# Cisco ONS 15454 DWDM Troubleshooting Guide

Product and Software Release 6.0
June 2012


**Corporate Headquarters**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100



Text Part Number: 78-17313-02

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

Modifying the equipment without Cisco's written authorization may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

• Turn the television or radio antenna until the interference stops.

• Move the equipment to one side or the other of the television or radio.

• Move the equipment farther away from the television or radio.

• Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

# CONTENTS

# FIGURES

# TABLES

# About this Guide

This section explains the objectives, intended audience, and organization of this publication and describes the conventions that convey instructions and other information.

The terms "Unidirectional Path Switched Ring" and "UPSR" may appear in Cisco literature. These terms do not refer to using Cisco ONS 15xxx products in a unidirectional path switched ring configuration. Rather, these terms, as well as "Path Protected Mesh Network" and "PPMN," refer generally to Cisco's path protection feature, which may be used in any topological network configuration. Cisco does not recommend using its path protection feature in any particular topological network configuration.

# Revision History

| Date | Notes |
|---|---|
| March 2007 | Revision History Table added for the first time |
| August 2007 | Updated About this Guide chapter. |
| September 2008 | Added WXC card information for OPWR-LFAIL and OPWR-HDEG alarms in Chapter 2, Alarm Troubleshooting. |
| June 2009 | Updated PWR-FAIL-A, PWR-FAIL-B, PWR-FAIL-RET-A, and PWR-FAIL-RET-B alarm details in Chapter 2, Alarm Troubleshooting. |
| August 2009 | Updated MEM-GONE alarm description in Chapter 2, Alarm Troubleshooting. |
| November 2009 | Update the section “Isolate the Cause of Power Supply Problems” in the chapter, “General Troubleshooting”. |
| February 2010 | Changed the BIEC parameter to BIT-EC in Chapter 5, “Performance Monitoring”. |
| June 2010 | Updated the description of the PWR-FAIL-A and PWR-FAIL-B alarms in the chapter, Alarm Troubleshooting. |
| February 2012 | Updated the section “IMPROPRMVL” in the chapter “Alarm Troubleshooting”. |
| May 2012 | Updated the section “Clear the UNC-WORD Condition” in the chapter “Alarm Troubleshooting”. |
| June 2012 | Document Part Number revisioned to 78-17313-02 and a full length book-PDF was generated. |

This section provides the following information:

- Document Objectives

- Audience
- Document Organization
- Related Documentation
- Document Conventions
- Obtaining Optical Networking Information

# Document Objectives

This guide gives troubleshooting information and troubleshooting-related parameters for the Cisco ONS 15454 (ANSI) and Cisco ONS 15454 SDH (ETSI) platforms, specifically the dense wavelength division multiplexing (DWDM) application that can operate on either platform. Use this guide in conjunction with the appropriate publications listed in the Related Documentation section.

# Audience

To use this publication, you should be familiar with Cisco or equivalent optical transmission hardware and cabling, telecommunications hardware and cabling, electronic circuitry and wiring practices, and preferably have experience as a telecomunications technician.

# Document Organization

The *Cisco ONS 15454 DWDM Troubleshooting Guide* is organized into the following chapters:

- Chapter 1, "General Troubleshooting," provides methods to discover hardware errors, such as failed ports, that adversely affect signal traffic; it also gives typical software problems that occur and their solutions.
- Chapter 2, "Alarm Troubleshooting," provides indexes, descriptions, and troubleshooting methods for all alarms and conditions generated by the ONS 15454.
- Chapter 3, "Transients Conditions," describes temporary (transient) conditions.
- Chapter 4, "Error Messages," provides a comprehensive list of all ONS 15454 error messages and their identification numbers.
- Chapter 5, "Performance Monitoring," defines performance monitoring parameters for all DWDM, transponder (TXP), and muxponder (MXP) cards.
- Chapter 6, "SNMP," describes simple network management protocol (SNMP) applications as they apply to the Cisco ONS 15454.

# Related Documentation

Use the *Cisco ONS 15454 DWDM Troubleshooting Guide* in conjunction with the following publications:

- *Cisco ONS 15454 DWDM Installation and Operations Guide, Release 6.0*
  Provides procedures to install, turn up, test, and maintain an ONS 15454 node and network. It also includes reference information.

- *Cisco ONS SONET TL1 Command Guide*
  Provides a full TL1 command and autonomous message set including parameters, AIDs, conditions and modifiers for the Cisco ONS 15454, ONS 15327, ONS 15600 and ONS 15310-CL systems.
- *Cisco ONS SONET TL1 Reference Guide*
  Provides general information, procedures, and errors for TL1 in the Cisco ONS 15454, ONS 15327, ONS 15600 and ONS 15310-CL systems.
- Cisco ONS 15454 SDH TL1 Command Guide
  Provides a full TL1 command and autonomous message set including parameters, AIDs, conditions and modifiers for the Cisco ONS 15454 SDH.
- *Cisco ONS 15454 SDH TL1 Reference Guide*
  Provides general information, procedures, and errors for TL1 in the Cisco ONS 15454 SDH.
- *Release Notes for the Cisco ONS 15454 Release 6.0*
  Provides caveats, closed issues, and new feature and functionality information.
- *Release Notes for the Cisco ONS 15454 SDH Release 6.0*
  Provides caveats, closed issues, and new feature and functionality information.

Refer to the following standards documentation referenced in this publication:

- Telcordia GR-253 CORE

# Document Conventions

This publication uses the following conventions:

| Convention | Application |
|---|---|
| **boldface** | Commands and keywords in body text. |
| *italic* | Command input that is supplied by the user. |
| [ ] | Keywords or arguments that appear within square brackets are optional. |
| { x \| x \| x } | A choice of keywords (represented by x) appears in braces separated by vertical bars. The user must select one. |
| Ctrl | The control key. For example, where Ctrl + D is written, hold down the Control key while pressing the D key. |
| `screen font` | Examples of information displayed on the screen. |
| **`boldface screen font`** | Examples of information that the user must enter. |
| < > | Command parameters that must be replaced by module-specific codes. |

**Note** Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the document.

**Caution** Means *reader be careful*. In this situation, the user might do something that could result in equipment damage or loss of data.

**Warning** **IMPORTANT SAFETY INSTRUCTIONS**

**This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.** Statement 1071

**SAVE THESE INSTRUCTIONS**

**Waarschuwing** **BELANGRIJKE VEILIGHEIDSINSTRUCTIES**

**Dit waarschuwingssymbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico's en dient u op de hoogte te zijn van de standaard praktijken om ongelukken te voorkomen. Gebruik het nummer van de verklaring onderaan de waarschuwing als u een vertaling van de waarschuwing die bij het apparaat wordt geleverd, wilt raadplegen.**

**BEWAAR DEZE INSTRUCTIES**

**Varoitus** **TÄRKEITÄ TURVALLISUUSOHJEITA**

**Tämä varoitusmerkki merkitsee vaaraa. Tilanne voi aiheuttaa ruumiillisia vammoja. Ennen kuin käsittelet laitteistoa, huomioi sähköpiirien käsittelemiseen liittyvät riskit ja tutustu onnettomuuksien yleisiin ehkäisytapoihin. Turvallisuusvaroitusten käännökset löytyvät laitteen mukana toimitettujen käännettyjen turvallisuusvaroitusten joukosta varoitusten lopussa näkyvien lausuntonumeroiden avulla.**

**SÄILYTÄ NÄMÄ OHJEET**

**Attention** **IMPORTANTES INFORMATIONS DE SÉCURITÉ**

**Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant entraîner des blessures ou des dommages corporels. Avant de travailler sur un équipement, soyez conscient des dangers liés aux circuits électriques et familiarisez-vous avec les procédures couramment utilisées pour éviter les accidents. Pour prendre connaissance des traductions des avertissements figurant dans les consignes de sécurité traduites qui accompagnent cet appareil, référez-vous au numéro de l'instruction situé à la fin de chaque avertissement.**

**CONSERVEZ CES INFORMATIONS**

**Warnung** **WICHTIGE SICHERHEITSHINWEISE**

**Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu Verletzungen führen kann. Machen Sie sich vor der Arbeit mit Geräten mit den Gefahren elektrischer Schaltungen und den üblichen Verfahren zur Vorbeugung vor Unfällen vertraut. Suchen Sie mit der am Ende jeder Warnung angegebenen Anweisungsnummer nach der jeweiligen Übersetzung in den übersetzten Sicherheitshinweisen, die zusammen mit diesem Gerät ausgeliefert wurden.**

**BEWAHREN SIE DIESE HINWEISE GUT AUF.**

**Avvertenza** **IMPORTANTI ISTRUZIONI SULLA SICUREZZA**

**Questo simbolo di avvertenza indica un pericolo. La situazione potrebbe causare infortuni alle persone. Prima di intervenire su qualsiasi apparecchiatura, occorre essere al corrente dei pericoli relativi ai circuiti elettrici e conoscere le procedure standard per la prevenzione di incidenti. Utilizzare il numero di istruzione presente alla fine di ciascuna avvertenza per individuare le traduzioni delle avvertenze riportate in questo documento.**

**CONSERVARE QUESTE ISTRUZIONI**

**Advarsel** **VIKTIGE SIKKERHETSINSTRUKSJONER**

**Dette advarselssymbolet betyr fare. Du er i en situasjon som kan føre til skade på person. Før du begynner å arbeide med noe av utstyret, må du være oppmerksom på farene forbundet med elektriske kretser, og kjenne til standardprosedyrer for å forhindre ulykker. Bruk nummeret i slutten av hver advarsel for å finne oversettelsen i de oversatte sikkerhetsadvarslene som fulgte med denne enheten.**

**TA VARE PÅ DISSE INSTRUKSJONENE**

**Aviso** **INSTRUÇÕES IMPORTANTES DE SEGURANÇA**

**Este símbolo de aviso significa perigo. Você está em uma situação que poderá ser causadora de lesões corporais. Antes de iniciar a utilização de qualquer equipamento, tenha conhecimento dos perigos envolvidos no manuseio de circuitos elétricos e familiarize-se com as práticas habituais de prevenção de acidentes. Utilize o número da instrução fornecido ao final de cada aviso para localizar sua tradução nos avisos de segurança traduzidos que acompanham este dispositivo.**

**GUARDE ESTAS INSTRUÇÕES**

**¡Advertencia!** **INSTRUCCIONES IMPORTANTES DE SEGURIDAD**

**Este símbolo de aviso indica peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considere los riesgos de la corriente eléctrica y familiarícese con los procedimientos estándar de prevención de accidentes. Al final de cada advertencia encontrará el número que le ayudará a encontrar el texto traducido en el apartado de traducciones que acompaña a este dispositivo.**

**GUARDE ESTAS INSTRUCCIONES**

**Varning!** **VIKTIGA SÄKERHETSANVISNINGAR**

**Denna varningssignal signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanliga förfaranden för att förebygga olyckor. Använd det nummer som finns i slutet av varje varning för att hitta dess översättning i de översatta säkerhetsvarningar som medföljer denna anordning.**

**SPARA DESSA ANVISNINGAR**

**FONTOS BIZTONSÁGI ELOÍRÁSOK**

**Ez a figyelmezeto jel veszélyre utal. Sérülésveszélyt rejto helyzetben van. Mielott bármely berendezésen munkát végezte, legyen figyelemmel az elektromos áramkörök okozta kockázatokra, és ismerkedjen meg a szokásos balesetvédelmi eljárásokkal. A kiadványban szereplo figyelmeztetések fordítása a készülékhez mellékelt biztonsági figyelmeztetések között található; a fordítás az egyes figyelmeztetések végén látható szám alapján keresheto meg.**

**ORIZZE MEG EZEKET AZ UTASÍTÁSOKAT!**

**Предупреждение** **ВАЖНЫЕ ИНСТРУКЦИИ ПО СОБЛЮДЕНИЮ ТЕХНИКИ БЕЗОПАСНОСТИ**

**Этот символ предупреждения обозначает опасность. То есть имеет место ситуация, в которой следует опасаться телесных повреждений. Перед эксплуатацией оборудования выясните, каким опасностям может подвергаться пользователь при использовании электрических цепей, и ознакомьтесь с правилами техники безопасности для предотвращения возможных несчастных случаев. Воспользуйтесь номером заявления, приведенным в конце каждого предупреждения, чтобы найти его переведенный вариант в переводе предупреждений по безопасности, прилагаемом к данному устройству.**

**СОХРАНИТЕ ЭТИ ИНСТРУКЦИИ**

警告 重要的安全性说明

此警告符号代表危险。您正处于可能受到严重伤害的工作环境中。在您使用设备开始工作之前，必须充分意识到触电的危险，并熟练掌握防止事故发生的标准工作程序。请根据每项警告结尾提供的声明号码来找到此设备的安全性警告说明的翻译文本。

请保存这些安全性说明

警告 安全上の重要な注意事項

「危険」の意味です。人身事故を予防するための注意事項が記述されています。装置の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止策に留意してください。警告の各国語版は、各注意事項の番号を基に、装置に付属の「Translated Safety Warnings」を参照してください。

これらの注意事項を保管しておいてください。

주의 **중요 안전 지침**

이 경고 기호는 위험을 나타냅니다. 작업자가 신체 부상을 일으킬 수 있는 위험한 환경에 있습니다. 장비에 작업을 수행하기 전에 전기 회로와 관련된 위험을 숙지하고 표준 작업 관례를 숙지하여 사고를 방지하십시오. 각 경고의 마지막 부분에 있는 경고문 번호를 참조하여 이 장치와 함께 제공되는 번역된 안전 경고문에서 해당 번역문을 찾으십시오.

이 지시 사항을 보관하십시오.

