual or automatic re-optimization. The conditions that can cause this failure include:

- maintenance activities, such as module replacement, module restart, and fiber cut occurred while DOC auto monitoring was running
- an internal communications issue (for example, the ILAN port is not cabled)
- an optical disconnect, such as a fiber break, within the DOC span of control
- a circuit pack or module within the DOC photonic domain was replaced or restarted

This alarm appears only on the affected DOC shelf.

This alarm can be raised when DOC is operating in either enhanced mode or enhanced auto monitor only mode. The alarm hold off time is about 3 to 5 minutes.

This alarm is cleared if the DOC **Primary state** is changed to OOS. However, this will not clear the underlying problem.

> ***Note:*** It is recommended that DOC be placed OOS before inserting a standby CTM. If it is not or you click **Re-Optimize** during the standby CTM insertion, the DOC Action Failed: Optimize alarm can be raised after the insertion. In this case, the alarm will clear in approximately five minutes.

Impact

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

Procedure 4-72 (continued)
DOC Action Failed: Optimize

Prerequisites

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

Step	Action
1	If maintenance activities, such as module replacement, module restart, or fiber cut occurred while DOC auto re-optimize was running, then this alarm will be active. If this is the case, and the maintenance activities are complete, the alarm should clear autonomously during the next DOC auto re-optimize run.
2	Check for and clear active alarms using Procedure 4-76, "DOC Invalid Photonic Domain" on page 4-153 procedure in this document. After the DOC Invalid Photonic Domain alarm clears, the DOC Action Failed: Optimize alarm will clear autonomously during the next DOC Auto Monitor run.
3	**If** the original alarm has / **Then** cleared / the procedure is complete not cleared / go to step 4
4	Check for and clear any of the following alarms on all the network elements that are active within the DOC span of control: • Adjacency Far End Not Discovered • Adjacency Provisioning Error • Automatic Power Reduction Active • Automatic Shutoff • Channel Controller: Unexpected Loss Detected • Circuit Pack Failed • Circuit Pack Mismatch • Circuit Pack Missing • Circuit Pack Unknown • Gauge Threshold Crossing Alert Summary • Optical Line Fail • OSC Loss of Signal • Shutoff Threshold Crossed ***Note:*** If the Optical Line Fail alarm is active, clear this alarm first. After the preceding alarms clear, the DOC Action: Fault Detected alarm should clear autonomously during the next DOC auto re-optimize run.

Procedure 4-72 (continued)
DOC Action Failed: Optimize

Step	Action
5	**If** the original alarm has / **Then** cleared / the procedure is complete not cleared / go to step 6
6	Clear all other active alarms on the network elements within the DOC span of control. For optimal DOC operation, the system must be alarm free. Use the DOC **Logs** window to view the DOC logs to determine whether another network element reported an error. Review the DOC logs from the other network element. After the other alarms and conditions clear, the DOC Action Failed: Optimize alarm should clear autonomously during the next DOC auto re-optimize run.
7	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 4-73
DOC Action: Fault Detected

Alarm ID: 873

Probable cause

This alarm is raised during DOC automatic fault detection, when DOC detects a fault or the action is not completed. The conditions that can cause this failure include:

- maintenance activities, such as module replacement, module restart, and fiber cut occurred while DOC monitoring was running
- a module power value crossed the operating threshold
- a module within the DOC photonic domain was replaced or restarted
- an internal communications issue (for example, the ILAN port is not cabled)
- an optical disconnect (such as a fiber break) within the DOC span of control
- malfunctioning hardware
- incorrect provisioning

This alarm appears only on the affected DOC network element.

This alarm is cleared if the DOC **Primary state** is changed to OOS. However, this will not clear the underlying problem.

For the RLA module, if the VOA facility primary state is OOS, a “DOC Action: Fault Detected” alarm is raised.

Note 1: It is recommended that DOC be placed OOS before inserting the standby CTM. If it is not, and no DOC action is being executed, the DOC Action: Fault Detected alarm can be raised after the standby CTM insertion. In this case, the alarm will clear in approximately one minute.

Note 2: When this alarm is raised, the Channel Fault Status (CFS) is not necessarily updated.

Impact

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

Procedure 4-73 (continued)
DOC Action: Fault Detected

Prerequisites

To perform this procedure, you must:

- use an account with at least a level 4 UPC
- have the engineering documentation package (EDP) containing adjacency details

Step	Action
1	If maintenance activities, such as module replacement, module restart, or fiber cut occurred during the fault detection operation, then this alarm will be active. Ensure that the maintenance activities have completed.
2	Check for and clear active "DOC Invalid Photonic Domain" alarms using Procedure 4-76, "DOC Invalid Photonic Domain" on page 4-153 procedure in this document.
3	**If** the original alarm has / **Then** cleared / the procedure is complete not cleared / go to step 4
4	Check for and clear any of the following alarms on all the network elements that are active within the DOC span of control: • Adjacency Far End Not Discovered • Adjacency Provisioning Error • Automatic Power Reduction Active • Automatic Shutoff • Channel Controller: Unexpected Loss Detected • Circuit Pack Failed • Circuit Pack Mismatch • Circuit Pack Missing • Circuit Pack Unknown • Gauge Threshold Crossing Alert Summary • Optical Line Fail • OSC Loss of Signal • Shutoff Threshold Crossed ***Note:*** If the Optical Line Fail alarm is active, clear this alarm first.

Procedure 4-73 (continued)
DOC Action: Fault Detected

Step	Action

5 **If** the original alarm has **Then**

cleared	the procedure is complete
not cleared	go to step 6

6 Clear all other active alarms on the network elements within the DOC span of control. For optimal DOC operation, the system must be alarm free.

Use the DOC **Logs** window to view the DOC logs to determine if another network element reported an error. Review the DOC logs from the other network element.

7 **If** the original alarm has **Then**

cleared	the procedure is complete
not cleared	go to step 8

8 Verify, and if necessary, correct the following provisioned data (refer to the EDP):

- Tx and Rx adjacency parameters (**Adjacency type** and all power-related parameters)
- Line adjacency parameter (**Fiber type**)
- AMP optical facility parameters (**Primary state**, **Mode**, **Target Gain**, **Target Power**, and **Target Peak Power**)
- OPTMON facility parameters (**Primary state**)
- CHC facility parameters primary state

9 **If** the original alarm has **Then**

cleared	the procedure is complete
not cleared	go to step 10

10 Run DOC fault detection again (wait at least one minute).

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

—end—

Procedure 4-74
DOC Consecutive Re-Opt Threshold Crossed

Alarm ID: 874

Probable cause

This alarm is raised when DOC performs 25 re-optimizations in a row, with no separation by successful auto-monitoring cycles. That is, when DOC completes an optimization, the next monitoring cycle detects that another re-optimization is required. This can occur when there are continuous power fluctuations of greater than 1.0 dB, which causes DOC to detect that an optimization is required.

The optimization type can either be an 'SPPC-only optimization' or a 'full optimization', which includes both SPPC and incremental OSNR optimization. For more information on various optimization types, refer to *Photonic Layer Guide*, NTRN15DA.

This alarm appears only on the affected DOC shelf.

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
- have the engineering documentation package (EDP) containing provisioning details

Step	Action
1	If the alarm occurs during maintenance activities, such as module replacement, module restart, or fiber cut, complete the activities. After the maintenance activities are complete, wait five minutes. The alarm should clear autonomously during the next DOC auto re-optimize.
2	Check for and clear active"DOC Invalid Photonic Domain" alarms using Procedure 4-76, "DOC Invalid Photonic Domain" on page 4-153 procedure in this document. After the DOC Invalid Photonic Domain alarm clears, the DOC Consecutive Re-Opt Threshold Crossed alarm should clear autonomously during the next DOC auto re-optimize.

Procedure 4-74 (continued)
DOC Consecutive Re-Opt Threshold Crossed

Step	Action

3 **If** the original alarm has **Then**

cleared	the procedure is complete
not cleared	go to step 4

4 Check for and clear any of the following alarms on all the network elements that are active within the DOC span of control:

- Adjacency Far End Not Discovered
- Adjacency Provisioning Error
- Automatic Power Reduction Active
- Automatic Shutoff
- Circuit Pack Failed
- Circuit Pack Mismatch
- Circuit Pack Missing
- Circuit Pack Unknown
- Gauge Threshold Crossing Alert Summary
- Optical Line Fail
- OSC Loss of Signal
- Shutoff Threshold Crossed

Note: If the Optical Line Fail alarm is active, clear this alarm first.

After the above alarms clear, the DOC Consecutive Re-Opt Threshold Crossed alarm should clear autonomously during the next DOC auto re-optimize.

5 **If** the original alarm has **Then**

cleared	the procedure is complete
not cleared	go to step 6

6 Use any active Gauge Threshold Crossing Alert Summary alarms to help determine the exact cause of the power fluctuation. Fix the cause of the power fluctuation, and let the system re-optimize.

7 **If** the original alarm has **Then**

cleared	the procedure is complete
not cleared	go to step 8

Procedure 4-74 (continued)
DOC Consecutive Re-Opt Threshold Crossed

Step	Action
8	Clear all other active alarms on the network elements within the DOC span of control. For optimal DOC operation, the system must be alarm free. Use the DOC **Logs** window to view the DOC logs to determine which section is reporting not-optimal and for what reason, and if another network element reported an error. If necessary, review the DOC logs from the other network element. After the other alarms and conditions clear, the DOC Consecutive Re-Opt Threshold Crossed alarm should clear autonomously during the next DOC auto re-optimize.
9	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 4-75
DOC Domain Not Optimized

Alarm ID: 551

Probable cause

This alarm is raised when the system is not optimal, and the conditions that cause the alarm cannot be cleared by automatic re-optimization or automatic monitoring. The conditions that can cause this alarm include:

- a channel addition or deletion has failed (in the case of the alarm raised in a broadcast domain, the failed addition or deletion may have occurred within the primary domain where the traffic is broadcast)
- DOC has determined that the system is not optimal

This alarm appears only on the affected DOC shelf.