Aviso **INSTRUÇÕES IMPORTANTES DE SEGURANÇA**

**Este símbolo de aviso significa perigo. Você se encontra em uma situação em que há risco de lesões corporais. Antes de trabalhar com qualquer equipamento, esteja ciente dos riscos que envolvem os circuitos elétricos e familiarize-se com as práticas padrão de prevenção de acidentes. Use o número da declaração fornecido ao final de cada aviso para localizar sua tradução nos avisos de segurança traduzidos que acompanham o dispositivo.**

**GUARDE ESTAS INSTRUÇÕES**

Advarsel **VIGTIGE SIKKERHEDSANVISNINGER**

**Dette advarselssymbol betyder fare. Du befinder dig i en situation med risiko for legemesbeskadigelse. Før du begynder arbejde på udstyr, skal du være opmærksom på de involverede risici, der er ved elektriske kredsløb, og du skal sætte dig ind i standardprocedurer til undgåelse af ulykker. Brug erklæringsnummeret efter hver advarsel for at finde oversættelsen i de oversatte advarsler, der fulgte med denne enhed.**

**GEM DISSE ANVISNINGER**

تحذير **إرشادات الأمان الهامة**

**يوضح رمز التحذير هذا وجود خطر. وهذا يعني أنك متواجد في مكان قد ينتج عنه التعرض لإصابات. قبل بدء العمل، احذر مخاطر التعرض للصدمات الكهربائية وكن على علم بالإجراءات القياسية للحيلولة دون وقوع أي حوادث. استخدم رقم البيان الموجود في أخر كل تحذير لتحديد مكان ترجمته داخل تحذيرات الأمان المترجمة التي تأتي مع الجهاز.**

**قم بحفظ هذه الإرشادات**

Upozorenje **VAŽNE SIGURNOSNE NAPOMENE**

**Ovaj simbol upozorenja predstavlja opasnost. Nalazite se u situaciji koja može prouzročiti tjelesne ozljede. Prije rada s bilo kojim uređajem, morate razumjeti opasnosti vezane uz električne sklopove, te biti upoznati sa standardnim načinima izbjegavanja nesreća. U prevedenim sigurnosnim upozorenjima, priloženima uz uređaj, možete prema broju koji se nalazi uz pojedino upozorenje pronaći i njegov prijevod.**

**SAČUVAJTE OVE UPUTE**

Upozornění

**DŮLEŽITÉ BEZPEČNOSTNÍ POKYNY**

**Tento upozorňující symbol označuje nebezpečí. Jste v situaci, která by mohla způsobit nebezpečí úrazu. Před prací na jakémkoliv vybavení si uvědomte nebezpečí související s elektrickými obvody a seznamte se se standardními opatřeními pro předcházení úrazům. Podle čísla na konci každého upozornění vyhledejte jeho překlad v přeložených bezpečnostních upozorněních, která jsou přiložena k zařízení.**

**USCHOVEJTE TYTO POKYNY**

Προειδοποίηση

ΣΗΜΑΝΤΙΚΕΣ ΟΔΗΓΙΕΣ ΑΣΦΑΛΕΙΑΣ

Αυτό το προειδοποιητικό σύμβολο σημαίνει κίνδυνο. Βρίσκεστε σε κατάσταση που μπορεί να προκαλέσει τραυματισμό. Πριν εργαστείτε σε οποιοδήποτε εξοπλισμό, να έχετε υπόψη σας τους κινδύνους που σχετίζονται με τα ηλεκτρικά κυκλώματα και να έχετε εξοικειωθεί με τις συνήθεις πρακτικές για την αποφυγή ατυχημάτων. Χρησιμοποιήστε τον αριθμό δήλωσης που παρέχεται στο τέλος κάθε προειδοποίησης, για να εντοπίσετε τη μετάφρασή της στις μεταφρασμένες προειδοποιήσεις ασφαλείας που συνοδεύουν τη συσκευή.

ΦΥΛΑΞΤΕ ΑΥΤΕΣ ΤΙΣ ΟΔΗΓΙΕΣ

אזהרה

**הוראות בטיחות חשובות**

סימן אזהרה זה מסמל סכנה. אתה נמצא במצב העלול לגרום לפציעה. לפני שתעבוד עם ציוד כלשהו, עליך להיות מודע לסכנות הכרוכות במעגלים חשמליים ולהכיר את הנהלים המקובלים למניעת תאונות. השתמש במספר ההוראה המסופק בסופה של כל אזהרה כד לאתר את התרגום באזהרות הבטיחות המתורגמות שמצורפות להתקן.

**שמור הוראות אלה**

Opomena

ВАЖНИ БЕЗБЕДНОСНИ НАПАТСТВИЈА
Симболот за предупредување значи опасност. Се наоѓате во ситуација што може да предизвика телесни повреди. Пред да работите со опремата, бидете свесни за ризикот што постои кај електричните кола и треба да ги познавате стандардните постапки за спречување на несреќни случаи. Искористете го бројот на изјавата што се наоѓа на крајот на секое предупредување за да го најдете неговиот период во преведените безбедносни предупредувања што се испорачани со уредот.
ЧУВАЈТЕ ГИ ОВИЕ НАПАТСТВИЈА

**Ostrzeżenie** **WAŻNE INSTRUKCJE DOTYCZĄCE BEZPIECZEŃSTWA**

**Ten symbol ostrzeżenia oznacza niebezpieczeństwo. Zachodzi sytuacja, która może powodować obrażenia ciała. Przed przystąpieniem do prac przy urządzeniach należy zapoznać się z zagrożeniami związanymi z układami elektrycznymi oraz ze standardowymi środkami zapobiegania wypadkom. Na końcu każdego ostrzeżenia podano numer, na podstawie którego można odszukać tłumaczenie tego ostrzeżenia w dołączonym do urządzenia dokumencie z tłumaczeniami ostrzeżeń.**

**NINIEJSZE INSTRUKCJE NALEŻY ZACHOWAĆ**

**Upozornenie** **DÔLEŽITÉ BEZPEČNOSTNÉ POKYNY**

**Tento varovný symbol označuje nebezpečenstvo. Nachádzate sa v situácii s nebezpečenstvom úrazu. Pred prácou na akomkoľvek vybavení si uvedomte nebezpečenstvo súvisiace s elektrickými obvodmi a oboznámte sa so štandardnými opatreniami na predchádzanie úrazom. Podľa čísla na konci každého upozornenia vyhľadajte jeho preklad v preložených bezpečnostných upozorneniach, ktoré sú priložené k zariadeniu.**

**USCHOVAJTE SI TENTO NÁVOD**

# Obtaining Optical Networking Information

This section contains information that is specific to optical networking products. For information that pertains to all of Cisco, refer to the Obtaining Documentation and Submitting a Service Request section.

## Where to Find Safety and Warning Information

For safety and warning information, refer to the *Cisco Optical Transport Products Safety and Compliance Information* document that accompanied the product. This publication describes the international agency compliance and safety information for the Cisco ONS 15454 system. It also includes translations of the safety warnings that appear in the ONS 15454 system documentation.

## Cisco Optical Networking Product Documentation CD-ROM

Optical networking-related documentation, including Cisco ONS 15xxx product documentation, is available in a CD-ROM package that ships with your product. The Optical Networking Product Documentation CD-ROM is updated periodically and may be more current than printed documentation.

# Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

CHAPTER 1

# General Troubleshooting

This chapter provides procedures for troubleshooting the most common problems encountered when operating a Cisco ONS 15454 DWDM shelf in ANSI or ETSI platforms. To troubleshoot specific alarms, see Chapter 2, "Alarm Troubleshooting." If you cannot find what you are looking for, contact Cisco Technical Support (1 800 553-2447).

**Note** In this chapter, "ONS 15454" refers to both ANSI and ETSI versions of the platform unless otherwise noted.

This chapter includes the following sections on network problems:

**Note** For dense wavelength division multiplexing (DWDM) network acceptance tests, refer to NTP-G16 in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

- 1.1 Loopback Description, page 1-2—Explains in general terms the types of loopback tests (facility and terminal) that can be run along with general loopback behavior and card loopback behavior.
- 1.2 Troubleshooting MXP or TXP Circuit Paths With Loopbacks, page 1-6—Explains how to use loopbacks tests described in "1.1 Loopback Description" section on page 1-2 to isolate trouble on muxponder (MXP) and transponder (TXP) circuits.
- 1.3 Troubleshooting DWDM Circuit Paths With ITU-T G.709 Monitoring, page 1-22—Explains how to utilize performance monitoring (PM) and threshold crossing alerts (TCA) to locate signal degrades on DWDM circuit paths.

The remaining sections describe symptoms, problems, and solutions that are categorized according to the following topics:

- 1.4 Using CTC Diagnostics, page 1-30—Explains how to perform card LED tests and download a diagnostic file for Cisco Technical Support.
- 1.5 Restoring the Database and Default Settings, page 1-32—Provides procedures for restoring software data and restoring the node to the default setup.
- 1.6 PC Connectivity Troubleshooting, page 1-32—Provides troubleshooting procedures for PC and network connectivity to the ONS 15454.
- 1.7 CTC Operation Troubleshooting, page 1-38—Provides troubleshooting procedures for Cisco Transport Controller (CTC) login or operation problems.
- 1.8 Timing, page 1-48—Provides troubleshooting procedures for circuit creation and error reporting as well as timing reference errors and alarms.

- 1.9 Fiber and Cabling, page 1-51—Provides troubleshooting procedures for fiber and cabling connectivity errors.
- 1.10 Power Supply Problems, page 1-55—Provides troubleshooting procedures for power supply problems.
- 1.11 Power Up Problems for Node and Cards, page 1-57— Explains power up problems in a node or cards typically caused an improper power supply.
- 1.12 Network Level (Internode) Problems, page 1-57—Provides troubleshooting procedures for problems between nodes, such as fiber cuts and optical channel network connection (OCHNC) circuit creation failure.
- 1.13 Node Level (Intranode) Problems, page 1-79—Provides troubleshooting procedures for variable optical attenuator (VOA) startup problems.

# 1.1 Loopback Description

Use loopbacks and hairpin circuits to test newly created circuits before running live traffic or to logically locate the source of a network failure. All ONS 15454 and ONS 15454 SDH TXP and MXP cards allow loopbacks and hairpin test circuits. Other cards do not allow loopbacks, including OPT-BST, OPT-PRE, OSC-CSM, AD-xB-xx.x, and AD-xC-xx.x cards.

To create a loopback on an ANSI or SONET port, the port must be in the Out-of-Service and Management, Maintenance (OOS-MA,MT) service state. After you create the loopback, the service state becomes Out-of-Service and Management, Loopback and Maintenance (OOS-MA,LPBK & MT).

To create a loopback on an SDH or ETSI port, the port must be in the Locked, maintenance administrative state and the Locked-Enabled, loopback & maintenance administrative state.

**Caution** Facility or terminal loopbacks can be service-affecting. To protect traffic, apply a lockout or Force switch to the target loopback port. Basic directions for these procedures exist in Chapter 2, "Alarm Troubleshooting." For more information about these operations, refer to the "Maintain the Node" chapter in the *Cisco ONS 15454 DWDM Procedure Guide*.

**Note** In CTC, a facility loopback is sometimes called "facility (line)" loopback, and a terminal loopback is sometimes called a "terminal (inward)" loopback. This is done to indicate the terminating direction of the signal: a facility loopback is sent outward toward the span, whereas a terminal loopback is redirected inward toward its originating port.

## 1.1.1 Facility Loopbacks

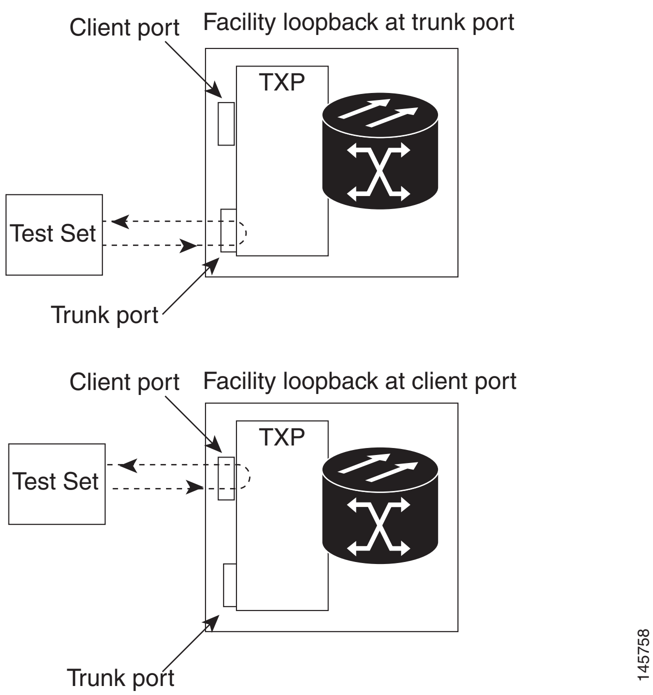
The following sections give general information about facility loopback operations and specific information about ONS 15454 or ONS 15454 SDH card loopback activity.

### 1.1.1.1 General Behavior

A facility loopback tests the line interface unit (LIU) of a card, the electrical interface assembly (EIA), and related cabling. After applying a facility loopback on a port, use a test set to run traffic over the loopback. A successful facility loopback isolates the LIU, the EIA, or the cabling plant as the potential cause of a network problem.

To test a card LIU, connect an optical test set to a trunk or client port and perform a facility loopback. Alternately, use a loopback or hairpin circuit on a card that is farther along the circuit path. For example, Figure 1-1 shows a facility loopback at a trunk port and at a client port on a TXP card.

***Figure 1-1 Facility Loopback Path on a Near-End Transponder Card***




**Caution** Before performing a facility loopback on a TXP card, be sure that the card contains at least two data communications channel (DCC) paths to the node where the card is installed. A second DCC provides a nonlooped path to log into the node after the loopback is applied, enabling you to remove the facility loopback. Ensuring a second DCC is not necessary if you are directly connected to the node containing the loopback card.

**Caution** Ensure that the facility being loopbacked is not being used by the node for line timing. If it is, a timing loop will be created.

### 1.1.1.2 Card Behavior

Port loopbacks either terminate or bridge the loopback signal. All MXP and TXP facility loopbacks are terminated as shown in Table 1-1.

When a port terminates a facility loopback signal, the signal only loops back to the originating port and is not transmitted downstream. When a port bridges a loopback signal, the signal loops back to the originating port and is also transmitted downstream.

**Note** In Table 1-1, no alarm indication signal (AIS) is injected if the signal is bridged. If the signal is terminated, an applicable AIS is injected downstream.

*Table 1-1 DWDM Client Card Facility Loopback Behavior*

| Card/Port | Facility Loopback Signal |
|---|---|
| MXP, MXPP trunk ports | Bridged |
| MXP, MXPP client ports | Terminated |
| TXP, TXPP trunk ports | Bridged |
| TXP, TXPP client ports | Terminated |

The loopback itself is listed in the Conditions window. For example, the window would list the LPBKFACILITY condition for a tested port. (The Alarms window would show the AS-MT condition, which means that alarms are suppressed on the facility during loopback.)

With a client-side SONET or ANSI facility loopback, the client port service state is OOS-MA,LPBK & MT. However any remaining client and trunk ports can be in any other service state. For SONET or ANSI cards in a trunk-side facility loopback, the trunk port service state is OOS-MA,LPBK & MT service state and the remaining client and trunk ports can be in any other service state.

With a client-side SDH or ESTI facility loopback, the client port is in the Locked-enabled,maintenance & loopback service state, however the remaining client and trunk ports can be in any other service state. For MXP and TXP cards in a SDH or ETSI trunk-side facility loopback, the trunk port is in the Locked-enabled,maintenance & loopback service state and the remaining client and trunk ports can be in any other service state.

## 1.1.2 Terminal Loopbacks

The following sections give general information about terminal loopback operations and specific information about ONS 15454 card loopback activity.

### 1.1.2.1 General Behavior

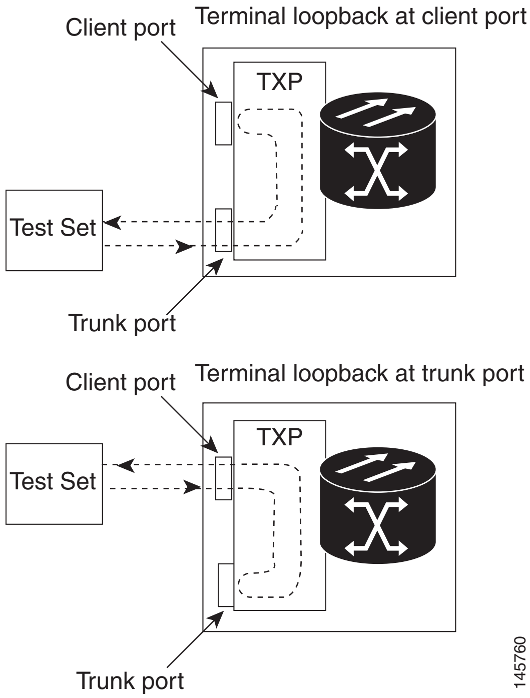
A terminal loopback tests a circuit path as it passes through a TXP or MXP card and loops back. For example, as shown in Figure 1-2, there are two types of terminal loopbacks shown for a TXP card.

The first is a terminal loopback at the client port. In this situation, the test set traffic comes in through the TXP trunk port, travels through the card, and turns around because of the terminal loopback in effect on the card just before it reaches the LIU of the client port. The signal is then sent back through the card to the trunk port and back to the test set.

The second is a terminal loopback at the trunk port. In this situation, the test set traffic comes in through the TXP client port, travels through the card, and turns around because of the terminal loopback in effect on the card just before it reaches the LIU of the trunk port. The signal is then sent back through the card to the client port and back to the test set.

This test verifies that the terminal circuit paths are valid, but does not test the LIU on the TXP card.

***Figure 1-2 Terminal Loopback on a TXP Card***




### 1.1.2.2 Card Behavior

ONS 15454 and ONS 15454 SDH terminal port loopbacks can either terminate or bridge the signal. TXP terminal loopbacks are terminated as shown in Table 1-2. During terminal loopbacks, if a port terminates a terminal loopback signal, the signal only loops back to the originating port and is not transmitted downstream. If the port bridges a loopback signal, the signal loops back to the originating port and is also transmitted downstream. Client card terminal loopback bridging and terminating behaviors are listed in Table 1-2.

**Note** In Table 1-2, no AIS signal is injected if the signal is bridged. If the signal is terminated, an applicable AIS is injected downstream.

***Table 1-2 Client Card Terminal Loopback Behavior***

| Card/Port | Terminal Loopback Signal |
|---|---|
| MXP, MXPP trunk ports | Bridged |
| MXP, MXPP client ports | Terminated |
| TXP, MXPP trunk ports | Bridged |
| TXP, MXPP client ports | Terminated |

The MXP and TXP trunk and client ports can simultaneously maintain different service states.

- For SONET or ANSI TXP and TXPP cards with a client-side terminal loopback, the client port is in the OOS-MA,LPBK & MT service state and trunk port must be in IS-NR service state.
- For SONET or ANSI MXP and MXPP cards with a client-side terminal loopback, the client port is in the OOS-MA,LPBK & MT service state and the remaining client and trunk ports can be in any service state.
- In SONET or ANSI MXP or TXP trunk-side terminal loopbacks, the trunk port is in the OOS-MA,LPBK & MT service state and the client ports must be in IS-NR service state for complete loopback functionality. A terminal loopback affects all client ports because it is performed on the aggregate signal.
- For SDH or ETSI TXP and TXPP client-side facility loopbacks, the client port is in the Locked-enabled,maintenance & loopback service state and the trunk port must be in Unlocked-enabled service state.
- For SDH or ETSI MXP and MXPP cards with a client-side terminal loopback the client port is in the Locked-enabled,maintenance & loopback service state and remaining client and trunk ports can be in any service state.
- In SDH and ETSI MXP or TXP trunk-side terminal loopbacks, the trunk port is in the Locked-enabled,maintenance & loopback service state and the client ports must be in Unlocked-enabled service state for complete loopback functionality. A facility loopback affects all client ports because it is performed on the aggregate signal.

The loopback itself is listed in the Conditions window. For example, the window would list the LPBKTERMINAL condition or LPBKFACILITY condition for a tested port. (The Alarms window would show the AS-MT condition, which indicates that all alarms are suppressed on the port during loopback testing.)

# 1.2 Troubleshooting MXP or TXP Circuit Paths With Loopbacks

Facility loopbacks and terminal loopbacks are often used together to test the circuit path through the network or to logically isolate a fault. Performing a loopback test at each point along the circuit path systematically isolates possible points of failure. MXP or TXP loopback tests differ from other testing in that loopback testing does not require circuit creation. MXP or TXP client ports are statically mapped to the trunk ports so no signal needs to traverse the cross-connect card (in a circuit) to test the loopback.

You can use these procedures on transponder cards (TXP, TXPP) or muxponder cards (MXP, MXPP) cards. The example in this section tests an MXP or TXP circuit on a three-node bidirectional line switched ring (BLSR) or multiswitched path ring (MS-SPRing). Using a series of facility loopbacks and terminal loopbacks, the example scenario traces the circuit path, tests the possible failure points, and eliminates them. The logical progression contains six network test procedures:

**Note** MXP and TXP card client ports do not appear when you click the **Maintenance > Loopback** tab unless they have been provisioned. Do this in the card view by clicking the **Provisioning > Pluggable Port Modules** tab. For information about provisioning client ports, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Note** The test sequence for your circuits will differ according to the type of circuit and network topology.

1. A facility loopback on the source-node MXP or TXP port

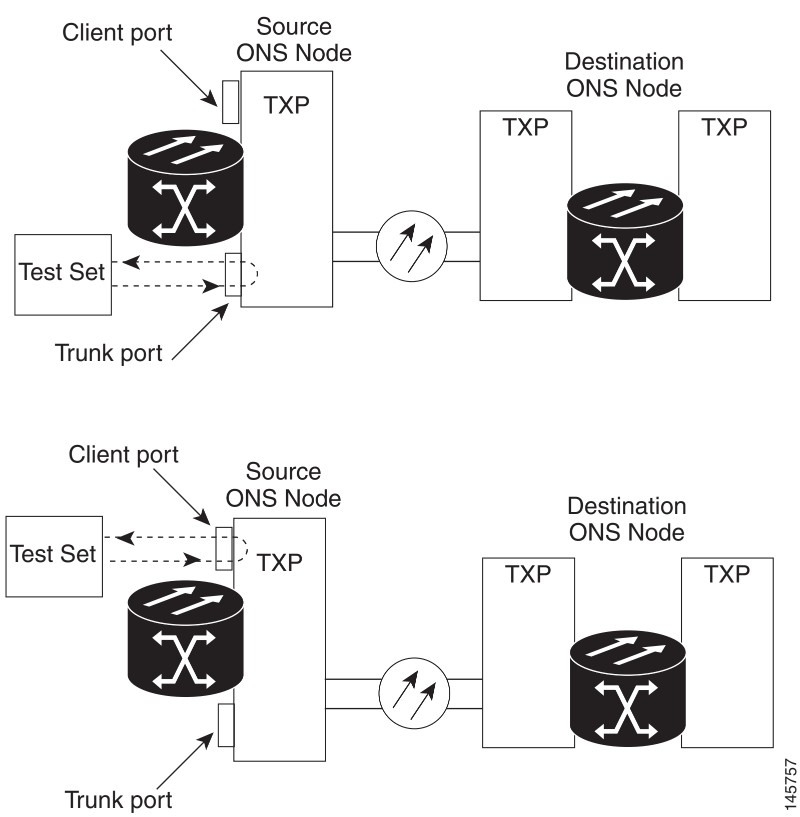
2. A terminal loopback on the source-node MXP or TXP port
3. A facility loopback on the intermediate-node MXP or TXP port
4. A terminal loopback on the intermediate-node MXP or TXP port
5. A facility loopback on the destination-node MXP or TXP port
6. A terminal loopback on the destination-node MXP or TXP port

**Note** Facility and terminal loopback tests require on-site personnel.

## 1.2.1 Perform a Facility Loopback on a Source-Node MXP or TXP Port

This facility loopback test is performed on the node source port in the network circuit. In the testing situation used in this example, the source muxponder or transponder port under test is located in the source node. Facility loopback can be performed at the trunk port or at a client port. Completing a successful facility loopback on this port isolates the source MXP or TXP port as a possible failure point. Figure 1-3 shows the facility loopback examples on source ONS node TXP ports (client and trunk).

*Figure 1-3 Facility Loopback on a Circuit Source MXP or TXP Port*




**Caution** Performing a loopback on an in-service circuit is service-affecting.

**Note** Facility loopbacks require on-site personnel.

Complete the "Create the Facility Loopback on the Source-Node MXP or TXP Port" procedure on page 1-8.

## Create the Facility Loopback on the Source-Node MXP or TXP Port

**Step 1** Connect an optical test set to the port you are testing.

**Note** For specific procedures to connect, set up, and use the test set equipment, consult the manufacturer.

Use appropriate cabling to attach the transmit (Tx) and receive (Rx) terminals of the optical test set to the port you are testing. The Tx and Rx terminals connect to the same port.

**Step 2** Adjust the test set accordingly. (Refer to manufacturer instructions for test set use.)

**Step 3** In CTC node view, double-click the card to display the card view.

**Step 4** Click the **Maintenance > Loopback** tabs.

**Step 5** Choose **OOS,MT** (or **locked,maintenance**) from the Admin State column for the port being tested. If this is a multiport card, select the appropriate row for the desired port.

**Step 6** Choose **Facility (Line)** from the Loopback Type column for the port being tested. If this is a multiport card, select the appropriate row for the desired port.

**Step 7** Click **Apply**.

**Step 8** Click **Yes** in the confirmation dialog box.

**Note** It is normal for the "LPBKFACILITY (ESCON)" condition on page 2-83, "LPBKFACILITY (FC)" condition on page 2-83, "LPBKFACILITY (GE)" condition on page 2-84, "LPBKFACILITY (ISC)" condition on page 2-84or the "LPBKFACILITY (TRUNK)" condition on page 2-85 to appear during loopback setup. The condition clears when you remove the loopback.

**Step 9** Complete the "Test and Clear the MXP or TXP Facility Loopback Circuit" procedure on page 1-8.

## Test and Clear the MXP or TXP Facility Loopback Circuit

**Step 1** If the test set is not already sending traffic, send test traffic on the loopback circuit.

**Step 2** Examine the traffic received by the test set. Look for errors or any other signal information that the test set is capable of indicating.

**Step 3** If the test set indicates no errors, no further testing is necessary with the facility loopback. Clear the facility loopback:

a. Click the **Maintenance > Loopback** tabs.

b. Choose **None** from the Loopback Type column for the port being tested.

c. Choose the appropriate state to place the port in service, out of service and disabled, out of service for maintenance, or automatically in service from the Admin State column for the port being tested.

d. Click **Apply**.

e. Click **Yes** in the confirmation dialog box.

**Step 4** Complete the "Test the MXP or TXP Card" procedure on page 1-9.

## Test the MXP or TXP Card

**Step 1** Complete the "Physically Replace a Card" procedure on page 2-154 for the suspected bad card and replace it with a known-good one.

**Caution** Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Refer to the procedures in the "2.9.1 Protection Switching, Lock Initiation, and Clearing" section on page 2-149. For more information, refer to the "Maintain the Node" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Step 2** Resend test traffic on the loopback circuit with a known-good card installed.

**Step 3** If the test set indicates no errors, the problem was probably the defective card. Return the defective card to Cisco through the Return Materials Authorization (RMA) process. Contact Cisco Technical Support (1 800 553-2447).

**Step 4** Complete the "Physically Replace a Card" procedure on page 2-154 for the faulty card.

**Step 5** Clear the facility loopback:

a. Click the **Maintenance > Loopback** tabs.

b. Choose **None** from the Loopback Type column for the port being tested.

c. Choose the appropriate state to place the port in service, out of service and disabled, out of service for maintenance, or automatically in service from the Admin State column for the port being tested.

d. Click **Apply**.

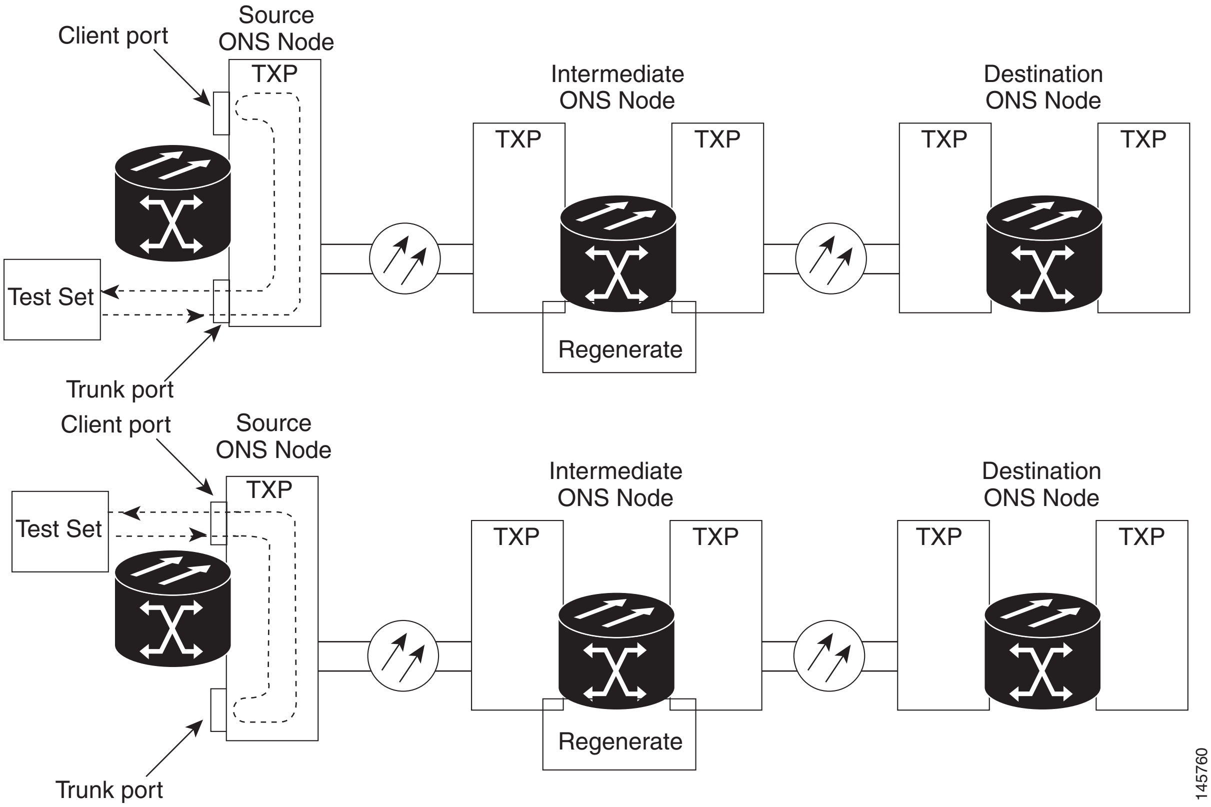
e. Click **Yes** in the confirmation dialog box.