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 engineering documentation package (EDP) containing adjacency details

Step	Action	
1	**If**	**Then** go to
	the DOC Action Failed: Add alarm is active	"DOC Action Failed: Add" on page 4-133
	the DOC Action Failed: Delete alarm is active	"DOC Action Failed: Delete" on page 4-136
	the DOC Action Failed: Monitor alarm is active	"DOC Action Failed: Monitor" on page 4-139
	the DOC Action Failed: Optimize alarm is active	"DOC Action Failed: Optimize" on page 4-142
	the DOC Action Failed: Add alarm is active	"DOC Action Failed: Add" on page 4-133
	none of the above alarms are active	step 2

Procedure 4-75 (continued)
DOC Domain Not Optimized

Step	Action
2	Wait for the re-optimization or DOC Auto Monitor run to complete, or click the **Re-Optimize** button to trigger an immediate re-optimization. If the re-optimization fails, follow the appropriate alarm clearing procedure(s) in this document for any alarms raised as a result of the failed optimization.
3	**If** the original alarm has / **Then** cleared — the procedure is complete not cleared — go to step 4
4	Clear all other active alarms on the network elements within the DOC span of control. For optimal DOC operation, the system must be alarm free. Use the DOC **Logs** window to view the DOC logs to determine if another network element reported an error. Review the DOC logs from the other network element.
5	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 4-76
DOC Invalid Photonic Domain

Alarm ID: 552

Probable cause

This alarm is active during system lineup and test (SLAT), and only appears on the affected DOC shelf.

This alarm is raised when DOC cannot retrieve a valid Network Topology. Conditions that can cause this include:

- an internal communications issue (for example, the ILAN port is not cabled)
- an optical disconnect, such as a fiber break, within the DOC span of control
- an incorrectly provisioned shelf parameter
- an upstream circuit pack has undergone a restart operation. The alarm clears once the restart has completed.
- more than two DOC shelves are provisioned within the optical system
- a channel has been optimized in the system, and an upstream Tx on the same channel has been provisioned. To prevent this alarm from being raised, enter the second Rx adjacency for the reused wavelength before provisioning the second Tx adjacency.
- DOC is detecting that a DOC-controlled channel is expanded past its previous egress point. In this case, the alarm clears when DOC detects that the expanded DOC-controlled channel is contracted back to its original egress point.
- DOC is detecting that a DOC-controlled channel is contracted prior to its previous egress point. In this case, the alarm clears when DOC detects that the contracted DOC-controlled channel is expanded back to its original egress point.
- DOC is detecting that one or more DOC-controlled channels no longer has a topology present within the domain. This can occur on a database restore where there has been a capacity change since the database was collected, and where databases are restored only on a subset of nodes in the domain traversed by the modified channels.

Impact

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

Procedure 4-76 (continued)
DOC Invalid Photonic Domain

Prerequisites

To perform this procedure, you must:

- use an account with at least a level 3 UPC
- have the engineering documentation package (EDP) containing shelf details

Step	Action
1	**If** the system is / **Then** being SLATed: no action is required. The alarm clears after SLAT. The procedure is complete. already SLATed: go to step 2
2	Verify that both DOC site network elements are commissioned and connected to the network.
3	**If** the original alarm has / **Then** cleared: the procedure is complete not cleared: go to step 4
4	Verify that the shelf parameters are correctly provisioned. Correct any discrepancies.
5	**If** the original alarm has / **Then** cleared: the procedure is complete not cleared: go to step 6
6	If a channel has been optimized in the system and an upstream Tx on the same channel has been provisioned, remove the Tx adjacency or add an Rx adjacency to terminate the wavelength properly. DOC clears the alarm after the topology rebuilds. Refer to the “Editing facility parameters” procedure in Part 1 of *Configuration - Provisioning and Operating*, 323-1851-311.
7	**If** the original alarm has / **Then** cleared: the procedure is complete not cleared: go to step 8

Procedure 4-76 (continued)
DOC Invalid Photonic Domain

Step	Action
8	Check if any of the following alarms, which indicate an internal communications or equipment problem, are active within the DOC span of control, and clear them using the procedures in this document: • Circuit Pack Failed • Circuit Pack Mismatch • Circuit Pack Missing • Circuit Pack Unknown • Circuit Pack Upgrade Failed • Database Integrity Fail • Database Restore in Progress • Database Restore Failed • Database Commit Failed • Duplicate IP Address • Duplicate Shelf Detected • OSPF Adjacency Loss alarms • Packet Rate Limit Exceeded • Shelf Data Missing • Software Auto-Upgrade in Progress
9	If you have cleared any alarms in step 8, wait at least 15 minutes. **If** the original alarm has — **Then** cleared — the procedure is complete not cleared — go to step 10

Procedure 4-76 (continued)
DOC Invalid Photonic Domain

Step	Action
10	Check for and clear any of the following alarms on all the network elements that are active within the DOC span of control: • Adjacency Far End Not Discovered • Adjacency Mismatch • Adjacency Provisioning Error • Automatic Power Reduction Active • Automatic Shutoff • Optical Line Fail • OSC Loss of Signal ***Note:*** If the Optical Line Fail alarm is active, clear this alarm first.
11	If you have cleared any alarms in step 10, wait at least 15 minutes. **If** the original alarm has — **Then** cleared — the procedure is complete not cleared — go to step 12
12	Clear all other active alarms on the network elements within the DOC span of control. For optimal DOC operation, the system must be alarm free.
13	**If** the original alarm has — **Then** cleared — the procedure is complete not cleared — go to step 14
14	Use the DOC logs to determine if a DOC-controlled channel has expanded past its previous egress point. The **Overall Status** for the channel appears as "Network Topology unavailable". Refer to the Domain Optical Controller (DOC) procedures in Part 2 of *Configuration - Provisioning and Operating*, 323-1851-311. The DOC logs may show a message such as: `<date> <time> Invalid topology, controlled wavelength=<wavelength> starting in section <TID-SHELF-TX PathID> was expanded beyond its egress point.` If any expanded channels are identified, contract the channel back to its original egress point by placing the corresponding ADJ-RX facility OOS. Refer to the "Editing facility parameters" procedure in Part 1 of *Configuration - Provisioning and Operating*, 323-1851-311. The Domain Optical Controller **Destination TID-Shelf-RxPathID** column (specifically the last part of the entry) of the expanded channel indicates where to edit the ADJ-RX.

Procedure 4-76 (continued)
DOC Invalid Photonic Domain

Step	Action

15 **If** the original alarm has **Then**

cleared	the procedure is complete
not cleared	go to step 16

16 Use the DOC logs to determine if a DOC-controlled channel is contracted prior to its previous egress point. The **Overall Status** for the channel appears as “Network Topology unavailable.

The DOC logs may show a message such as:

```
<date> <time> Invalid topology, controlled
wavelength=<wavelength> starting in section <TID-SHELF-TX
PathID> was contracted from section <TID-SHELF-TX PathID> to
section <TID-SHELF-TX PathID>.
```

If any contracted channels are identified, expand the channel back to its original egress point by placing the corresponding ADJ-RX facility IS. Refer to the “Editing facility parameters” procedure in Part 1 of *Configuration - Provisioning and Operating*, 323-1851-311.

17 **If** the original alarm has **Then**

cleared	the procedure is complete
not cleared	go to step 18

18 Use the DOC window to view the DOC logs in order to determine if the current or another network element reported an error. If another network element has reported an error, review the DOC logs and provisioning of the other network element. Refer to the “Displaying the DOC logs for the summary table” procedure in Part 2 of *Configuration - Provisioning and Operating*, 323-1851-311.

ATTENTION

If the following DOC log is reported, refer to The “Unique log Identifier: 131330” procedure in *Fault Management - Customer Visible Logs*, 323-1851-840.

```
<date> <time> Invalid topology, missing previously controlled
wavelength=<wavelength> nm ingress=<TID-SHELF-TX PATHID>.
```

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

—end—

Procedure 4-77
Domain Optical Controller Disabled

Alarm ID: 1145

Probable cause

This alarm is raised when the Domain Optical Controller (DOC) facility has been put into an out-of-service state by the user or due to an upgrade activity.

This alarm is raised against the DOC facility itself.

Impact

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

Prerequisites

To perform this procedure, you must:

- be able to connect to the network element
- use an account with at least a level 3 UPC

Step	Action
1	Ensure that there is no software upgrade or network maintenance in progress on the network and the DOC facility can be put in-service state.
2	Manually put the DOC facility in-service from Site Manager, or use the RST-DOC TL1 command. Refer to the “Editing the DOC Settings” procedure in Part 2 of *Configuration - Provisioning and Operating*, 323-1851-311.
3	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 4-78
Dormant Account Detected

Alarm ID: 1372

Probable cause

This alarm is raised when there is at least one user account that has become dormant. This can be verified by opening the User Profile Application in Site Manager and looking at the "Password status" column. The alarm clears when there is "NO" DORMANT account left in the system.

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 Change the status of the dormant account to "Valid" account, "Disabled" account, or delete the dormant user account.

If you want to	**Then** go to
change the status of the dormant account to Valid	step 2
change the status of the dormant account to Disabled	step 3
Delete the dormant user account	step 4

2 In Site Manager, open a User Profile Application, select DORMANT account, select “Enable” button. This will change the password status from Dormant to Valid. Go to step 5.

3 In Site Manager, open a User Profile Application, select DORMANT account, select “Disable” button. This will change the password status from Dormant to Disabled. Go to step 5.

4 Site Manager, open a User Profile Application, select DORMANT account, select "Delete" button. This will delete the Dormant user account.

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

—end—

Procedure 4-79
Duplicate Adjacency Discovered

Alarm ID: 1071

Probable cause

This alarm is raised against an ADJ facility when two or more ports at the far-end have the same TID-SHELF-SLOT-PORT Addresses.

This alarm is also raised when you change the node name and then revert it back to the original name. The alarm clears after the CTM restart s completed or when you delete the original name in the Site Manager.