**Step 6** Complete the "1.2.2 Perform a Terminal Loopback on a Source-Node MXP or TXP Port" procedure on page 1-9.

# 1.2.2 Perform a Terminal Loopback on a Source-Node MXP or TXP Port

The terminal loopback test is performed on the node source MXP or TXP muxponder or transponder port. For the circuit in this example, it is the source TXP trunk port or a client port in the source node. Completing a successful terminal loopback to a node source port verifies that the circuit is through the source port. Figure 1-4 shows an example of a terminal loopback on a source TXP port and a client TXP port.

*Figure 1-4 Terminal Loopback on a Source-Node MXP or TXP Port*




**Caution** Performing a loopback on an in-service circuit is service-affecting.

**Note** Terminal loopbacks require on-site personnel.

Complete the "Create the Terminal Loopback on a Source-Node MXP or TXP Port" procedure on page 1-10.

## Create the Terminal Loopback on a Source-Node MXP or TXP Port

**Step 1** Connect an optical test set to the port you are testing:

**Note** For specific procedures to connect, set up, and use the test set equipment, consult the manufacturer.

**a.** If you just completed the "1.2.1 Perform a Facility Loopback on a Source-Node MXP or TXP Port" procedure on page 1-7, leave the optical test set hooked up to the MXP or TXP port in the source node.

b. If you are starting the current procedure without the optical test set hooked up to the source port, use appropriate cabling to attach the Tx and Rx terminals of the optical test set to the port you are testing. Both Tx and Rx connect to the same port.

**Step 2** Adjust the test set accordingly. (Refer to manufacturer instructions for test set use.)

**Step 3** In node view, double-click the card that requires the loopback.

**Step 4** Click the **Maintenance > Loopback** tabs.

**Step 5** Select **OOS,MT** (or **locked,maintenance**) from the Admin State column. If this is a multiport card, select the row appropriate for the desired port.

**Step 6** Select **Terminal (Inward)** from the Loopback Type column. If this is a multiport card, select the row appropriate for the desired port.

**Step 7** Click **Apply**.

**Step 8** Click **Yes** in the confirmation dialog box.

**Step 9** Complete the "Test and Clear the MXP or TXP Port Terminal Loopback Circuit" procedure on page 1-11.

## Test and Clear the MXP or TXP Port Terminal Loopback Circuit

**Step 1** If the test set is not already sending traffic, send test traffic on the loopback circuit.

**Step 2** Examine the test traffic being received by the test set. Look for errors or any other signal information that the test set is capable of indicating.

**Step 3** If the test set indicates no errors, no further testing is necessary on the loopback circuit. Clear the terminal loopback state on the port:

a. Double-click the card in the source node with the terminal loopback.

b. Click the **Maintenance > Loopback** tabs.

c. Select **None** from the Loopback Type column for the port being tested.

d. Choose the appropriate state to place the port in service, out of service and disabled, out of service for maintenance, or automatically in service from the Admin State column for the port being tested.

e. Click **Apply**.

f. Click **Yes** in the confirmation dialog box.

**Step 4** Complete the "Test the MXP or TXP Card" procedure on page 1-11.

## Test the MXP or TXP Card

**Step 1** Complete the "Physically Replace a Card" procedure on page 2-154 for the suspected bad card and replace it with a known-good one.

**Caution** Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Refer to the procedures in the "2.9.1 Protection Switching, Lock Initiation, and Clearing" section on page 2-149. For more information, refer to the "Maintain the Node" chapter in the *Cisco ONS 15454 DWDM Procedure Guide*.

**Step 2** Resend test traffic on the loopback circuit with a known-good card.

**Step 3** If the test set indicates no errors, the problem was probably the defective card. Return the defective card to Cisco through the RMA process. Contact Cisco Technical Support (1 800 553-2447).

**Step 4** Complete the "Physically Replace a Card" procedure on page 2-154 for the defective card.

**Step 5** Clear the terminal loopback on the port before testing the next segment of the network circuit path:

a. Double-click the card in the source node with the terminal loopback.

b. Click the **Maintenance > Loopback** tabs.

c. Select **None** from the Loopback Type column for the port being tested.

d. Choose the appropriate state to place the port in service, out of service and disabled, out of service for maintenance, or automatically in service from the Admin State column for the port being tested.

e. Click **Apply**.

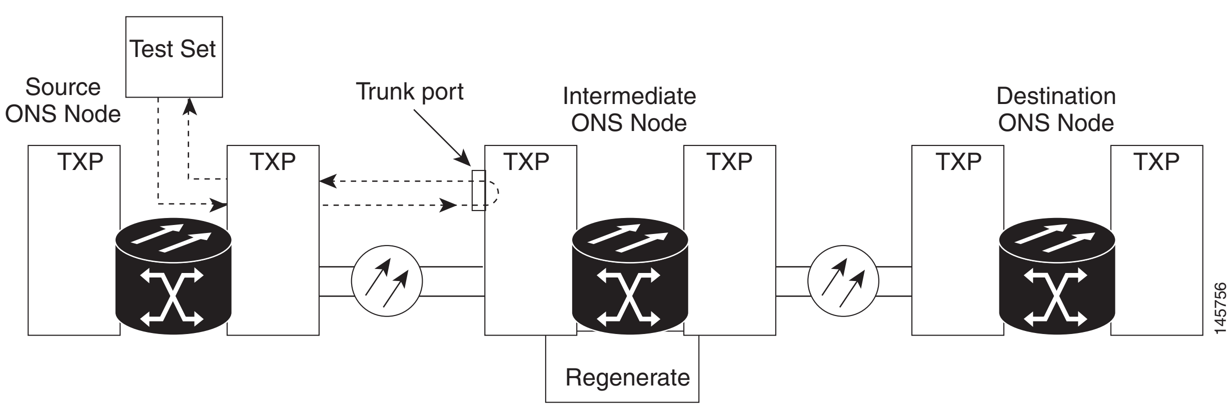
f. Click **Yes** in the confirmation dialog box.

**Step 6** Complete the "1.2.3 Create a Facility Loopback on an Intermediate-Node MXP or TXP Port" procedure on page 1-12.

## 1.2.3 Create a Facility Loopback on an Intermediate-Node MXP or TXP Port

Performing the facility loopback test on an intermediate port isolates whether this node is causing circuit failure. In the situation shown in Figure 1-5, the test is being performed on an intermediate MXP or TXP port.

***Figure 1-5 Facility Loopback on an Intermediate-Node MXP or TXP Port***



**Caution** Performing a loopback on an in-service circuit is service-affecting.

**Note** Facility loopbacks require on-site personnel.

Complete the "Create a Facility Loopback on an Intermediate-Node MXP or TXP Port" procedure on page 1-13.

## Create a Facility Loopback on an Intermediate-Node MXP or TXP Port

**Step 1** Connect an optical test set to the port you are testing:

**Note** For specific procedures to connect, set up, and use the test set equipment, consult the manufacturer.

a. If you just completed the "1.2.2 Perform a Terminal Loopback on a Source-Node MXP or TXP Port" procedure on page 1-9, leave the optical test set hooked up to the source-node port.

b. If you are starting the current procedure without the optical test set hooked up to the source port port, use appropriate cabling to attach the Tx and Rx terminals of the optical test set to the port you are testing. Both Tx and Rx connect to the same port.

**Step 2** Adjust the test set accordingly. (Refer to manufacturer instructions for test set use.)

**Step 3** In node view, double-click the intermediate-node card that requires the loopback.

**Step 4** Click the **Maintenance > Loopback** tabs.

**Step 5** Select **OOS,MT** (or **locked,maintenance**) from the Admin State column. If this is a multiport card, select the row appropriate for the desired port.

**Step 6** Select **Facility (Line)** from the Loopback Type column. If this is a multiport card, select the row appropriate for the desired port.

**Step 7** Click **Apply**.

**Step 8** Click **Yes** in the confirmation dialog box.

**Step 9** Complete the "Test and Clear the MXP or TXP Port Facility Loopback Circuit" procedure on page 1-13.

## Test and Clear the MXP or TXP Port Facility Loopback Circuit

**Step 1** If the test set is not already sending traffic, send test traffic on the loopback circuit.

**Step 2** Examine the traffic received by the test set. Look for errors or any other signal information that the test set is capable of indicating.

**Step 3** If the test set indicates no errors, no further testing is necessary with the facility loopback. Clear the facility loopback from the port:

a. Click the **Maintenance > Loopback** tabs.

b. Choose **None** from the Loopback Type column for the port being tested.

c. Choose the appropriate state to place the port in service, out of service and disabled, out of service for maintenance, or automatically in service from the Admin State column for the port being tested.

d. Click **Apply**.

e. Click **Yes** in the confirmation dialog box.

**Step 4** Complete the "Test the MXP or TXP Card" procedure on page 1-14.

## Test the MXP or TXP Card

**Step 1** Complete the "Physically Replace a Card" procedure on page 2-154 for the suspected bad card and replace it with a known-good one.

**Caution** Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Refer to the procedures in the "2.9.1 Protection Switching, Lock Initiation, and Clearing" section on page 2-149. For more information, refer to the "Maintain the Node" chapter in the *Cisco ONS 15454 DWDM Procedure Guide*.

**Step 2** Resend test traffic on the loopback circuit with a known-good card installed.

**Step 3** If the test set indicates no errors, the problem was probably the defective card. Return the defective card to Cisco through the RMA process. Contact Cisco Technical Support (1 800 553-2447).

**Step 4** Complete the "Physically Replace a Card" procedure on page 2-154 for the faulty card.

**Step 5** Clear the facility loopback from the port:

a. Click the **Maintenance > Loopback** tabs.

b. Choose **None** from the Loopback Type column for the port being tested.

c. Choose the appropriate state to place the port in service, out of service and disabled, out of service for maintenance, or automatically in service from the Admin State column for the port being tested.

d. Click **Apply**.

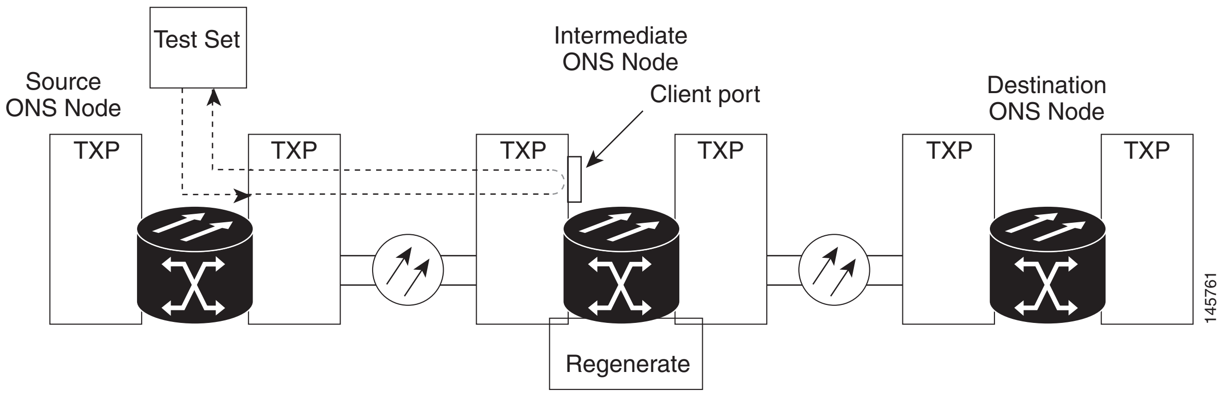
e. Click **Yes** in the confirmation dialog box.

**Step 6** Complete the "1.2.4 Create a Terminal Loopback on Intermediate-Node MXP or TXP Ports" procedure on page 1-14.

## 1.2.4 Create a Terminal Loopback on Intermediate-Node MXP or TXP Ports

In the next troubleshooting test, you perform a terminal loopback on the intermediate-node port to isolate whether the intermediate client or trunk port is causing circuit trouble. In the example situation in Figure 1-6, the terminal loopback is performed on an intermediate MXP or TXP port in the circuit. If you successfully complete a terminal loopback on the node, this node is excluded from possible sources of circuit trouble.

*Figure 1-6 Terminal Loopback on an Intermediate-Node MXP or TXP Port*




**Caution** Performing a loopback on an in-service circuit is service-affecting.

**Note** Terminal loopbacks require on-site personnel.

Complete the "Create a Terminal Loopback on Intermediate-Node MXP or TXP Ports" procedure on page 1-15.

## Create a Terminal Loopback on Intermediate-Node MXP or TXP Ports

**Step 1** Connect an optical test set to the port you are testing:

**Note** For specific procedures to connect, set up, and use the test set equipment, consult the manufacturer.

- **a.** If you just completed the "1.2.3 Create a Facility Loopback on an Intermediate-Node MXP or TXP Port" section on page 1-12, leave the optical test set hooked up to the source-node port.
- **b.** If you are starting the current procedure without the optical test set hooked up to the source port, use appropriate cabling to attach the Tx and Rx terminals of the optical test set to the port you are testing. Both Tx and Rx connect to the same port.

**Step 2** Adjust the test set accordingly. (Refer to manufacturer instructions for test set use.)

**Step 3** Create the terminal loopback on the destination port being tested:

- **a.** Go to the node view of the intermediate node:
  - Choose **View > Go To Other Node** from the menu bar.
  - Choose the node from the drop-down list in the Select Node dialog box and click **OK**.
- **b.** In node view, double-click the card that requires the loopback.
- **c.** Click the **Maintenance > Loopback** tabs.
- **d.** Select **OOS,MT** (or **locked,maintenance**) from the Admin State column. If this is a multiport card, select the row appropriate for the desired port.

e. Select **Terminal (Inward)** from the Loopback Type column. If this is a multiport card, select the row appropriate for the desired port.

f. Click **Apply**.

g. Click **Yes** in the confirmation dialog box.

**Step 4** Complete the "Test and Clear the MXP or TXP Terminal Loopback Circuit" procedure on page 1-16.

## Test and Clear the MXP or TXP Terminal Loopback Circuit

**Step 1** If the test set is not already sending traffic, send test traffic on the loopback circuit.

**Step 2** Examine the test traffic being received by the test set. Look for errors or any other signal information that the test set is capable of indicating.

**Step 3** If the test set indicates no errors, no further testing is necessary on the loopback circuit. Clear the terminal loopback from the port:

a. Double-click the intermediate-node card with the terminal loopback to display the card view.

b. Click the **Maintenance > Loopback** tabs.

c. Select **None** from the Loopback Type column for the port being tested.

d. Choose the appropriate state to place the port in service, out of service and disabled, out of service for maintenance, or automatically in service from the Admin State column for the port being tested.

e. Click **Apply**.

f. Click **Yes** in the confirmation dialog box.

**Step 4** Complete the "Test the MXP or TXP Card" procedure on page 1-16.

## Test the MXP or TXP Card

**Step 1** Complete the "Physically Replace a Card" procedure on page 2-154 for the suspected bad card and replace it with a known-good one.

**Caution** Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Refer to the procedures in the "2.9.1 Protection Switching, Lock Initiation, and Clearing" section on page 2-149. For more information, refer to the "Maintain the Node" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Step 2** Resend test traffic on the loopback circuit with a known-good card.

**Step 3** If the test set indicates no errors, the problem was probably the defective card. Return the defective card to Cisco through the RMA process. Contact Cisco Technical Support (1 800 553-2447).

**Step 4** Complete the "Physically Replace a Card" procedure on page 2-154 for the defective card.

**Step 5** Clear the terminal loopback on the port:

a. Double-click the source-node card with the terminal loopback.

b. Click the **Maintenance > Loopback** tabs.

c. Select **None** from the Loopback Type column for the port being tested.

d. Choose the appropriate state to place the port in service, out of service and disabled, out of service for maintenance, or automatically in service from the Admin State column for the port being tested.

e. Click **Apply**.

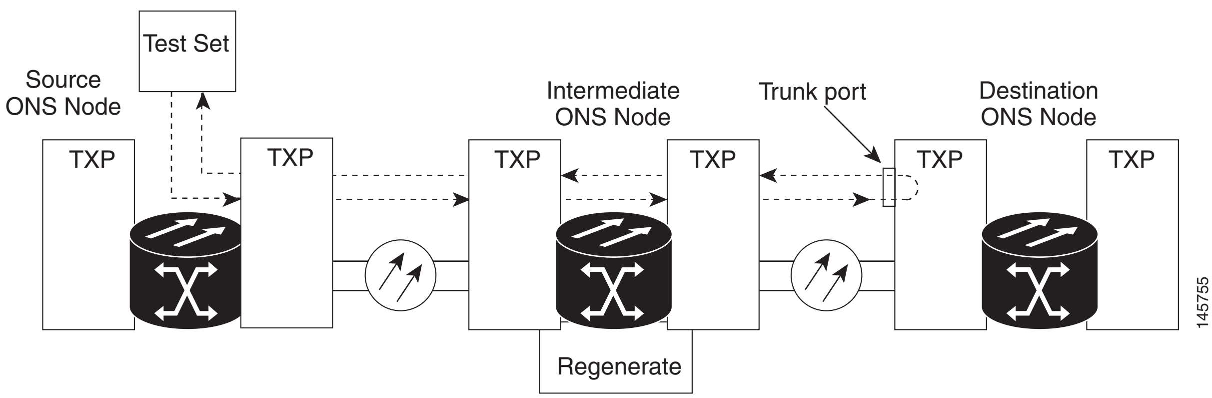
f. Click **Yes** in the confirmation dialog box.

**Step 6** Complete the "1.2.5 Perform a Facility Loopback on a Destination-Node MXP or TXP Port" procedure on page 1-17.

## 1.2.5 Perform a Facility Loopback on a Destination-Node MXP or TXP Port

You perform a facility loopback test at the destination port to determine whether this local port is the source of circuit trouble. The example in Figure 1-7 shows a facility loopback being performed on a TXP client or trunk port at a destination node.

***Figure 1-7 Facility Loopback on a Destination-Node MXP or TXP Port***




**Caution** Performing a loopback on an in-service circuit is service-affecting.

**Note** Facility loopbacks require on-site personnel.

Complete the "Create the Facility Loopback on a Destination-Node MXP or TXP Port" procedure on page 1-18.

## Create the Facility Loopback on a Destination-Node MXP or TXP Port

**Step 1** Connect an optical test set to the port you are testing:

> **Note** For specific procedures to connect, set up, and use the test set equipment, consult the manufacturer.

a. If you just completed the "1.2.4 Create a Terminal Loopback on Intermediate-Node MXP or TXP Ports" procedure on page 1-14, leave the optical test set hooked up to the source-node port.

b. If you are starting the current procedure without the optical test set hooked up to the source port, use appropriate cabling to attach the Tx and Rx terminals of the optical test set to the port you are testing. Both Tx and Rx connect to the same port.

**Step 2** Adjust the test set accordingly. (Refer to manufacturer instructions for test set use.)

**Step 3** Create the facility loopback on the destination port being tested:

a. Go to the node view of the destination node:
   - Choose **View** > **Go To Other Node** from the menu bar.
   - Choose the node from the drop-down list in the Select Node dialog box and click **OK**.

b. In node view, double-click the card that requires the loopback.

c. Click the **Maintenance > Loopback** tabs.

d. Select **OOS,MT** (or **locked,maintenance**) from the Admin State column. If this is a multiport card, select the row appropriate for the desired port.

e. Select **Facility (Line)** from the Loopback Type column. If this is a multiport card, select the row appropriate for the desired port.

f. Click **Apply**.

g. Click **Yes** in the confirmation dialog box.

**Step 4** Complete the "Test and Clear the MXP or TXP Facility Loopback Circuit" procedure on page 1-18.

## Test and Clear the MXP or TXP Facility Loopback Circuit

**Step 1** If the test set is not already sending traffic, send test traffic on the loopback circuit.

**Step 2** Examine the traffic received by the test set. Look for errors or any other signal information that the test set is capable of indicating.

**Step 3** If the test set indicates no errors, no further testing is necessary with the facility loopback. Clear the facility loopback from the port:

a. Click the **Maintenance > Loopback** tabs.

b. Choose **None** from the Loopback Type column for the port being tested.

c. Choose the appropriate state to place the port in service, out of service and disabled, out of service for maintenance, or automatically in service from the Admin State column for the port being tested.

d. Click **Apply**.

e. Click **Yes** in the confirmation dialog box.

**Step 4** Complete the "Test the MXP or TXP Card" procedure on page 1-19.

## Test the MXP or TXP Card

**Step 1** Complete the "Physically Replace a Card" procedure on page 2-154 for the suspected bad card and replace it with a known-good one.

**Caution** Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Refer to the procedures in the "2.9.1 Protection Switching, Lock Initiation, and Clearing" section on page 2-149. For more information, refer to the "Maintain the Node" chapter in the *Cisco ONS 15454 DWDM Procedure Guide*.

**Step 2** Resend test traffic on the loopback circuit with a known-good card installed.

**Step 3** If the test set indicates no errors, the problem was probably the defective card. Return the defective card to Cisco through the RMA process. Contact Cisco Technical Support (1 800 553-2447).

**Step 4** Complete the "Physically Replace a Card" procedure on page 2-154 for the faulty card.

**Step 5** Clear the facility loopback on the port:

a. Click the **Maintenance > Loopback** tabs.

b. Choose **None** from the Loopback Type column for the port being tested.

c. Choose the appropriate state to place the port in service, out of service and disabled, out of service for maintenance, or automatically in service from the Admin State column for the port being tested.

d. Click **Apply**.

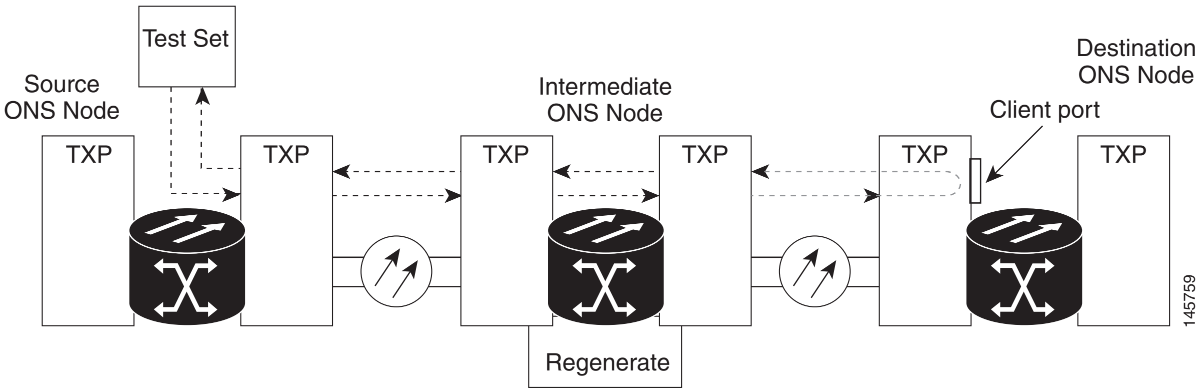
e. Click **Yes** in the confirmation dialog box.

**Step 6** Complete the "1.2.6 Perform a Terminal Loopback on a Destination-Node MXP or TXP Port" procedure on page 1-19.

# 1.2.6 Perform a Terminal Loopback on a Destination-Node MXP or TXP Port

The terminal loopback at the destination-node port is the final local hardware error elimination in the circuit troubleshooting process. If this test is completed successfully, you have verified that the circuit is good up to the destination port. The example in Figure 1-8 shows a terminal loopback on an destination node TXP port.

*Figure 1-8 Terminal Loopback on a Destination-Node MXP or TXP Port*




**Caution** Performing a loopback on an in-service circuit is service-affecting.

**Note** Terminal loopbacks require on-site personnel.

Complete the "Create the Terminal Loopback on a Destination-Node MXP or TXP Port" procedure on page 1-20.

## Create the Terminal Loopback on a Destination-Node MXP or TXP Port

**Step 1** Connect an optical test set to the port you are testing:

**Note** For specific procedures to connect, set up, and use the test set equipment, consult the manufacturer.

**a.** If you just completed the "1.2.5 Perform a Facility Loopback on a Destination-Node MXP or TXP Port" procedure on page 1-17, leave the optical test set hooked up to the source port.

**b.** If you are starting the current procedure without the optical test set hooked up to the source port, use appropriate cabling to attach the Tx and Rx terminals of the optical test set to the port you are testing. Both Tx and Rx connect to the same port.

**Step 2** Adjust the test set accordingly. (Refer to manufacturer instructions for test set use.)

**Note** It is normal for the "LPBKTERMINAL (ESCON)" condition on page 2-85, "LPBKTERMINAL (FC)" condition on page 2-86, "LPBKTERMINAL (GE)" condition on page 2-86, "LPBKTERMINAL (ISC)" condition on page 2-87 or the "LPBKTERMINAL (TRUNK)" condition on page 2-87 to appear during loopback setup. The condition clears when you remove the loopback.

**Step 3** Create the terminal loopback on the destination port being tested:

**a.** Go to the node view of the destination node:

- Choose **View > Go To Other Node** from the menu bar.

- Choose the node from the drop-down list in the Select Node dialog box and click **OK**.

**b.** In node view, double-click the card that requires the loopback.

**c.** Click the **Maintenance > Loopback** tabs.

**d.** Select **OOS,MT** (or **locked,maintenance**) from the Admin State column. If this is a multiport card, select the row appropriate for the desired port.

**e.** Select **Terminal (Inward)** from the Loopback Type column. If this is a multiport card, select the row appropriate for the desired port.

**f.** Click **Apply**.

**g.** Click **Yes** in the confirmation dialog box.

**Step 4** Complete the "Test and Clear the MXP or TXP Terminal Loopback Circuit" procedure on page 1-21.

## Test and Clear the MXP or TXP Terminal Loopback Circuit

**Step 1** If the test set is not already sending traffic, send test traffic on the loopback circuit.

**Step 2** Examine the test traffic being received by the test set. Look for errors or any other signal information that the test set is capable of indicating.

**Step 3** If the test set indicates no errors, no further testing is necessary on the loopback circuit. Clear the terminal loopback from the port:

**a.** Double-click the intermediate-node card with the terminal loopback.

**b.** Click the **Maintenance > Loopback** tabs.

**c.** Select **None** from the Loopback Type column for the port being tested.

**d.** Choose the appropriate state to place the port in service, out of service and disabled, out of service for maintenance, or automatically in service from the Admin State column for the port being tested.

**e.** Click **Apply**.

**f.** Click **Yes** in the confirmation dialog box.

**Step 4** If the test set indicates errors, the problem might be a faulty card.

**Step 5** Complete the "Test the MXP or TXP Card" procedure on page 1-21.

## Test the MXP or TXP Card

**Step 1** Complete the "Physically Replace a Card" procedure on page 2-154 for the suspected bad card and replace it with a known-good one.

**Caution** Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Refer to the procedures in the "2.9.1 Protection Switching, Lock Initiation, and Clearing" section on page 2-149. For more information, refer to the "Maintain the Node" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Step 2** Resend test traffic on the loopback circuit with a known-good card.

**Step 3** If the test set indicates no errors the problem was probably the defective card. Return the defective card to Cisco through the RMA process. Contact Cisco Technical Support (1 800 553-2447).

**Step 4** Complete the "Physically Replace a Card" procedure on page 2-154 for the defective card.

**Step 5** Clear the terminal loopback on the port:

- **a.** Double-click the source-node card with the terminal loopback.
- **b.** Click the **Maintenance > Loopback** tabs.
- **c.** Select **None** from the Loopback Type column for the port being tested.
- **d.** Choose the appropriate state to place the port in service, out of service and disabled, out of service for maintenance, or automatically in service from the Admin State column for the port being tested.
- **e.** Click **Apply**.
- **f.** Click **Yes** in the confirmation dialog box.

The entire circuit path has now passed its comprehensive series of loopback tests. This circuit qualifies to carry live traffic.

# 1.3 Troubleshooting DWDM Circuit Paths With ITU-T G.709 Monitoring

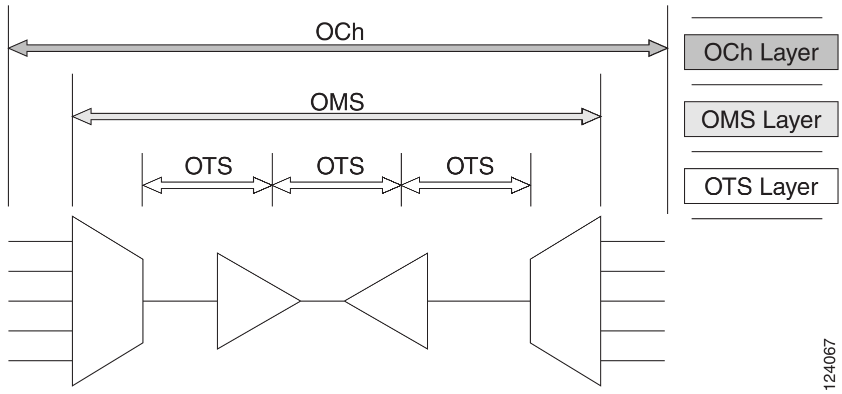
This section provides an overview of the optical transport network (OTN) specified in ITU-T G.709, *Network Node Interface for the Optical Transport Network*, and provides troubleshooting procedures for DWDM circuit paths in the ITU-T G.709 OTN using PM and TCAs.