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 on the shelves with a duplicate Far End Address
- have a network plan or other documents that allow you to determine the correct Far End Address

Step	Action
1	Identify the shelves raising this alarm.
2	Note the TID-SHELF-SLOT-PORT that the alarm is raised against. In the Active Alarms table, the TID appears in the Network Element column, and the SHELF-SLOT-PORT appears after “ADJ-” in the Unit column.
3	In the Site Manager Equipment and Facility Provisioning application, examine the ADJ facility type lists for each applicable equipment and each shelf. Search for the TID-SHELF-SLOT-PORT noted in step 2 in the Expected Far End Address column. Note all matches found for all shelves within the siteID.
4	Determine which port has the correct Far End Address and remove the duplicate entries by setting their Expected Far End Address formats to NULL or the correct value.
5	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 4-80
Duplicate IP Address

Alarm ID: 545

Probable cause

This alarm is raised when the system detects another network element with the same IP address. The alarm occurs at the same time on all network elements that share the same IP.

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 on the nodes with a duplicate IP
- have a network plan or other documents that allow you to determine the correct IPs

Step	Action
1	Identify the network elements raising this alarm.
2	Determine from network plans or other documents which network element has the correct IP.
3	Log into the network element with the duplicate IP and correct the IP address as follows: • From the Configuration menu, open the **Comms Setting Management** • In the **Comms Setting Management** click on **Interfaces** tab • In the Interface Type drop down menu, select **IP**. • Choose the **Edit** button to change the IP address. If a remote log in is not possible, log in locally using the RS-232 serial modem port or the craft LAN port. **CAUTION** **Risk of loss of functionality** Ensure every network element has an unique IP. If you are changing the IP of a network element, ensure that the new IP is correct.
4	Ensure no other Duplicate IP Address alarms exist. If there are other Duplicate IP Address alarms, repeat this procedure.
5	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 4-81
Duplicate Primary Shelf

Alarm ID: 714

Probable cause

This alarm indicates there are duplicate primary shelves within a consolidated node, and is raised against all primary shelves within a consolidated node that are provisioned to be a primary shelf.

Note: A primary shelf will not auto-enroll or allow manual addition of new member shelves while a duplicate primary shelf exists on the same network.

Impact

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

Prerequisites

To perform this procedure, you must:

- use an account with at least a level 3 UPC
- be able to log into both shelves in the duplicate primary condition
- have a network plan or other documents that allow you to determine the correct primary shelves

Step	Action
1	Identify the network elements raising the alarm. Refer to the Procedure 2-12, "Identifying the module, pluggable module/port, or facility that has raised an alarm" on page 2-31.
2	Determine from network plans or other documents which shelf should be the primary shelf.
3	Log into the network element that is incorrectly enabled as a primary shelf.

Procedure 4-81 (continued)
Duplicate Primary Shelf

Step	Action
4	**CAUTION** **Risk of loss of functionality** Disabling the primary shelf will cause an administrative restart of the affected shelf. It will be unavailable for management during this time frame, and may require re-provisioning of the network element. Ensure you have removed the appropriate duplicate primary. Record all the provisioning information required to re-add the incorrectly provisioned member shelf to the consolidated node. Then delete the invalid primary shelf from the consolidated node. Refer to the “Deleting a member shelf of a consolidated node” procedure in *Administration and Security*, 323-1851-301.
5	Re-add the deleted shelf as a member shelf of the consolidated node with the **Primary shelf** parameter set to **Disabled**. Refer to the “Adding a shelf to a consolidated node” procedure in *Administration and Security*, 323-1851-301.
6	Ensure no other Duplicate Primary Shelf alarms exist. If there are other Duplicate Primary Shelf alarms, repeat this procedure for the new duplicate.
7	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 4-82
Duplicate Shelf Detected

Alarm ID: 70

Probable cause

This alarm is raised when the CTM detects another network element with the same shelf number and TID (also referred to as node name). The alarm occurs at the same time on all network elements that share the same shelf number and TID. Each CTM of the network element with the same shelf number and TID detects the condition.

After a CTM restart, this alarm is masked for 20 minutes.

Note: This alarm is raised to detect invalid layer 0 network topology and is only applicable to photonic shelves (shelves with OTSes provisioned). This alarm is raised only in photonic networks and cannot be raised in the TIDS only with POTS NEs.

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
- ensure that you are the only active user logged into the network element
- be able to log into the nodes that do not have a unique shelf number and TID
- have a network plan or other documents that allow you to determine the correct shelf numbers and TIDs

Step	Action
1	Identify the network elements raising the alarm. Refer to the Procedure 2-12, "Identifying the module, pluggable module/port, or facility that has raised an alarm" on page 2-31.
2	Determine from network plans or other documents which shelf has incorrectly provisioned information.

Procedure 4-82 (continued)
Duplicate Shelf Detected

Step	Action
3	Note that changing the shelf number requires decommissioning and recommissioning of the network element.

CAUTION
Risk of loss of functionality
Traffic and data communications will be lost
Decommissioning a shelf results in a loss of all traffic and data communications associated with the shelf that is being decommissioned.

CAUTION
Risk of loss of functionality
Ensure that you have identified the correct duplicate. A software configuration restart is required to properly recover, removing network visibility of the member node for the duration of the restart.

If the	**Then**
shelf **Name** (TID) is incorrectly provisioned	correct the shelf name. Refer to the “Editing the shelf number” procedure in *Administration and Security*, 323-1851-301.
Shelf number is incorrectly provisioned	record all the provisioning information required to recommission the shelf. Decommission the shelf and re-add it with the correct shelf number. Refer to the “Deleting all shelf provisioning” procedure in *Administration and Security*, 323-1851-301.

4 Ensure no other Duplicate Shelf Detected alarms exist. If other duplicate shelf alarms exist, repeat this procedure for the new duplicate(s).

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

—end—

Procedure 4-83
Duplicate Site ID

Alarm ID: 871

Probable cause

This alarm is raised when both the site identifier and the shelf number of two or more shelves are the same. The alarm occurs at the same time on all network elements that share the same site identifier and shelf number. (The alarm is not raised when the site identifier is 0.) Each CTM detects the condition and raises the alarm against the shelf.

After a CTM restart, this alarm can be masked for 20 minutes.

Note: You can edit the site identifier. However, changing the shelf number requires decommissioning and recommissioning of the network element.

Impact

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

Prerequisites

To perform this procedure, you must:

- use an account with at least a level 4 UPC
- be able to log into the nodes that do not have a unique site identifier and shelf number
- have a network plan or other documents that allow you to determine the correct site identifiers and shelf numbers

Step	Action
1	Identify the network elements raising the alarm. Refer to the Procedure 2-12, "Identifying the module, pluggable module/port, or facility that has raised an alarm" on page 2-31.

Procedure 4-83 (continued)
Duplicate Site ID

Step	Action

2

CAUTION
Risk of loss of functionality
Traffic and data communications will be lost
Decommissioning a shelf results in a loss of all traffic and data communications associated with the shelf that is being decommissioned.

If	Then go to
the site identifier is incorrectly provisioned	step 3
the shelf number is incorrectly provisioned	step 4.

3 Determine from network plans or other documents which network element has the incorrect **site identifier**. Edit the incorrect **site identifier** to be something unique from all other shelves in the network. Refer to the "Editing the nodal shelf parameters" procedure in *Administration and Security*, 323-1851-301.

Go to step 6.

4 Record all the provisioning information required to recommission the shelf. Decommission the shelf and re-provision it with the correct information. Refer to the "Deleting all shelf provisioning information for a standalone shelf or all shelves of a consolidated node" procedure in *Administration and Security*, 323-1851-301.

5 Verify that no other Duplicate Site ID alarms exist.

If	Then
no other Duplicate Site ID alarms exist	the procedure is complete
other Duplicate Site ID alarms exist	repeat step 1 to step 3 for the other duplicate(s). Go to step 6.

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

—end—

Procedure 4-84
Equipment Configuration Mismatch

Alarm ID: 970

Probable cause

This alarm is raised against a Power Input Module that does not support the shelf powering configuration (or current rating) specified by the **Provisioned shelf current** shelf attribute (provisioned shelf power configuration and feeder amperage). The alarm is also raised in the case of two mismatched Power Input Modules. Refer to the "Equipment provisioning validation based on shelf power capacity" section in *Administration and Security*, 323-1851-301, for further details.

This alarm is raised against mismatched fan modules (fan modules with different ordering codes).

Impact

Against fans

Critical, service-affecting (C, SA) alarm if two or more fan alarms exist
Major, non-service-affecting (M, NSA) alarm if one fan alarm exists

Against Power Input Cards

Major, 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 - 6500-T Series Shelves*, 323-1851-201.6.

Step	Action

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

1	**If** the alarm is raised against	**Then** go to
	fan modules	step 2
	Power Input Modules	step 5

Procedure 4-84 (continued)
Equipment Configuration Mismatch

Step	Action
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 cooling fan module with a fan that has the correct PEC. Refer to the “Replacing a shelf fan module or a SM fan module” procedure in *Fault Management - Module Replacement for T-Series*, 323-1851-546.
4	**If** the original alarm has / **Then** cleared / the procedure is complete not cleared / go to step 10
5	Retrieve and record the Provisioned shelf current value, and the inventory information for the Power Input Modules. Refer to the “Displaying node information” procedure in *Administration and Security*, 323-1851-301.
6	If the equipped Power Input Modules are the same type, set the **Provisioned Shelf Current** to a setting that is compatible with the Power Input Modules and their configuration but does not exceed the current rating of the feeders. Refer to the “Determining the provisioned shelf current value” procedure in *Administration and Security*, 323-1851-301.
7	**If** the original alarm has / **Then** cleared / the procedure is complete not cleared / go to step 8
8	Remove the alarmed Power Input Module or the Power Input Module that is not compatible with the required **Provisioned Shelf Current** setting. Refer to the “Replacing the Power Input Module” procedure in *Fault Management - Module Replacement for T-Series*, 323-1851-546. The “Circuit Pack Missing” alarm is raised for that Power Input Module, and the “Equipment Configuration Mismatch” alarm clears.
9	Insert a replacement Power Input Module into the shelf. Ensure that the equipped Power Input Modules are compatible with the retrieved **Provisioned Shelf Current** setting in step 5, and that all equipped Power Input Modules have the same amperage capacity (which is greater than or equal to the current associated with the Provisioned shelf current setting).
10	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 4-85
Error alarms (ETTP)

Use this procedure to clear alarms associated with the error alarms.