## 1.3.1 G.709 Monitoring in Optical Transport Networks

Recommendation ITU-T G.709 is part of a suite of recommendations covering the full functionality of an OTN. ITU-T G.709 enables single-wavelength SONET transparent optical wavelength-based networks. ITU-T G.709 adds the Operation, Administration, Maintenance, and Provisioning (OAM&P) functionality of SONET/SDH to DWDM optical networks. It adds extra overhead to existing SONET, Ethernet, or asynchronous transfer mode (ATM) bit streams for performance management and improvement.

Like traditional SONET networks, ITU-T G.709 optical networks have a layered design (Figure 1-9). This structure enables localized monitoring that helps you isolate and troubleshoot network problems.

*Figure 1-9 Optical Transport Network Layers*




# 1.3.2 Optical Channel Layer

The optical channel (OCH) layer is the outermost part of the OTN and spans from client to client. The optical channel is built as follows:

1. A client signal such as SONET, Gigabit Ethernet, IP, ATM, Fibre Channel, or enterprise system connection (ESCON) is mapped to a client payload area and combined with an overhead to create the optical channel payload unit (OPUk).
2. A second overhead is added to the OPUk unit to create the optical channel data unit (ODUk).
3. A third overhead including forward error correction (FEC) is added to the ODUk to create the optical channel transport unit (OTUk).
4. A fourth overhead is added to the OTUk to create the entire OCH layer.

# 1.3.3 Optical Multiplex Section Layer

The optical multiplex section (OMS) of the OTN allows carriers to identify errors occurring within DWDM network sections. The OMS layer consists of a payload and an overhead (OMS-OH). It supports the ability to monitor multiplexed sections of the network, for example, the span between an optical multiplexer such as the 32MUX-O card and an optical demultiplexer such as the 32DMX-O card.

# 1.3.4 Optical Transmission Section Layer

The optical transmission section (OTS) layer supports monitoring partial spans of a network's multiplexed sections. This layer consists of a payload and an overhead (OTS-OH). It is a transmission span between two elements in an optical network, such as between:

- A multiplexer such as the 32MUX-O card and an amplifier such as the OPT-PRE card
- An amplifier and another amplifier, such as the OPT-BST card and the OPT-PRE card
- An amplifier such as the OPT-BST card and a demultiplexer such as the 32DMX card

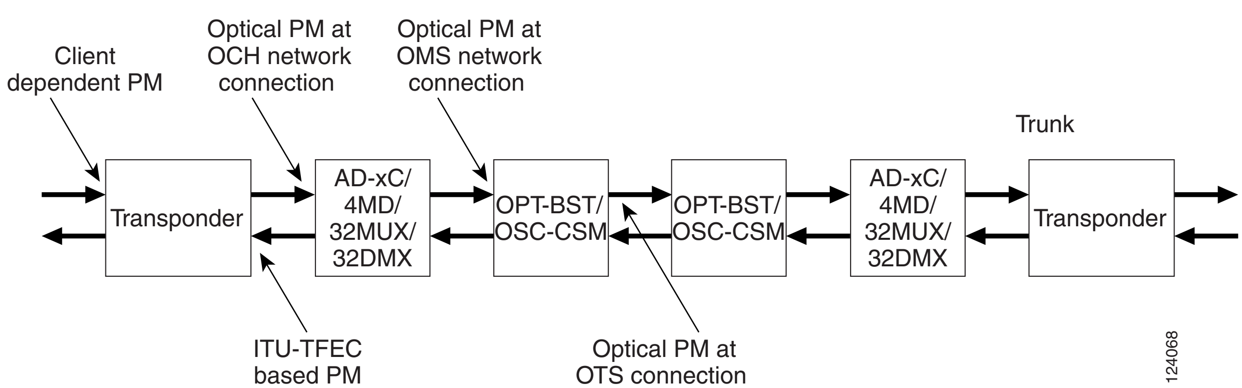
## 1.3.5 Performance Monitoring Counters and Threshold Crossing Alerts

PM counters and TCAs can be used for identifying trouble and troubleshooting problems in ITU-T G.709 optical transport networks. ITU-T Recommendation M.2401 recommends that the following PM parameters be monitored at the ODUk layer:

- SES (severely errored seconds)—A one-second period that contains greater than or equal to 30 percent errored blocks or at least one defect. SES is a subset of the errored second (ES) parameter, which is a one-second period with one or more errored blocks or at least one defect.
- BBE (background block error counter)—An errored block not occurring as part of an SES. BBE is a subset of the errored block (EB) parameter, which is a block in which one or more bits are in error.

Different PM count parameters are associated with different read points in a network. Figure 1-10 illustrates the PM read points that are useful in identifying DWDM circuit points of failure. Chapter 5, "Performance Monitoring," lists all PM parameters and provides block diagrams of signal entry points, exit points, and interconnections between the individual circuit cards. Consult these specifications to determine which PM parameters are associated with the system points you want to monitor or provision with CTC or TL1. The monitoring points can vary according to your configuration.

*Figure 1-10 Performance Monitoring Points on ONS DWDM*




TCAs are used to monitor performance through the management interface by indicating whether preset thresholds have been crossed, or whether a transmission (such as a laser transmission) is degraded. TCAs are not associated with severity levels. They are usually associated with rate, counter, and percentage parameters that are available at transponder monitoring points. Chapter 5, "Performance Monitoring," contains more information about these alerts.

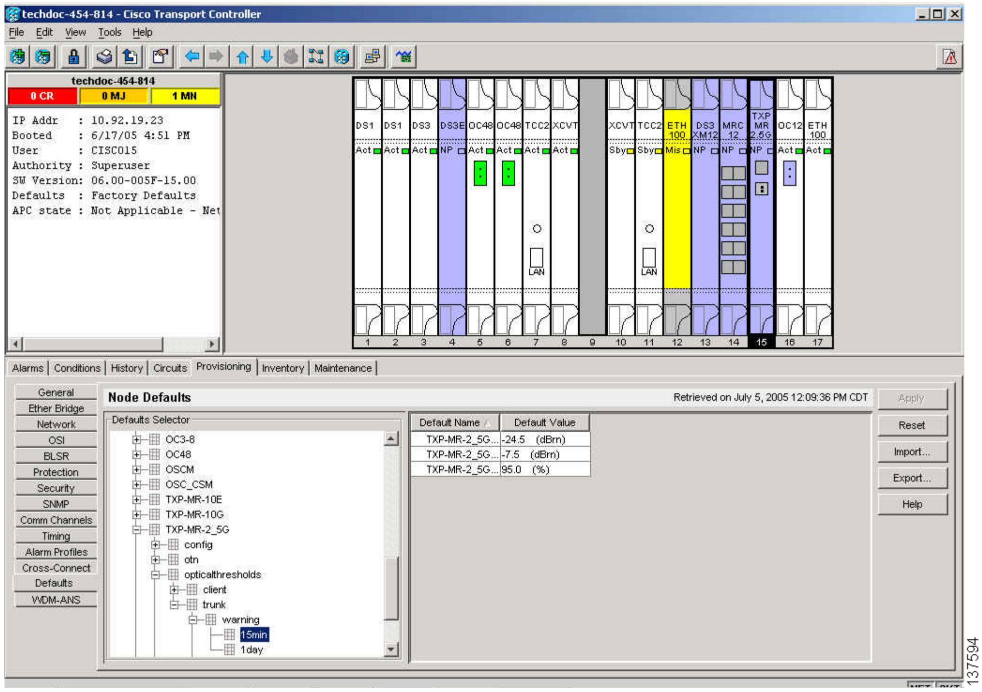
Select and complete the following procedures according to your network parameters.

## Set Node Default BBE or SES Card Thresholds

Complete the following procedure to provision default node ODUk BBE and SES PM thresholds for TXP cards.

**Step 1** In node view, click the **Provisioning** > **Defaults** tabs (Figure 1-11).

*Figure 1-11 Set Default BBE/SES Card Thresholds*



**Step 2** In the Defaults Selector field, click the transponder or muxponder card you wish to provision, then click **opticalthresholds > trunk > warning > 15min** in the drop-down list.

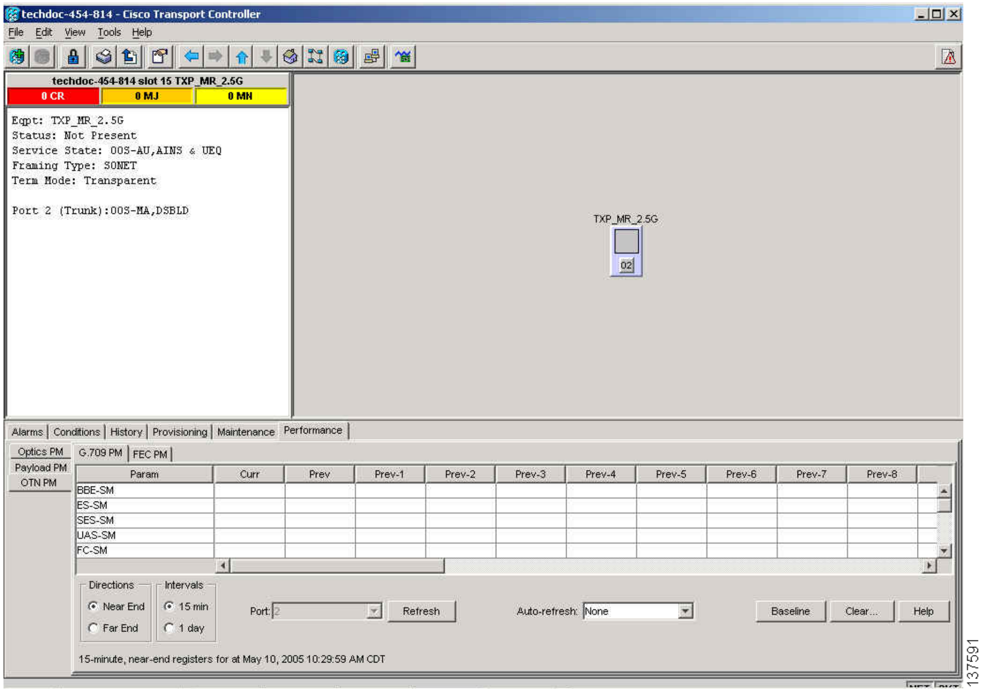
## Provision Individual Card BBE or SES Thresholds in CTC

Complete the following procedure to provision BBE or SES PM thresholds in CTC for an individual TXP card.

**Step 1** In node view, double-click the applicable transponder or muxponder card (TXP_MR_10G, TXPP_MR_2.5G, or MXP_2.5G_10G.)

**Step 2** Click the **Provisioning** > **OTN** > **G.709 Thresholds** tabs (Figure 1-12).

*Figure 1-12 Provision Card BBE/SES Thresholds*




**Step 3** In the Directions area, click the **Near End** radio button.

**Step 4** In the Intervals area, click the **15 Min** radio button.

**Step 5** In the Types area, click the **PM (ODUk)** radio button.

**Step 6** In the SES and BBE fields, enter threshold numbers, for example 500 and 10000.

## Provision Card PM Thresholds Using TL1

Complete the following procedure if you wish to provision PM thresholds in TL1 rather than in CTC.

**Step 1** Open a TL1 command line (click **Tools > Open TL1 Connection**).

**Step 2** On the TL1 command line, use the following syntax:

SET-TH-OCH:[<TID>]:<AID>:<CTAG>::<MONTYPE>,<THLEV>,[<LOCN>],,[<TMPER>];

where:

- Access Identifier (AID) identifies the NE to which the command pertains. All the STS, VT1, facility and DS1 AIDs are supported.
- The parameter MONTYPE is the monitored type.
- The parameter THLEV is optional and indicates a threshold count value (the number of errors which must be exceeded before the threshold is crossed).
- The parameter LOCN specifies the location associated with the particular command.
- The parameter TMPER is optional and is an accumulation time period for performance counters, with possible values of 1-DAY, 1-HR, 1-MIN, 15-MIN, and RAW-DATA.

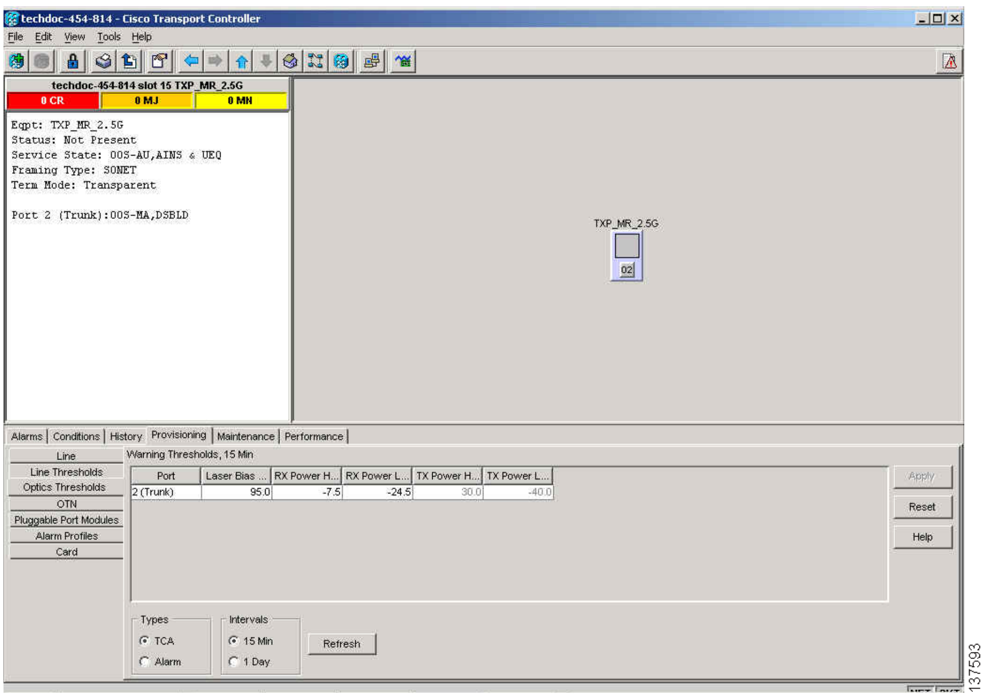
**Note** For a more information about this command and a list of TL1 commands, refer to the *Cisco SONET TL1 Command Guide* at the following link: http://www.cisco.com/en/US/products/hw/optical/ps2006/products_command_reference_book09186a0080483b9b.html

## Provision Optical TCA Thresholds

Complete the following procedure to provision TCA thresholds in CTC.

**Step 1** In card view, click the **Provisioning** > **Optics Thresholds** tabs (Figure 1-13).

***Figure 1-13 Provision Optical TCA Thresholds***




**Step 2** In the Types area, click **TCA**.

**Step 3** In the Intervals area, click **15 Min**.

**Step 4** In the Laser Bias High (%) field, enter the threshold value, for example, 81.0 percent.

# 1.3.6 Forward Error Correction

In DWDM spans, FEC reduces the quantities of retiming, reshaping, and regeneration (3R) needed to maintain signal quality. The following two PM parameters are associated with FEC:

- BIT-EC—Bit errors corrected (BIT-EC) indicates the number of bit errors corrected in the DWDM trunk line during the PM time interval.

- UNC-WORDS—The number of uncorrectable words detected in the DWDM trunk line during the PM time interval.

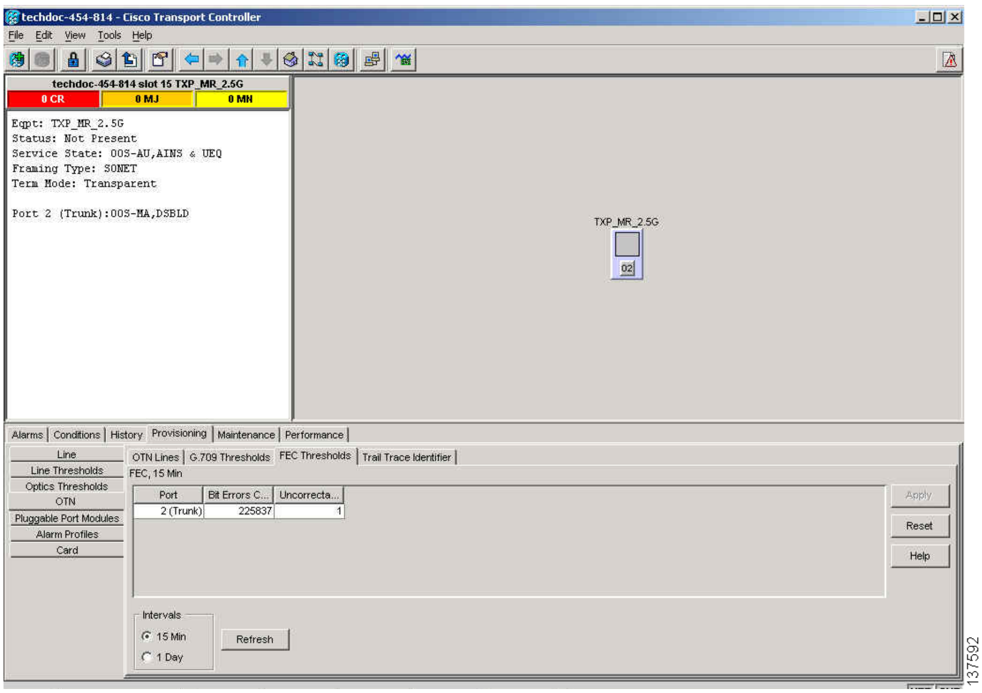
Complete the following procedure to provision BIT-EC and UNC-WORDS PM parameters for FEC.

## Provision Card FEC Thresholds

**Step 1** In node view, double-click a transponder or muxponder card to open the card view. (In this example, cards such as the TXP_MR_10G, TXPP_MR_2.5G, and MXP_2.5G_10G are applicable.)

**Step 2** Click the **Provisioning** > **OTN** > **FEC Thresholds** tabs (Figure 1-14).

***Figure 1-14 Provision Card FEC Thresholds***




**Step 3** In the Bit Errors Corrected field, enter a threshold number, for example 225837.

**Step 4** In the Uncorrectable Words field, enter a threshold number, for example, 2.

**Step 5** In the Intervals area, click **15 Min**.

# 1.3.7 Sample Trouble Resolutions

The following sample trouble resolutions use PM and TCAs to isolate degrade points.

**Symptom** There is a BBE TCA on a single transponder pair.

**Possible Cause** The transponder input power is out of range.

**Recommended Action** Check the input power on the transponder. It should be within the specified/supported range.

**Possible Cause** There are dirty trunk connectors on the transponder.

**Recommended Action** Check the connector on the trunk port.

**Possible Cause** There is a degraded trunk patchcord between the transponder and the DWDM port.

**Recommended Action** Check the patchcord on the transponder DWDM port.

**Possible Cause** There are dirty client connectors on the ADxC-xx.x card transmit port or the demultiplexer (DMX) has crossed the near-end TCA.

**Recommended Action** Check the connector on the OCH port of the ADxC-xx.x card.

**Possible Cause** There are dirty client connectors on the ADxC-xx.x card receive port or the multiplexer (MUX) has crossed the far-end TCA point.

**Recommended Action** If an optical channel bypass exists along the line, check the connectors.

**Symptom** There is a BBE TCA on all transponders connected to an ADxB-xx.x card.

**Possible Cause** The transponder input power is out of range.

**Recommended Action** Check the input power on the transponder. It should be within the specified/supported range.

**Possible Cause** There is a dirty connector on the 4MD-xx.x card port.

**Recommended Action** Check the connector on the drop port of the 4MD-xx.x card.

**Possible Cause** There is a dirty connector on the ADxB-xx.x card drop port, and it has crossed the near-end TCA point.

**Recommended Action** Check the connector on the drop port of the ADxB-xx.x card.

**Possible Cause** There is a dirty connector on the ADxB-xx.x card add port and it has crossed the far-end TCA.

**Recommended Action** Check the patchcord on the 4MD-xx.x or AD1B-xx.x card.

**Possible Cause** There is a degraded patchcord between the ADxB-xx.x and 4MD-xx.x cards.

**Recommended Action** If an optical band bypass exists along the line, check the band connectors.

**Symptom** There is a BBE TCA on all transponders that the OCH passes through a single OTS section.

**Possible Cause** This is not a transponder or channel-related issue.

**Recommended Action** The problem is in the intercabinet signal path preceding the transponder. Refer to the *Cisco ONS 15454 DWDM Procedure Guide* for more information about configurations and acceptance tests for this area.

**Symptom** You have a laser bias current (LBC) TCA on a single transponder.

**Possible Cause** The laser of the transponder is degrading.

**Recommended Action** The problem is within the laser circuitry. Check the OPT-PRE or OPT-BST optical amplifier cards. Refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide* for more information about setting up these cards.

# 1.4 Using CTC Diagnostics

In Software Release 6.0, CTC provides diagnostics for the following functions:

- Verifying proper card ASIC functionality
- Verifying standby card operation
- Verifying proper card LED operation
- Diagnostic circuit creation
- Customer problem notifications detected by alarms
- Provision of a downloadable, machine-readable diagnostic information file to be used by Cisco Technical Support

Some of these functions, such as ASIC verification and standby card operation, are invisibly monitored in background functions. Change or problem notifications are provided in the Alarms and Conditions windows. Other diagnostic functions—verifying card LED function, creating bidirectional diagnostic circuits, and also downloading diagnostic files for technical support—are available to the user in the node view Maintenance > Diagnostic tab. The user-operated diagnostic features are described in the following paragraphs.

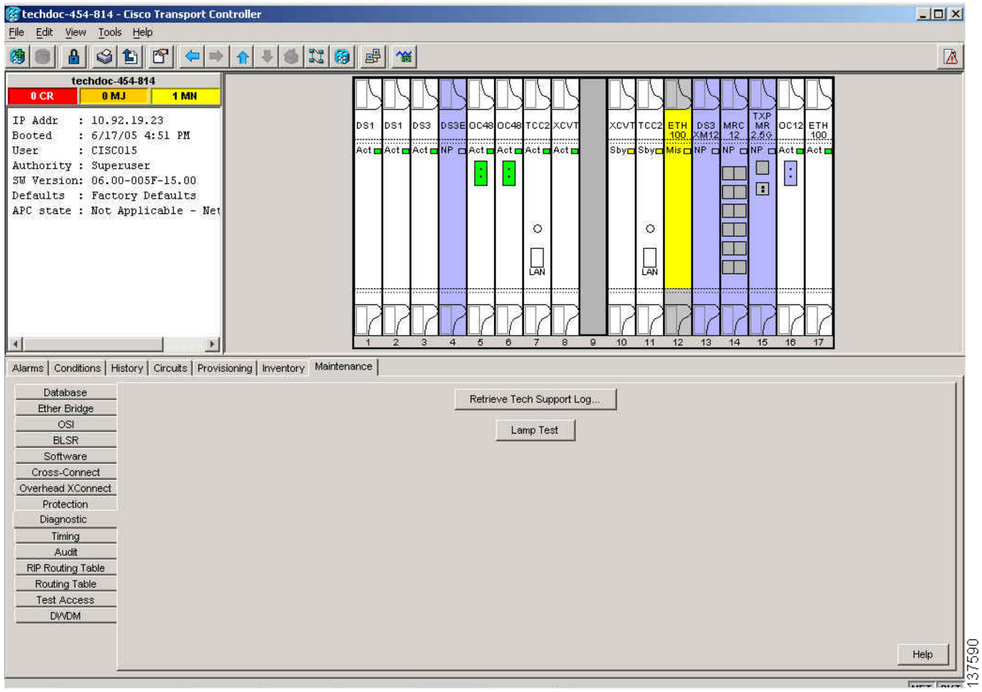
## 1.4.1 Card LED Lamp Tests

A card LED lamp test determines whether card-level indication LEDs are operational. This diagnostic test is run as part of the initial ONS 15454 turn-up, during maintenance routines, or any time you question whether an LED is in working order. Maintenance or higher-level users can complete the following tasks to verify LED operation.

### Verify Card LED Operation

**Step 1** In node view, click the **Maintenance > Diagnostic** tabs (Figure 1-15).

*Figure 1-15 CTC Node View Diagnostic Window*




**Step 2** Click **Lamp Test**.

**Step 3** Watch to make sure all the port LEDs illuminate simultaneously for several seconds, with the following durations:

- For tri-color LEDs: three 5-second cycles
- For dual-color LEDs: one 5-second cycle and one 10-second cycle
- For the AIC or AIC-I: one 15-second cycle

**Step 4** Click **OK** in the Lamp Test Run dialog box.

## 1.4.2 Retrieve Diagnostics File Button

When you click the Retrieve Diagnostics File button in the Maintenance window, CTC retrieves system data that can be off-loaded by a Maintenance or higher-level user to a local directory and sent to Technical Support for troubleshooting purposes. The diagnostics file is in machine language and is not human-readable, but can be used by Cisco Technical Support for problem analysis. Complete the following task to off-load the diagnostics file.

**Note** In addition to the machine-readable diagnostics file, the ONS 15454 also stores an audit trail of all system events such as user logins, remote logins, configuration, and changes. This audit trail is considered a record-keeping feature rather than a troubleshooting feature. Information about the feature is located in the "Maintain the Node" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

### Off-Load the Diagnostics File

**Step 1** In node view, click the **Maintenance > Diagnostic** tabs (Figure 1-15).

**Step 2** Click **Retrieve Tech Support Log**.

**Step 3** In the Saving Diagnostic File dialog box, navigate to the directory (local or network) where you want to save the file.

**Step 4** Enter a name in the File Name field.

You do not have to give the archive file a particular extension. It is a compressed file (gzip) that can be unzipped and read by Cisco Technical Support.

**Step 5** Click **Save**.

The Get Diagnostics status window shows a progress bar indicating the percentage of the file being saved, then shows "Get Diagnostics Complete."

**Step 6** Click **OK**.

# 1.5 Restoring the Database and Default Settings

This section contains troubleshooting for node operation errors that require restoration of software data or the default node setup.

## 1.5.1 Restore the Node Database

**Symptom** One or more nodes do not function properly or have incorrect data.

**Possible Cause** Incorrect or corrupted node database.

**Recommended Action** Complete the procedures in the "Maintain the Node" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

# 1.6 PC Connectivity Troubleshooting

This section contains information about system minimum requirements, supported platforms, browsers, and Java Runtime Environments (JREs) for Software R6.0, and troubleshooting procedures for PC and network connectivity to the ONS 15454.

## 1.6.1 PC System Minimum Requirements

Workstations running CTC Software R6.0 for the Optical Networking System (ONS) products on Windows platforms need to have the following minimum requirements:

- Pentium III or higher processor
- Processor speed of at least 700 MHz

- 256 MB or more of RAM
- 50 MB or more of available hard disk space
- 20 GB or larger hard drive

## 1.6.2 Sun System Minimum Requirements

Workstations running Software R6.0 for the ONS products on Sun workstations need to have the following minimum requirements:

- UltraSPARC or faster processor
- 256 MB or more of RAM
- 50 MB or more of available hard disk space

## 1.6.3 Supported Platforms, Browsers, and JREs

Software R6.0 supports the following platforms:

- Windows NT
- Windows 98
- Windows XP
- Windows 2000
- Solaris 8
- Solaris 9

Software R6.0 supports the following browsers and JREs:

- Netscape 7 browser (PC or Solaris 8 or 9 with Java plug-in 1.4.2)
- PC platforms with Java plug-in 1.4.2
- Internet Explorer 6.0 browser (on PC platforms with Java plug-in 1.4.2)
- Mozilla 1.7 (Solaris only)

**Note** You can obtain browsers at the following URLs:

- Netscape: http://channels.netscape.com/ns/browsers/default.jsp
- Internet Explorer: http://www.microsoft.com
- Mozilla: http://mozilla.org

**Note** The required JRE version is JRE 1.4.2. It is compatible with R4.6 and later.

**Note** JRE 1.4.2 for Windows and Solaris is available on Software R6.0 product CDs.

## 1.6.4 Unsupported Platforms and Browsers

Software R6.0 does not support the following platforms:

- Windows 95
- Solaris 2.5
- Solaris 2.6

Software R6.0 does not support the following browsers and JREs:

- Netscape 4.73 for Windows.
- Netscape 4.76 on Solaris.
- Netscape 7 on Solaris 8 or 9 is only supported with JRE 1.4.2.

## 1.6.5 Unable to Verify the IP Configuration of Your PC

**Symptom** When connecting your PC to the ONS 15454, you are unable to successfully ping the IP address of your PC to verify the IP configuration.

**Possible Cause** The IP address was entered incorrectly.

**Recommended Action** Verify that the IP address used to ping the PC matches the IP address displayed when in the Windows IP Configuration information retrieved from the system. See the "Verify the IP Configuration of Your PC" procedure on page 1-34.

**Possible Cause** The IP configuration of your PC is not properly set.

**Recommended Action** Verify the IP configuration of your PC. Complete the "Verify the IP Configuration of Your PC" procedure on page 1-34. If this procedure is unsuccessful, contact your network administrator for instructions to correct the IP configuration of your PC.