Excessive Error Ratio (ETTP)

Alarm ID: 1454

Probable cause

This alarm is raised against an ETTP facility of the 20x10G SFP+ PKT/OTN I/F, 2x100G CFP2 I/F, 40X10G SFP+ PKT/OTN I/F, or 5x100G/12x40G PKT/OTN I/F modules.

This alarm is raised against a facility when at least 20 percent of the received frames are errored each second for three consecutive seconds

The alarm clears when these conditions do not occur for 10 consecutive seconds.

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

- have an optical power meter with the same optical connectors as the network element
- if required, obtain a supported SFP+/CFP2/CFP2-ACO/QSFP+/QSFP28 optical transceiver module
- observe all safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - 6500-T Series Shelves*, 323-1851-201.6

Step	Action	
1	Verify if there are alarms of higher order from the alarm hierarchy. Refer to “Alarm hierarchies and alarm severities” in Chapter 3 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	From the **Class** field in the **Active Alarms** application, determine if the alarm is raised against an Ethernet or WAN facility.	

Procedure 4-85 (continued)
Error alarms (ETTP)

Step	Action

Alarm raised against an Ethernet facility

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

CAUTION
Risk of traffic loss
Ensure that the correct module is identified. Removing the wrong optical fiber causes a traffic loss on an in-service facility.

CAUTION
Risk of laser radiation exposure
Laser radiation is present on the optical fiber. Do not look into the optical fiber.

5 Use the optical power meter to measure the receive power on the fiber connected to the pluggables on the I/F modules.

For information about technical specifications (minimum and maximum receive optical power) for the SFP+/CFP2/CFP2-ACO/QSFP+/QSFP28 supported with the interface modules, refer to the *6500 - T_Series Shelves-Guide*, 323-1851-103.

6

If the receive power on the fiber is	**Then** go to
below the minimum receive optical power	step 7
between the minimum and maximum receive optical power	step 11
above the maximum receive optical power	step 12

Receive power is below the minimum receive optical power

7 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).

8

If the adjusted receive power is	**Then** go to
still below the minimum receive optical power	step 9
within range (between the minimum and the maximum receive optical power)	step 11

9 Remove the Tx optical fiber from the far-end subtending client equipment.

Procedure 4-85 (continued)
Error alarms (ETTP)

Step	Action
10	Measure the transmit power at the far-end subtending client equipment. • 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 13.

Receive power is between the minimum and the maximum receive optical power

11	Clean all connections at both ends of the optical fiber link following your company standards and re-attach the optical fibers. Go to step 13.

Receive power is above the maximum receive optical power

12	Add the necessary attenuation to reduce the receive power to a value between the minimum and maximum receive optical power.

Determining if the alarm cleared

13

If the original alarm has	**Then**
cleared	the procedure is complete
not cleared	replace the SFP+/CFP2/CFP2-ACO/QSFP+/ QSFP28 corresponding to the facility raising the alarm. Refer to the “Replacing a Pluggable module” procedure in *Fault Management - Module Replacement for T-Series,* 323-1851-546.

14

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 *Fault Management - Module Replacement for T-Series, 323-1851-546*.

15	Clean and re-attach the optical fibers. Refer to the cleaning connectors procedures in *Installation - 6500-T Series Shelves*, 323-1851-201.6.
16	If the alarm does not clear, contact your next level of support or your Ciena support group. The procedure is complete.

—end—

Procedure 4-86
Error alarms (STTP)

Use this procedure to clear alarms associated with errors on the STTP.

Signal Degrade (STTP)

Alarm ID: 1465

Probable cause

This alarm is raised when the received STTP signal is significantly degraded.

One of the following conditions can cause this alarm:

- excessive attenuation
- dirty optical fibers
- dirty connectors
- improper connector seating
- transmit laser degrade
- threshold set too high
- incorrect or faulty cabling at source end

Impact

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

Signal Fail (STTP)

Alarm ID: 1464

Probable cause

This alarm is raised when the received signal is degraded to the point where it is unusable, and the circuit pack is unable to detect the framing bytes in the received signal.

One of the following conditions causes this alarm:

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

Impact

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

The network element cannot clear a Loss of Signal alarm until a framed STTP 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.

Prerequisites

To perform this procedure, you must:

- have the optical fiber/cable 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 safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - 6500-T Series Shelves,* 323-1851-201.6

Step	Action
1	Verify if there are alarms of higher order from the alarm hierarchy. Refer to chapter 3 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 Procedure 2-12, “Identifying the module, pluggable module/port, or facility that has raised an alarm” on page 2-31.
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, someone must be present at the remote site.
6	Retrieve all alarms at the transmit end. Clear any higher order alarms using the appropriate procedure. The following alarms can be ignored: • RFI/RDI alarm if the local alarm is Signal Degrade or Signal Fail • Excessive Error Rate alarm if the local alarm is Excessive Error Rate

Procedure 4-86 (continued)
Error alarms (STTP)

Step	Action
7	Retrieve the SDTH and compare the SDTH with the network diagram. Refer to the "Displaying node information" procedure in *Administration and Security,* 323-1851-301.

If the provisioned SDTH	**Then**
matches the SDTH on the network diagram	go to step 8
does not match the SDTH on the network diagram	edit the SDTH as required. Refer to the "Editing the nodal system parameters" procedure in *Administration and Security*, 323-1851-301. then go to step 8.

8	Ensure that the cross-connect signal rate on the entire path matches the optical fiber/cable connection information.

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

10	Wear an antistatic wrist strap to protect the shelf from static damage. Connect the wrist strap to the ESD jack on the shelf.
11	**CAUTION** **Risk of traffic loss** Ensure that the correct module is identified. Removing the wrong optical fiber/cable drops all traffic on the local shelf.

CAUTION
Risk of laser radiation exposure
Laser radiation is present on the optical fiber. Do not look into the optical fiber.

Remove the optical fiber from the circuit pack raising the alarm and use the optical power meter to measure the receive power.

12	**If** the power is	**Then** go to
	below the receiver sensitivity for this circuit pack	step 13
	above the receiver sensitivity for this circuit pack	step 16

For information about circuit pack technical specifications, refer to the *6500 - T_Series Shelves- Guide,* 323-1851-103.

Procedure 4-86 (continued)
Error alarms (STTP)

Step	Action

Power is below the receiver sensitivity

13 Adjust the local attenuation, if equipped, to try to get the receive power above the receiver sensitivity level.

14

If the receive power after adjustment is	**Then** go to
still below the receiver sensitivity	step 15
above the receiver sensitivity but below the maximum receiver power	step 16

15 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	**Then**
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 17.
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 *Fault Management - Module Replacement for T-Series*, 323-1851-546. Go to step 17.

Power is above the receiver sensitivity

16 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

17

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 an SFP/SFP+/CFP2/CFP2-ACO/QSFP+/QSFP28 module” procedure in *Fault Management - Module Replacement for T-Series,* 323-1851-546. Then, clean and re-attach both optical fibers. Refer to the cleaning connectors procedures in *Installation - 6500-T Series Shelves*, 323-1851-201.6.

Procedure 4-86 (continued)
Error alarms (STTP)

Step	Action	
18	**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 *Fault Management - Module Replacement for T-Series,* 323-1851-546. Then, clean and re-attach both optical fibers. Refer to the cleaning connectors procedures in *Installation - 6500-T Series Shelves*, 323-1851-201.6.
19	If the alarm does not clear, contact your next level of support or your Ciena support group.	

—end—

Procedure 4-87
ESI alarms

Use this procedure to clear alarms associated with ESI-A or ESI-B.

AIS (ESI)

Alarm ID: 104, 111

Probable cause

This alarm is raised when a CTM detects an AIS on the incoming ESI timing reference signal. The upstream equipment generates an AIS signal to tell downstream equipment that a failure occurred. This alarm indicates that the ESI source (external clock source equipment) for this shelf has a failure. This is not applicable to a 2 MHz ESI signal.

Impact

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

The ESI source is not available to the shelf. If this is the active source, a timing protection switch occurs if another source is provisioned and available. Otherwise, the shelf enters timing holdover mode.

Excessive Error Rate (ESI-A/B)

Alarm ID: 106, 112

Probable cause

This alarm is raised when a Bipolar Violation (BPV) on the incoming ESI timing reference signal is detected. This alarm indicates that the signal from an ESI source (external clock source equipment) is degraded. If this timing source is the active timing reference, the SM will switch to an alternate reference if it is available.

A bipolar violation refers to two consecutive positive or negative pulses without an opposite polarity pulse in between. The alarm is raised when this error occurs at a rate greater than 10^{-3}.

Note 1: This procedure assumes that the signal has been in service and is alarm free. Ensure that line coding provisioning for the shelf and external timing source is correct.

Note 2: Not applicable to a 2 MHz ESI signal.

Impact

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

Note: The ESI source is not available to the shelf. If this is the active source, a timing protection switch occurs if another source is provisioned and available, or the shelf enters timing holdover mode.

Loss of Frame (ESI)

Alarm ID: 103, 110

Probable cause

This alarm is raised when the CTM detects a loss of frame on the incoming ESI timing reference signal.

This procedure assumes that the signal has been in service and is alarm free. Ensure that frame provisioning for the shelf and ESI source (external clock source equipment) is correct. This is not applicable to a 2 MHz ESI signal.

Impact

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

The ESI source is not available to the shelf. If this is the active source, a timing protection switch occurs when another source is provisioned and available. Otherwise, the shelf enters timing holdover mode.

Loss of Signal (ESI)

Alarm ID: 102, 108

Probable cause

This alarm is raised when the CTM cannot detect a signal on the incoming ESI timing reference.

This alarm can also be raised when you perform a cold restart on a shelf connected in a row of multiple shelves with ESOs connected to the ESIs. The alarm remains active on all remaining shelves until the synchronization recovers.

Impact

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

The ESI source (external clock source equipment) is not available to the shelf. If this is the active reference, a timing protection switch occurs when another source is provisioned and available. Otherwise, the shelf enters timing holdover mode.

Prerequisites

To perform this procedure, you must observe all safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - 6500-T Series Shelves,* 323-1851-201.6.

Procedure 4-87 (continued)
ESI alarms

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**	**Then** go to
	there is an AIS, LOF, Excessive Error Rate, or LOS condition (AIS, Excessive Error Rate, and loss of frame do not apply to a 2 MHz signal)	step 3
	the signal is valid	step 4
3	The problem is with cabling or the external clock source equipment and the 6500 shelf is reporting a valid condition. Perform troubleshooting on the cabling or external clock source equipment according to your company procedure. The procedure is complete.	
4	Verify which CTM is the synchronization master by checking the L1 Sync LED on the faceplate of the CTM.	
5	If the L1 Sync LED on the Sync master CTM is yellow, operate a manual switch on the active CTM from the Protection Status application. If the CTM switch clears the alarm or L1 Sync LED on the newly active CTM is green, perform another manual switch on the newly active CTM card to confirm the faulty CTM.	
6	If any alarm is still active, replace the faulty CTM. Refer to the equipment replacement procedures in *Fault Management - Module Replacement*, 323-1851-546.	
7	If the alarm does not clear, contact your next level of support or your Ciena support group. **—end—**	

Procedure 4-88
Event Log full

Alarm ID: 1890, 1900, 1910, 1920

Probable cause

This alarm is raised when the event log for the Integrated Test Set is full.

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	In the Test Configuration tab, click the **Stop Test** button to stop the test.
2	Click **Clear Results** to clear the test results.
3	Restart the test. Refer to the “Performing a test with the integrated test set” procedure in Part 1 of *Configuration - Provisioning and Operating,* 323-1851-311.
4	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 4-89
Facility Provisioned Mismatch

Alarm ID: 101

Probable cause

This alarm is raised on a PTP facility of CFP2-ACO pluggable module when the provisioned Tx Power or Modulation format is outside of what is supported by the provisioned module. This alarm is raised during a reconfiguration of the CFP2-ACO plug (during In-Service ED-EQPT).

This alarm is also raised during SP restart if the provisioned Tx Power or Modulation scheme is outside of the XML data range.

Impact

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

Step	Action
1	Edit the modulation format and Provisioned Tx Power facility parameter values to the supported values on each CFP2-ACO pluggable module. Refer to PTP facility parameters table in Part 1 of Configuration - Provisioning and Operating for T-Series, 323-1851-311 for the supported parameter values on each CFP2-ACO pluggable PEC.
2	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 4-90
Fan Failed

Alarm ID: 224

Probable cause

This alarm is raised when a cooling fan module is equipped in the shelf but has failed

For cooling fan modules that have more than one integrated fan, the shelf will raise the alarm when one or more of the integrated fans is in a failed state.

Note: The red LED will be ON during a single power zone failure if a fan is powered by that zone. In this case, address the power feed failure first to restore the complete power to the fan.

Impact

Critical, service-affecting (C, SA) alarm

Prerequisites

To perform this procedure, you must observe all safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - 6500-T Series Shelves*, 323-1851-201.6.

ATTENTION

Ensure that you have the correct fan type. After removal of a cooling fan module, the cooling fan module must be replaced within 30 seconds to prevent the circuit packs from overheating due to insufficient airflow. Have a replacement fan module ready before removing the fan module.

CAUTION

Risk of traffic loss

Risk of damage to circuit packs and modules

Do not attempt to cause this alarm to be raised by removing any cooling fan modules or filler cards or by blocking the shelf air inlet or exhaust ports as it will compromise shelf cooling. A shelf with a compromised cooling system may result in circuit pack or module failures prior to the assertion of a High Temperature Warning or High Temperature alarm.

Procedure 4-90 (continued)
Fan Failed

Step	Action

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

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 Check whether the identified fan module is missing, has failed, or is not compatible with the shelf or its equipped Power Input Cards. The fan status is indicated by the LEDs on each fan module.

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

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

3

If the fan module	**Then** go to
has failed	step 4
is missing	step 7

Verifying the fan module

4 Verify that the fan module is fully inserted.

5 Make any necessary adjustments.

6

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

Procedure 4-90 (continued)
Fan Failed

Step	Action

Installing/replacing the fan module

7 Install the missing fan module(s) or replace the failed fan module(s). Refer to the “Replacing a shelf fan module or a SM fan module” procedure in *Fault Management - Module Replacement*, 323-1851-546.

CAUTION
Risk of traffic loss
Risk of personal injury
Use the handle on the front of the fan module to extract it. Do not hold or carry the fan modules in a manner that could cause detrimental contact to the fan blades (which will stop rotating when power is disconnected due to module extraction). You can provide extra support for the fan modules by holding the bottom of the fan module during extraction and insertion. A fan module should be handled by firmly grabbing the left and right sides taking care not to touch the fan blades.

Ensure you use the correct fan type.

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

—end—

Procedure 4-91
Fan Missing

Alarm ID: 223

Probable cause

This alarm is raised on a shelf when a fan module is missing.

Impact

Critical, service-affecting (C, SA) alarm

Prerequisites

To perform this procedure, you must observe all safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - 6500-T-Series Shelves*, 323-1851-201.6.

Step	Action

DANGER

Risk of eye injury

Wear eye protection such as safety goggles or safety glasses with side guards when you work with fan modules or in proximity to the shelf air exhaust.

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 Insert the fan module into the shelf. Refer to the “Replacing a SM fan module” procedure” procedure in *Fault Management - Module Replacement for T-Series,* 323-1851-546.

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

—end—

Procedure 4-92
Far End Client Signal Fail

Alarm IDs: 695, 1488, 1977

Probable cause

For the 20x10G SFP+ PKT/OTN I/F, 2x100G CFP2 I/F, or 2x100G WL3n I/F modules, this alarm is raised against the WAN or ODUCTP facility when the far-end mate port for this service is experiencing a client Rx signal fault.

For circuit packs with WAN facilities, this alarm is raised when the far-end mate port for this service is experiencing a client Rx signal fault.

Impact

Critical, service-affecting (C, SA) alarm, if the alarm is raised on an active traffic path
minor, non-service-affecting (m, NSA) alarm, if the alarm is raised on an inactive traffic path

Prerequisites

To perform this procedure, you must:

- observe all safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - 6500-T Series Shelves*, 323-1851-201.6
- have the optical fiber connection information (that is, how the optical modules on each network element connect to other network elements)
- have a fiber cleaning kit
- have the engineering documentation package (EDP) containing shelf details

Step	Action
1	Verify the fibers are properly connected and not crossed, looped back, or misconnected at the corresponding far-end client circuit pack.
2	Retrieve alarms from the corresponding far-end client circuit pack. Refer to the Procedure 2-2, “Retrieving active alarms for one or more network elements” on page 2-13.
3	Use the appropriate alarm clearing procedure to clear any alarms raised at the far-end client circuit pack.
4	If the alarms do not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 4-93
Far End Protection Line Fail

Alarm IDs: 1392

Probable cause

This alarm is raised to indicate that a protection line signal failure was received in the APS bytes sent by the far-end protection engine. This indicates that the far-end protection engine cannot switch traffic to the protection line because a fault was detected downstream. This alarm is raised for a 1+1 OTN configuration protection group.

This alarm is cleared if a signal failure condition prevents the reception of valid APS bytes.

This alarm only applies to bidirectional mode protection switching.

Impact

Major, 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 - 6500-T Series Shelves*, 323-1851-201.6.
- ensure that you have the optical fiber connection information on how the optical modules on each network element connect to other network elements

Step	Action
1	Starting at the far-end network element and going upstream, check all network elements for alarms against the protection line. Refer to the Procedure 2-2, “Retrieving active alarms for one or more network elements” on page 2-13. Clear all far-end alarms related to the protection line.
2	Clear all other unexpected standing alarms on the local 6500 network element by following the related trouble clearing procedures.
3	If the “Far End Protection Line Fail” alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 4-94
Fiber Loss Detection Disabled

Alarm ID: 1581

Probable cause

This alarm is raised when the “High Fiber Loss Detection Alarm” system parameter is set to Disabled on a shelf equipped with a Colorless OADM OTS. Colorless OADM OTS requires High Fiber Loss Detection.

The “High Fiber Loss Detection Alarm” parameter can be found in the Site Manager Node Information application under the System tab.

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	Enable the “High Fiber Loss Detection Alarm” system parameter. 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 4-95
Fiber Type Manual Provisioning Required

Alarm ID: 907

Probable cause

This alarm is raised against a ADJ-LINE facility when the fiber type for the line adjacency is set to ‘Unknownfiber type’ (not provisioned), putting the line adjacency out of service.

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 **Fiber Type** value of the alarmed line adjacency to a value other than ‘Unknownfiber type’. Refer to the “Editing facility parameters” procedure in Part 1 of *Configuration - Provisioning and Operating*, 323-1851-311.
2	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 4-96
Filter Replacement Timer Expired

Alarm ID: 1580

Probable cause

This alarm is raised to indicate that you must replace the air filter in the shelf.

The default value of the replacement time interval is 24 months.

On a 6500 T-Series shelf, there is one air filter for the shelf and one air filter for the switch modules. Both air filters need to be replaced at the same time.

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 - 6500-T Series Shelves*, 323-1851-201.6
- obtain a replacement air filter to install in the empty slot

Step	Action
1	Choose your next step. **If** you want to / **Then** go to replace the filter — step 2 set a new replacement time — step 3 reset the filter timer — step 4 disable the filter timer — step 5
2	Replace the air filter in the shelf. Refer to the “Replacing a shelf air filter or a SM air filter” procedure in *Fault Management - Module Replacement for T-Series*, 323-1851-546. Go to step 4.
3	Provision a new replacement time interval using Site Manager. Refer to the “Resetting the air filter replacement timer” procedure in *Administration and Security*, 323-1851-301. Go to step 6.
4	Reset the timer. The timer will reset to the value given by the replacement time interval. Refer to the “Resetting the air filter replacement timer” procedure in *Administration and Security*, 323-1851-301. Go to step 6.

Procedure 4-96 (continued)
Filter Replacement Timer Expired

Step	Action
5	Disable the timer. Refer to the “Editing the nodal shelf parameters” procedure in *Administration and Security*, 323-1851-301. ***Note:*** Disabling and re-enabling the timer that has already expired does not cause the timer to reset. The alarm is raised after re-enabling the timer.
6	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 4-97
Flash Banks Mismatch

Alarm ID: 222

Probable cause

This alarm is raised when an upgrade is interrupted. If an upgrade is interrupted, there can be different loads present on the CTM.

The alarm can also be raised during a CTM replacement procedure when a software load on either the flash bank of the network element is not up to date with respect to the release that is running on the network element.

Impact

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

Step	Action
1	If the alarm is raised during a CTM replacement, it will clear once the CTM replacement procedure is completed.
2	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 4-98
Frequency Out of Range (ETTP, STTP)

Alarm ID: 1615, 1616

Probable cause

This alarm is raised when the frequency limits exceed the IEEE 802.3 Tx frequency offset specifications of +/- 20ppm for 10GBASE-W and +/-100ppm for 10GBASE-R.

This alarm applies to ETTP and STTP facility client types on the 40x10G SFP+ PKT/OTN IF, 5x100G/12x40G QSFP PKT/OTN IF, 20x10G SFP+ PKT/OTN I/F and 2x100G CFP2 I/F modules.

Impact

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

Step	Action
1	If possible, clear all ETTP and STTP alarms from the network.
2	If the alarm does not clear, verify the subtending equipment to ensure that it meets the frequency specification. If the equipment does not meet the specification, change the client signal to use subtending equipment that is within specifications.
3	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 4-99
Gauge Threshold Crossing Alert Summary

Alarm ID: 724, 725, 726, 1972

Probable cause

This is a summary alarm for each AMP, VOA, and OPTMON facility, and is raised if one or more of the physical gauge power values crosses its provisioned PM threshold.

This alarm is masked by the Loss of Signal and Circuit Pack Failed alarms.

ATTENTION

PM thresholds stored in PM Profiles define the maximum deviation from the currently set baseline for a gauge power value. Resetting baselines of gauge power values is normally done by DOC, but may also be manually triggered by the user.

The typical cause for this alarm is reduced power levels on the port reporting the alarm. Conditions that can result in reduced power levels at a port include:

- a PM threshold setting that is too low for a gauge power value
- a faulty or incorrectly provisioned transmitter module
- a faulty or incorrectly provisioned receive module
- an optical signal degradation caused by a bent optical fiber or dirty optical connector
- improper optical cable mating
- a disconnected optical fiber at the amplifier output
- an optical fiber cut
- a disconnected or missing termination
- misprovisioning of an amplifier resulting in excessive power being injected into the mid-stage fiber-plant
- a power value has been reported as outside of range (OOR) and the baseline has been set as out of range (OOR) and the power fluctuates to a non-OOR value, then the alarm can be raised
- channels are added in a downstream domain of a branched network

Use this alarm to resolve the causes of the threshold crossings before a service-affecting problem occurs.

Procedure 4-99 (continued)
Gauge Threshold Crossing Alert Summary

Note: If this alarm is raised for amplifiers immediately after an upgrade, the alarm can be cleared by resetting the baseline.

This alarm clears automatically when all gauge readings fall within their threshold boundaries.

Note: This alarm can be cleared manually from the Site Manager PM screen by resetting the baseline.

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 safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - 6500-T Series Shelves*, 323-1851-201.6
- have the engineering documentation package (EDP) containing shelf details
- have a fiber cleaning kit
- obtain a replacement module or fiber patchcord, if required

Step	Action	
1	**If** this alarm	**Then**
	was raised as a result of a maintenance activity or during SLAT and it is expected	no action is required. The alarm will clear when the maintenance activity or SLAT is completed. The procedure is complete.
	is not expected	continue with step 2
2	Verify that the PM threshold values for the alarmed facility are correctly provisioned. Adjust the value if required.	
3	**If** the original alarm has	**Then**
	cleared	the procedure is complete
	not cleared	go to step 4

Procedure 4-99 (continued)
Gauge Threshold Crossing Alert Summary

Step	Action	
4	**If**	**Then**
	channels were added or deleted on downstream domains	manually update of TCA thresholds. See *Performance Monitoring*, 323-1851-520. If the alarm does not clear, go to step 5
	otherwise	go to step 5
5	Verify that the optical power is within range. If both the minimum and maximum values are outside of range, you can enable automatic in-service (AINS) for the facility until a valid signal is present. Refer to the “Editing facility parameters” procedure in Part 1 of *Configuration - Provisioning and Operating*, 323-1851-311. If the power level is too close to the Input Loss of Signal Threshold configured in the Amp properties, the alarm is going to be toggled. In this case, edit the Threshold 1 dB below the threshold level on the Amp settings.	
6	**If** the original alarm has	**Then**
	cleared	the procedure is complete
	not cleared	go to step 7
7	Using the alarm details for the Gauge Threshold Crossing Alert Summary alarm, note the Unit and Class against which the alarm is raised.	
8	Retrieve the PMs for the Shelf, Type, and Facility based on the information noted in step 7.	
9	From the PM application, note the facility parameter that has an Untimed value that crossed the threshold value.	
10	Check for and clear any of the following alarms on all network elements before clearing this alarm: • Automatic Power Reduction Active • Automatic Shutoff • Input Loss of Signal • Loss of Signal (OPTMON) • Optical Line Fail • OSC Loss of Signal • Output Loss of Signal • Shutoff Threshold Crossed	

Procedure 4-99 (continued)
Gauge Threshold Crossing Alert Summary

Step	Action

11 **If** the original alarm has **Then**

cleared	the procedure is complete
not cleared	go to step 12

12 Determine if there are other Gauge Threshold Crossing Alert Summary alarms raised in the network and begin by troubleshooting the most upstream Gauge Threshold Crossing Alert Summary alarm. To troubleshoot the most upstream Gauge Threshold Crossing Alert Summary alarm, verify the optical patchcord connected to the port reporting the alarm.

Note: Ensure the optical patchcord 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 *Installation - 6500-T Series Shelves*, 323-1851-201.6.

13 **If** the original alarm has **Then**

cleared	the procedure is complete
not cleared	go to step 14

14 If the alarm is reported against the OPIN parameter of a Line A In (port 8) facility and the OPR parameter of an OSC A Out (port 4) facility, then verify the outside fiber plant.

15 If the alarm is reported against the OPOUT parameter of CMD Channel In VOA facility, make sure that the transmitting subtending equipment is functioning correctly and transmitting a valid signal.

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

—end—

Procedure 4-100
GCC0/GCC1 Link Failure

Alarm ID: 1723, 1724, 1725

Probable cause

This alarm is raised when the network element communications fail on the ITU-T G.709 general communication channel (GCC0, GCC1) link. This alarm can also be raised if the facility (ODUCTP, ODUTTP, or OTUTTP) is physically looped back (Tx interface connected to Rx interface).

For all circuit packs, the GCC link is controlled by lower layer SDCC and not a circuit (IISIS or OSPF). Therefore, even if there are no IISIS or OSPF circuits provisioned, the GCC link is still up between near-end and far-ends and no GCC Link Failure alarm is raised.

If only one end of a GCC PPP link is provisioned while the other end is not, the link state of the PPP link at the first end will not be up. Therefore the alarm is raised on the first end. The alarm will be cleared after the PPP link is provisioned at the other end.

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 - 6500-T Series Shelves*, 323-1851-201.6
- have the optical fiber connection information (that is, how the optical modules on each network element connect to other network elements)
- clear all remote alarms present against the optical fiber
- use an account with at least a level 3 UPC

Step	Action
1	Identify the facility raising the alarm. Refer to the Procedure 2-12, “Identifying the module, pluggable module/port, or facility that has raised an alarm” on page 2-31.
2	Use the optical fiber connection information to identify the network element and the module that is the source of the signal reporting the alarm.
3	Wait five minutes after the alarm was raised in case a CTM or interface circuit pack restart at the remote terminal caused the alarm.

Procedure 4-100 (continued)
GCC0/GCC1 Link Failure

Step	Action

4 **If** the original alarm has **Then**

cleared	the procedure is complete
not cleared	go to step 5

5 Ensure the following comms parameters (in the Site Manager **Comms Setting Management** application) exist at each end of the GCC0/GCC1 link for the circuit pack reporting the alarm:

— GCC0/GCC1 PPP interface (under **Interfaces**, **Interface type**=PPP)

— GCC0/GCC1 Lower Layer DCC/GCC interface (under **Interfaces**, **Interface type**=Lower Layer DCC/GCC)

Refer to the "Retrieving communications settings" procedure in Part 1 of *Configuration - Provisioning and Operating*, 323-1851-311.

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 Log into the remote network element using the external IP address.

- If the login is successful, go to step 11.
- If the login fails, go to step 8.

8

If	Then
the remote network element is only accessible through GCC0/GCC1	the login may not be possible, as the GCC0/GCC1 has failed. Go to step 9
otherwise	go to step 11.

9 Replace the required module at the remote site determined in step 2. Refer to the equipment replacement procedures in *Fault Management - Module Replacement for T-Series*, 323-1851-546.

10 **If** the original alarm has **Then**

cleared	the procedure is complete
not cleared	go to step 11

11 Replace the required module at the network element originally reporting the alarm. Refer to the equipment replacement procedures in *Fault Management - Module Replacement for T-Series*, 323-1851-546.

12 If the alarm is still active, the alarm can be the result of mis-fibering causing a physical loopback along the photonic layer. Check the optical fibering along the path of the channel.

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

—end—

Procedure 4-101
High Fiber Loss

Alarm ID: 1239

Probable cause

This alarm is raised against the originating ADJ-FIBER facility when the measured loss between this port and the far-end port is greater than either of the provisioned loss thresholds. A 0.5 dB hysteresis is also applied, which prevents the alarm from clearing until the measured loss has gone below the threshold(s) by more than 0.5 dB. The calculated fiber loss is reported against the ADJ-FIBER facility.

For the WL3n Tx to CCMD 16x12, this alarm is raised against the CCMD 16x12 ADJ-FIBER (receive direction).

For a Photonic configuration, this alarm is supported for the following interconnections:

- RLA to another RLA passing through FIM
- RLA to same RLA passing through FIM MPO loopback connector
- RLA to same RLA passing through FIM LC loopback connector
- RLA to “AMP4 Module” passing through FIM
- “AMP4 Module” to RLA passing through FIM
- “AMP4 Module” to same “AMP4 Module” passing through FIM MPO loopback connector
- CCMD 16x12 to “AMP4 Module” passing through an MPO cable
- CCMD 8x4 to “RLA Module” passing through AMP4 and FIM
- “AMP4 Module” to CCMD 16x12 passing through an MPO cable

For the control and Connection Validation applications to work properly, appropriate system parameters must be enabled. The “Shelf Synch” is set to “Yes”, the “Dark Fiber Loss Measurement” is set to “On” and the “High Fiber Loss Detection” Alarm is set to “Enabled”. The “Dark Fiber Loss Measurement” and the “High Fiber Loss” Alarm Detection Alarm parameter in the Site Manager Node Information application and the System tab are enabled by default.

Procedure 4-101 (continued)
High Fiber Loss

Note: For the colorless CMD configurations in 6500 Release11.1, when the CCMD and the transponder are on different shelves, the Fiber Loss value will not be available between the CCMD Tx port and the transponder port on SPLI-managed adjacencies. If there is an actual high fiber loss condition on the fiber, the Fiber Loss value is displayed as N/A instead of an actual value and no “High Fiber Loss” alarm is raised. In this case, the fiber loss can either be measured manually or by comparing the transponder provisioned Tx power value in the PTP facility and the received optical power value on the CCMD Tx port (OPR-OTS PM value on the OPTMON facility of the CCMD Tx port).

Impact

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

When the fiber loss exceeds the user-provisioned Fiber Loss Minor Threshold (default is 3 dB), the alarm is raised with a minor severity. “Fiber Loss Minor Threshold” threshold possible values are 1 to 30 with 0.01 resolution.

When the fiber loss exceeds the user-provisioned Fiber Loss Major Threshold (default is 10 dB), the alarm is raised with a Major severity. “Fiber Loss Major Threshold” threshold possible values are 1 to 30 with 0.01 resolution, but must be greater than the “Fiber Loss Minor Threshold” value.

For Connection Validation applications on dark fibers, this alarm is always raised as Minor, non-service-affecting (m, NSA) alarm when:

- fiber loss exceeds the user provisioned fiber loss minor threshold (default is 3 dB)
- fiber loss exceeds the user provisioned fiber loss major threshold (default is 10 dB)
- input power is considered Out of Range, for which the fiber loss displays as “LOS” in the ADJ-FIBER facility.

Prerequisites

To perform this procedure, you must:

- use an account with at least a level 3 UPC
- observe all safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - 6500-T Series Shelves*, 323-1851-201.6

Procedure 4-101 (continued)
High Fiber Loss

- have a fiber cleaning kit (for Photonic configurations, both MPO and LC cleaning kits are needed. See the “Cleaning connectors” chapter in *Installation - 6500-T Series Shelves*, 323-1851-201.6
- obtain a fiber patchcord, if required

Step	Action

1

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

Check the fibers involved in the High Fiber Loss alarm (all fibers between the port where the alarm is raised and the port specified as the Far End Address for this adjacency):

- For a Photonic configuration, verify that the MPO cable for the subfiber that has the alarm and the far-end of the MPO cable are connected properly. The far-end location of the MPO cable can be determined by verifying the MPO adjacency far-end Address where the alarm is raised. Verify that the CMD MPO cables are fibered to the AMP4 and the AMP4 is fibered to the FIM.

2 Determine the far-end MPO adjacency from the local subfiber adjacency far-end address. Check that the MPO cable is connected properly. Determine the far-end of this MPO cable by looking at the MPO adjacency far-end address.

3 Check that the MPO cable is connected properly to the FIM. Check that the loopback connector is connected properly.

4

If the original alarm has	**Then**
cleared 5 minutes after insertion of the fiber	the procedure is complete
not cleared	go to step 5

Procedure 4-101 (continued)
High Fiber Loss

Step	Action

5 **If** | **Then** go to

If	Then go to
the alarm is raised against an RLA sub-fiber	step 6
the alarm is raised against a CCMD sub-fiber	step 14
the alarm is raised against an MPO cable connecting a CCMD16x12	step 19
otherwise	step 19

6 If the RLA subfiber loopbacks to itself, clean the loopback connector. Refer to the “Cleaning connectors” chapter in *Installation - 6500-T Series Shelves*, 323-1851-201.6.

7 If the alarm did not clear five minutes after insertion of the fiber, clean the MPO cables between the RLA and the FIM on both ends.

CAUTION
Risk of traffic loss
Ensure to switch any traffic that is on any of the other subfibers on the MPO, away from the ROADM.

8 If the RLA subfiber goes to another RLA or AMP4 on the CCMD16x12 or CCMD 8x4, clean the MPO cables between the RLA and the FIM. Clean the MPO cable of the newly installed module first.

CAUTION
Risk of traffic loss
Ensure to switch any traffic that is on the MPO cables. The traffic will be lost when you clean the cables.

9 **If** | **Then** go to

If	Then go to
the fiber adjacency points back to itself	step 10
otherwise	step 19

10 Verify that the actual fibering matches the is provisioned fibering.

11 Using the Shelf Level View application in Site Manager, determine which MPO to clean.

12 Remove and clean the MPO or LC loopback as applicable.

13 Clean the FIM port and replace the MPO loopback. Go to step 23.

14 Clean the Common MPO port. Refer to the “Cleaning connectors” chapter in *Installation - 6500-T Series Shelves*, 323-1851-201.6.

15 Clean the MPO cable and reconnect it to the card.

Procedure 4-101 (continued)
High Fiber Loss

Step	Action
16	Clean the MPO port on the FIM.
17	Clean the MPO cable and reconnect it to the FIM.
18	If the alarm is raised on the CCMD16x12, clean the jumper fibers on the dark fiber or the Manual loopback path fiber as follows.

a. If you performed a manual loopback in a CDC configuration and the alarm on a jumper subfiber is raised on a dark fiber, clean the jumper MPO cable.

CAUTION
Risk of traffic loss
Ensure to switch traffic that is on any of the subfibers.

b. Verify the MPO loopback connector that the subfiber passes through in the FIM

The ordering of the cleaning must be:

— Verify the loopback connector first since this does not impact traffic

— Verify the jumper cable next

The waiting period of five minutes does not apply here since there is no automatic test done by connection validation. Re-run the Manual Loopback test again to clear the alarm.

c. If you performed a manual loopback and the alarm is raised on one of the subfibers in the path, cancel the manual loopback test. Make sure you wait up to five minutes after the completion of the manual loopback before verifying this.

d. If the alarms is raised on the jumper subfibers, clean the cable.

CAUTION
Risk of traffic loss
Ensure to switch traffic that is on any of the subfibers.

e. Re-run the manual connection validation test to clear the alarm and wait five minutes to ensure there are no new alarms. Go to step 23.

Procedure 4-101 (continued)
High Fiber Loss

Step	Action
19	Check the Excess Loss provisioning. If there are lossy elements (patch panels and pads are typical examples of lossy elements) between the two ports, the loss of the element itself should be provisioned in the Excess Loss field. Refer to the “Editing facility parameters” procedure in Part 1 of *Configuration - Provisioning and Operating*, 323-1851-311.
20	If the reported loss is less than the Major or Minor threshold, but not by 0.5 dB, the alarm is being held on due to a 0.5 dB hysteresis. The threshold is likely too low. Adjust the threshold.
21	If the reported loss is greater than 1.5 dB, this is likely a problem in the circuit packs or fibering that must be resolved. Contact your next level of support or your Ciena support group.
22	For losses less than 1.5 dB if all other steps have been taken, clear the alarm by adjusting the threshold.
23	If the alarm does not clear, contact your next level of support or your Ciena support group.

—end—

Procedure 4-102
High Optical Power

Alarm ID: 1800

Probable cause

This alarm is raised on the CCMD16x12, AMP4, or RLA modules.

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 safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - 6500-T Series Shelves*, 323-1851-201.6

Step	Action

ATTENTION
DO NOT disconnect fibers or remove dust caps until instructed to do so (safely), in the following steps.

DANGER
Risk of laser radiation exposure
Laser radiation is present on the optical fiber. Do not look into the optical fiber.

1 Replace the upstream amplifier connected to the RLA port that has raised the alarm. Follow the steps in the “Replacing an amplifier module” procedure in *Fault Management - Module Replacement for T-Series*, 323-1851-546.

2

If the original alarm has	**Then**
cleared	the procedure is complete
not cleared	go to step 3

3 Replace the RLA. Refer to “Replacing an RLA 20x1 C-Band w/Upgrade 1xSFP module” in *Fault Management - Module Replacement for T-Series*, 323-1851-546.

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

—end—

Procedure 4-103
High Temperature

Alarm ID: 378

Probable cause

This alarm is raised against a slot when the recorded temperature is too high.

The following conditions can cause this alarm:

- The operating environment exceeds the temperature and/or altitude limits specified for the shelf. Refer to the 6500 - T_Series Shelves- Guide*, 323-1851-103*.
- There are one or more empty slots in the shelf which must be equipped with modules, circuit packs, or filler cards. Any “Circuit Pack Missing” or “Slot Empty” alarms must be cleared first.
- The shelf cooling system is not functioning correctly. Any “Fan Failed” alarms must be cleared first.
- The shelf is operating without a cooling fan module equipped (for example, one or more fan modules are missing or not fully inserted).
- The air exhaust port or air inlet plenum is blocked.
- The air filter has a blockage.
- The shelf exhaust air is being trapped in an enclosed space or cabinet and is re-circulating into the air inlet plenum.
- Hot exhaust air from other equipment is mixing with the shelf's intake air.
- There is a problem with a circuit pack or module in the shelf.

Note: It may take some time for a shelf to cool off and the alarm to clear after the cause is corrected.

Impact

Critical, service-affecting (C, SA) alarm

Prerequisites

To perform this procedure, you must observe all safety requirements described in the “Observing product and personnel safety guidelines” chapter in *Installation - 6500-T Series Shelves,* 323-1851-201.6.

Procedure 4-103 (continued)
High Temperature

Step	Action

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

CAUTION
Risk of damage to circuit packs and modules
Do not attempt to cause this alarm to be raised by removing any cooling fan modules or filler cards or by blocking the shelf air inlet or exhaust ports as it will compromise shelf cooling. A shelf with a compromised cooling system may result in circuit pack or module failures prior to the assertion of a High Temperature Warning or High Temperature alarm.

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 Make sure that the shelf operating environment is within the specified temperature and altitude limits. Refer to the *6500 - T_Series Shelves- Guide,* 323-1851-103.

3

If the operating temperature for the altitude is	**Then**
within the specified limits	go to step 4
not within the specified limits	correct the office temperature and go to step 8

4 Perform visual checks to ensure that the shelf air intake is not obstructed and that air is exhausting from each fan module or from the shelf's exhaust port as applicable. Verify the following:

- Make sure that there is clearance between the back of the shelf and any other shelf, wall, or obstruction.
- Inspect the grill at the air exhaust of the cooling unit or the grill integrated into the shelf cover/door, the grill on the cooling fan module, and the grill on the air inlet plenum. If any have an accumulation of dust, vacuum the grill.

Procedure 4-103 (continued)
High Temperature

Step	Action
5	Visually inspect the shelf to confirm that all slots are filled (including all circuit pack subslots and common equipment slots). Refer to the "Displaying shelf inventory information" procedure in Part 1 of *Configuration - Provisioning and Operating,* 323-1851-311.
6	**If** the shelf has — **Then** go to all slots filled — step 8 empty slots — step 7
7	Re-insert any missing circuit packs or install filler cards into any empty slots. Refer to the equipment replacement procedures in *Fault Management - Module Replacement for T-Series*, 323-1851-546.
8	Remove and inspect the shelf air filter and replace it with a new one if there is a visible accumulation of dust. Refer to the "Replacing a shelf air filter or a SM air filter" procedure in *Fault Management - Module Replacement for T-Series*, 323-1851-546.
9	Monitor the temperatures on the circuit packs by retrieving the inventory and check whether the current temperature of all the supported circuit packs decreases. If the temperature did not decrease even after ten minutes or if the CTM is still reporting a current temperature of 50 °C or greater, continue to the step 10. ***Note:*** The "High Temperature" alarm automatically clears if the temperature drops to an appropriate level.
10	Replace the cooling fan module(s). Refer to the "Replacing a shelf fan module or a SM fan module" procedure in *Fault Management - Module Replacement_T-Series*, 323-1851-546.
11	Monitor the temperatures on the cards by retrieving the inventory and check whether the current temperature of all the supported circuit packs decreases. If the temperature did not decrease even after ten minutes or if the CTM is still reporting a current temperature of 50 °C or greater, go to step 12.
12	If the alarm does not clear, it could be due to a problem with a circuit pack. Contact your next level of support or your Ciena support group.

—end—

Procedure 4-104
High Temperature Warning

Alarm ID: 1143

Probable cause

This alarm is raised as a warning to the user when the module temperature is high for five or more minutes or when the shelf cooling system is not functioning correctly. The following conditions are applicable:

- The operating environment exceeds the temperature and/or altitude limits specified for the shelf. Refer to the *6500 - T_Series Shelves- Guide*, 323-1851-103.
- There are one or more empty slots in the shelf which must be equipped with modules, circuit packs, or filler cards. Any “Circuit Pack Missing” or “Slot Empty” alarms must be cleared first.
- The shelf cooling system is not functioning correctly. Any “Fan Failed” alarms must be cleared first.
- The shelf is operating without a cooling fan module equipped (one or more fan modules are missing or not fully inserted).
- The air exhaust port or air inlet plenum is blocked.
- The air filter has a blockage.
- The shelf exhaust air is being trapped in an enclosed space or cabinet and is re-circulating into the air inlet plenum.
- Hot exhaust air from other equipment is mixing with the shelf's intake air.
- There is a problem with a circuit pack or module in the shelf.

ATTENTION

If a high temperature warning condition prevails for a while, it could potentially lead to a “High Temperature” condition. Refer to “High Temperature” on page 4-208 for high temperature condition information.

The Raised temperature warning condition is cleared on a slot automatically if the temperature on these circuit packs decreases to an acceptable level.

Temperature can be monitored through inventory retrieval, which displays the current and average temperature on the supported circuit packs. Refer to the “Displaying shelf inventory information” procedure in Part 1 of *Configuration - Provisioning and Operating*, 323-1851-311.

Procedure 4-104 (continued)
High Temperature Warning

Impact

Major, 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 - 6500-T Series Shelves,* 323-1851-201.6.

Step	Action

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

CAUTION
Risk of damage to circuit packs and modules
Do not attempt to cause this alarm to be raised by removing any cooling fan modules or filler cards or by blocking the shelf air inlet or exhaust ports as it will compromise shelf cooling. A shelf with a compromised cooling system may result in circuit pack or module failures prior to the assertion of a High Temperature Warning or High Temperature alarm.

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 Make sure that the shelf operating environment is within the specified temperature and altitude limits. Refer to the *6500 - T_Series Shelves- Guide,* 323-1851-103.

3

If the operating temperature for the altitude is	**Then**
within the specified limits	go to step 4
not within the specified limits	correct the office temperature and go to step 4

Procedure 4-104 (continued)
High Temperature Warning

Step	Action
4	Perform visual checks to ensure that the shelf air intake is not obstructed and the air is exhausting from each fan module or from the shelf exhaust port as applicable. Verify the following: • Make sure that there is clearance between the back of the shelf and any other shelf, wall, or obstruction. • Inspect the grill at the air exhaust of the cooling unit or the grill integrated into the shelf cover/door, the grill on the cooling fan module, and the grill on the air inlet plenum. If any have an accumulation of dust, vacuum the grill.
5	Visually inspect the shelf to confirm that all slots are filled (including all circuit pack subslots and common equipment slots).
6	**If** the shelf has — **Then** go to all slots filled — step 8 empty slots — step 7
7	Re-insert any missing circuit packs or install filler cards into any empty slots. Refer to the equipment replacement procedures in *Fault Management - Module Replacement*, 323-1851-546.
8	Remove and inspect the shelf air filter and replace it with a new one if there is a visible accumulation of dust. Refer to the “Replacing a shelf air filter or a SM air filter” procedure in *Fault Management - Module Replacement for T-Series*, 323-1851-546.
9	Monitor the temperatures on the circuit packs by retrieving the inventory and check whether the current temperature of all the supported circuit packs decreases. If the temperature does not decrease after ten minutes, go to step 10. If the temperature falls to normal on all the supported circuit packs wait for 6 minutes for the alarm to clear.
10	**If** the original alarm has — **Then** cleared — the procedure is complete not cleared, even after all the circuit packs are at a normal temperature for more than six minutes — go to step 11
11	Replace the cooling fans module(s) “Replacing a shelf fan module or a SM fan module” procedures in *Fault Management - Replacement for T-Series*, 323-1851-546.
12	If the alarm does not clear, it could be due to a problem with a circuit pack. Contact your next level of support or your Ciena support group.

—end—

Procedure 4-105
Home Path Not defined

Alarm ID: 1772

Probable cause

This alarm is raised when an SNC with Reserved Home Path enabled does not have a Home Path. This can occur if the SNC Home Path is released without successfully setting up a new Home Path.

The alarm can also be raised when an SNC with Reserved Home Path is in the STARTING state. You need to ensure that the SNC can setup over dynamic routing or the DTLSET.

This alarm is raised when the Home Path OSRP line bandwidth is locked and the regroom operation of the Reserved Home Path enabled SNC (for example, make current path as home path) is failed.

The alarm will be cleared when the SNC Home Path is setup successfully or when Retain Home Path is disabled on the SNC.

Impact

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

Prerequisites

To perform this procedure, you must:

- ensure the Primary State of the SNC to be regroomed is in-service. Refer to the “Regrooming a sub-network connection” procedure in *Configuration - Control Plane*, 323-1851-330.
- use an account with at least a level 3 UPC

Step	Action
1	If the alarm is raised because the OSRP line bandwidth is locked out and the SNC with Reserved Home Path enabled regroom operation failed, disable the bandwidth lockout and regroom the SNC again. Refer to the “Regrooming a sub-network connection*” procedure in Configuration - Control Plane*, 323-1851-330.

Procedure 4-105 (continued)
Home Path Not defined

Step	Action
2	Otherwise, regroom the SNC for a new Home path or regroom the SNC to the current path by enabling the “Make current path as home path” check box. Refer to the “Regrooming a sub-network connection*” procedure in Configuration - Control Plane*, 323-1851-330.
3	Alternatively, disable (uncheck) the Retain Home Path checkbox when regrooming the SNC if you do not need Retain Home path functionality for this SNC. Refer to the “Regrooming a sub-network connection*” procedure in Configuration - Control Plane*, 323-1851-330.
4	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 for T-Series, Part 1 of 2

Release 12.0
Publication: 323-1851-544
Document status: Standard
Issue 1
Document release date: January 2017

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

ciena