### Verify the IP Configuration of Your PC

**Step 1** Open a DOS command window by selecting **Start > Run** from the Start menu.

**Step 2** In the Open field, type **command** and then click **OK**. The DOS command window appears.

**Step 3** At the prompt in the DOS window, type **ipconfig** and press the **Enter** key.

The Windows IP configuration information appears, including the IP address, the subnet mask, and the default gateway.

**Note** The winipcfg command only returns the information above if you are on a network.

**Step 4** At the prompt in the DOS window, type **ping** followed by the IP address shown in the Windows IP configuration information previously displayed.

**Step 5** Press the **Enter** key to execute the command.

If the DOS window returns multiple (usually four) replies, the IP configuration is working properly.

If you do not receive a reply, your IP configuration might not be properly set. Contact your network administrator for instructions to correct the IP configuration of your PC.

## 1.6.6 Browser Login Does Not Launch Java

**Symptom** The message "Loading Java Applet" does not appear and the JRE does not launch during the initial login.

**Possible Cause** The PC operating system and browser are not properly configured.

**Recommended Action** Reconfigure the PC operating system Java Plug-in Control Panel and the browser settings. Complete the "Reconfigure the PC Operating System Java Plug-in Control Panel" procedure on page 1-35 and the "Reconfigure the Browser" procedure on page 1-35.

### Reconfigure the PC Operating System Java Plug-in Control Panel

**Step 1** From the Windows start menu, click **Settings > Control Panel**.

**Step 2** If **Java Plug-in** does not appear, the JRE might not be installed on your PC:

- **a.** Run the Cisco ONS 15454 software CD.
- **b.** Open the *CD-drive*:\Windows\JRE folder.
- **c.** Double-click the **j2re-1_4_2-win** icon to run the JRE installation wizard.
- **d.** Follow the JRE installation wizard steps.

**Step 3** From the Windows start menu, click **Settings > Control Panel**.

**Step 4** In the Java Plug-in Control Panel window, double-click the **Java Plug-in 1.4.2** icon.

**Step 5** Click the **Advanced** tab on the Java Plug-in Control Panel.

**Step 6** Navigate to **C:\ProgramFiles\JavaSoft\JRE\1.4.2**.

**Step 7** Select **JRE 1.4**.

**Step 8** Click **Apply**.

**Step 9** Close the Java Plug-in Control Panel window.

### Reconfigure the Browser

**Step 1** From the Start Menu, launch your browser application.

**Step 2** If you are using Netscape Navigator:

- **a.** From the Netscape Navigator menu bar, click the **Edit > Preferences** menus.
- **b.** In the Preferences window, click the **Advanced > Proxies** categories.
- **c.** In the Proxies window, click the **Direct connection to the Internet** check box and click **OK**.
- **d.** From the Netscape Navigator menu bar, click the **Edit > Preferences** menus.

e. In the Preferences window, click the **Advanced > Cache** categories.

f. Confirm that the Disk Cache Folder field shows one of the following paths:

- For Windows 98/ME: **C:\ProgramFiles\Netscape\Communicator\cache**
- For Windows NT/2000/XP: **C:\ProgramFiles\Netscape***username***\Communicator\cache**

g. If the Disk Cache Folder field is not correct, click **Choose Folder**.

h. Navigate to the file listed in Step f, and click **OK**.

i. Click **OK** in the Preferences window and exit the browser.

**Step 3** If you are using Internet Explorer:

a. From the Internet Explorer menu bar, click the **Tools > Internet Options** menus.

b. In the Internet Options window, click the **Advanced** tab.

c. In the Settings menu, scroll down to Java (Sun) and click the **Use Java 2 v1.4.2 for** *applet* **(requires restart)** check box.

d. Click **OK** in the Internet Options window and exit the browser.

**Step 4** Temporarily disable any virus-scanning software on the computer. See the "1.7.4 Browser Stalls When Downloading CTC JAR Files From TCC2/TCC2P Card" section on page 1-41.

**Step 5** Verify that the computer does not have two network interface cards (NICs) installed. If the computer does have two NICs, remove one.

**Step 6** Restart the browser and log onto the ONS 15454.

## 1.6.7 Unable to Verify the NIC Connection on Your PC

**Symptom** When connecting your PC to the ONS 15454, you are unable to verify that the NIC connection is working properly because the link LED is not illuminated or flashing.

**Possible Cause** The CAT-5 cable is not plugged in properly.

**Recommended Action** Confirm that both ends of the cable are properly inserted. If the cable is not fully inserted due to a broken locking clip, the cable should be replaced.

**Possible Cause** The CAT-5 cable is damaged.

**Recommended Action** Ensure that the cable is in good condition. If in doubt, use a known-good cable. Often, cabling is damaged due to pulling or bending. (For information about installing cable, refer to the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.)

**Possible Cause** Incorrect type of CAT-5 cable is being used.

**Recommended Action** If connecting an ONS 15454 directly to your laptop, a PC, or a router, use a straight-through CAT-5 cable. When connecting the ONS 15454 to a hub or a LAN switch, use a crossover CAT-5 cable. For details on the types of CAT-5 cables, see the "1.9.2.1 Crimp Replacement LAN Cables" section on page 1-52.

**Possible Cause** The NIC is improperly inserted or installed.

**Recommended Action** If you are using a Personal Computer Memory Card International Association (PCMCIA)-based NIC, remove and reinsert the NIC to make sure the NIC is fully inserted. (If the NIC is built into the laptop or PC, verify that the NIC is not faulty.)

**Possible Cause** The NIC is faulty.

**Recommended Action** Confirm that the NIC is working properly. If you have no issues connecting to the network (or any other node), then the NIC should be working correctly. If you have difficulty connecting a to the network (or any other node), then the NIC might be faulty and needs to be replaced.

## 1.6.8 Verify PC Connection to the ONS 15454 (ping)

**Symptom** The TCP/IP connection was established and then lost.

**Possible Cause** A lost connection between the PC and the ONS 15454.

**Recommended Action** Use a standard ping command to verify the TCP/IP connection between the PC and the ONS 15454 TCC2/TCC2P card. A ping command should work if the PC connects directly to the TCC2/TCC2P card or uses a LAN to access the TCC2/TCC2P card. Complete the "Ping the ONS 15454" procedure on page 1-37.

### Ping the ONS 15454

**Step 1** Display the command prompt:

a. If you are using a Microsoft Windows operating system, from the Start Menu choose **Run**, enter **command** in the Open field of the Run dialog box, and click **OK**.

b. If you are using a Sun Solaris operating system, from the Common Desktop Environment (CDE) click the **Personal Application tab** and click **Terminal.**

**Step 2** For both the Sun and Microsoft operating systems, at the prompt enter:

**ping** *ONS-15454-IP-address*

For example:

**ping 198.168.10.10**

**Step 3** If the workstation has connectivity to the ONS 15454, the ping is successful and displays a reply from the IP address. If the workstation does not have connectivity, a "Request timed out" message appears.

**Step 4** If the ping is successful, it demonstrates that an active TCP/IP connection exists. Restart CTC.

**Step 5** If the ping is not successful, and the workstation connects to the ONS 15454 through a LAN, check that the workstation's IP address is on the same subnet as the ONS node.

**Step 6** If the ping is not successful and the workstation connects directly to the ONS 15454, check that the link light on the workstation's NIC is illuminated.

## 1.6.9 The IP Address of the Node is Unknown

**Symptom** The IP address of the node is unknown and you are unable to login.

**Possible Cause** The node is not set to the default IP address.

**Recommended Action** Leave one TCC2/TCC2P card in the shelf. Connect a PC directly to the remaining TCC2/TCC2P card and perform a hardware reset of the card. The TCC2/TCC2P card transmits the IP address after the reset to enable you to capture the IP address for login. Complete the "Retrieve Unknown Node IP Address" procedure on page 1-38.

### Retrieve Unknown Node IP Address

**Step 1** Connect your PC directly to the active TCC2/TCC2P card Ethernet port on the faceplate.

**Step 2** Start the Sniffer application on your PC.

**Step 3** Perform a hardware reset by pulling and reseating the active TCC2/TCC2P card.

**Step 4** After the TCC2/TCC2P card completes resetting, it broadcasts its IP address. The Sniffer software on your PC will capture the IP address being broadcast.

# 1.7 CTC Operation Troubleshooting

This section contains troubleshooting procedures for CTC login or operation problems.

## 1.7.1 CTC Colors Do Not Appear Correctly on a UNIX Workstation

**Symptom** When running CTC on a UNIX workstation, the colors do not appear correctly. For example, both major and minor alarms appear in the same color.

**Possible Cause** When running in 256-color mode on a UNIX workstation, color-intensive applications such as Netscape might use all of the colors.

**Recommended Action** CTC requires a full 24-color palette to run properly. When logging into CTC on a UNIX workstation, run as many colors as your adapter will support. In addition, you can use the -install or the -ncols 32 command line options to limit the number of colors that Netscape uses. Complete the "Limit Netscape Colors" procedure on page 1-38. If the problem persists after limiting Netscape colors, exit any other color-intensive applications in use.

### Limit Netscape Colors

**Step 1** Close the current session of Netscape.

**Step 2** Launch Netscape from the command line by entering one of the following commands:

- **netscape -install** (installs Netscape colors for Netscape use)
- **netscape -ncols 32** (limits Netscape to 32 colors so that if the requested color is not available, Netscape chooses the closest color option)

## 1.7.2 Unable to Launch CTC Help After Removing Netscape

**Symptom** After removing Netscape and running CTC using Internet Explorer, you are unable to launch CTC Help and receive an "MSIE is not the default browser" error message.

**Possible Cause** Loss of association between browser and Help files.

**Recommended Action** When the CTC software and Netscape are installed, the Help files are associated with Netscape by default. When you remove Netscape, the Help files are not automatically associated with Internet Explorer as the default browser. Reset Internet Explorer as the default browser so that CTC associates the Help files to the correct browser. Complete the "Reset Internet Explorer as the Default Browser for CTC" procedure on page 1-39 to associate the CTC Help files to the correct browser.

### Reset Internet Explorer as the Default Browser for CTC

**Step 1** Open the Internet Explorer browser.

**Step 2** From the menu bar, click **Tools** > **Internet Options**. The Internet Options window appears.

**Step 3** In the Internet Options window, click the **Programs** tab.

**Step 4** Click the **Internet Explorer should check to see whether it is the default browser** check box.

**Step 5** Click **OK**.

**Step 6** Exit any and all open and running CTC and Internet Explorer applications.

**Step 7** Launch Internet Explorer and open a new CTC session. You should now be able to access the CTC Help.

## 1.7.3 Unable to Change Node View to Network View

**Symptom** When activating a large, multinode BLSR from Software R3.2 to Software R3.3, some of the nodes appear grayed out. Logging into the new CTC, the user is unable to change node view to network view on any nodes, from any workstation. This is accompanied by an "Exception occurred during event dispatching: java.lang.OutOfMemoryError" in the java window.

**Possible Cause** The large, multinode BLSR requires more memory for the graphical user interface (GUI) environment variables.

**Recommended Action** Set the system or user CTC_HEAP environment variable to increase the memory limits. Complete the "Set the CTC_HEAP and CTC_MAX_PERM_SIZE_HEAP Environment Variables for Windows" procedure on page 1-40 or the "Set the CTC_HEAP and CTC_MAX_PERM_SIZE_HEAP Environment Variables for Solaris" procedure on page 1-41 to enable the CTC_HEAP variable change.

**Note** This problem typically affects large networks where additional memory is required to manage large numbers of nodes and circuits.

### Set the CTC_HEAP and CTC_MAX_PERM_SIZE_HEAP Environment Variables for Windows

**Note** Before proceeding with the following steps, ensure that your system has a minimum of 1 GB of RAM. If your system does not have a minimum of 1 GB of RAM, contact the Cisco Technical Assistance Center (TAC).

**Step 1** Close all open CTC sessions and browser windows.

**Step 2** From the Windows **Start** menu, choose **Control Panel > System**.

**Step 3** In the System Properties window, click the **Advanced** tab.

**Step 4** Click the **Environment Variables** button to open the Environment Variables window.

**Step 5** Click the **New** button under the System variables field.

**Step 6** Type `CTC_HEAP` in the Variable Name field.

**Step 7** Type `512` in the Variable Value field, and then click the **OK** button to create the variable.

**Step 8** Again, click the **New** button under the System variables field.

**Step 9** Type `CTC_MAX_PERM_SIZE_HEAP` in the Variable Name field.

**Step 10** Type `128` in the Variable Value field, and then click the **OK** button to create the variable.

**Step 11** Click the **OK** button in the Environment Variables window to accept the changes.

**Step 12** Click the **OK** button in the System Properties window to accept the changes.

### Set the CTC_HEAP and CTC_MAX_PERM_SIZE_HEAP Environment Variables for Solaris

**Step 1** From the user shell window, kill any CTC sessions and broswer applications.

**Step 2** In the user shell window, set the environment variables to increase the heap size.

**Example**

The following example shows how to set the environment variables in the C shell:

```
% setenv CTC_HEAP 512
% setenv CTC_MAX_PERM_SIZE_HEAP 128
```

## 1.7.4 Browser Stalls When Downloading CTC JAR Files From TCC2/TCC2P Card

**Symptom** The browser stalls or hangs when downloading a CTC Java archive (JAR) file from the TCC2/TCC2P card.

**Possible Cause** McAfee VirusScan software might be interfering with the operation. The problem occurs when the VirusScan Download Scan is enabled on McAfee VirusScan 4.5 or later.

**Recommended Action** Disable the VirusScan Download Scan feature. Complete the "Disable the VirusScan Download Scan" procedure on page 1-41.

### Disable the VirusScan Download Scan

**Step 1** From the Windows Start menu, choose **Programs > Network Associates > VirusScan Console**.

**Step 2** Double-click the **VShield** icon listed in the VirusScan Console dialog box.

**Step 3** Click **Configure** on the lower part of the Task Properties window.

**Step 4** Click the **Download Scan** icon on the left of the System Scan Properties dialog box.

**Step 5** Uncheck the **Enable Internet download scanning** check box.

**Step 6** Click **Yes** when the warning message appears.

**Step 7** Click **OK** in the System Scan Properties dialog box.

**Step 8** Click **OK** in the Task Properties window.

**Step 9** Close the McAfee VirusScan window.

## 1.7.5 CTC Does Not Launch

**Symptom** CTC does not launch; usually an error message appears before the login window appears.

**Possible Cause** The Netscape browser cache might point to an invalid directory.

**Recommended Action** Redirect the Netscape cache to a valid directory. Complete the "Redirect the Netscape Cache to a Valid Directory" procedure on page 1-42.

### Redirect the Netscape Cache to a Valid Directory

---

**Step 1** Launch Netscape.

**Step 2** Open the **Edit** menu.

**Step 3** Choose **Preferences**.

**Step 4** In the Category column on the left side, expand the **Advanced** category and choose the **Cache** tab.

**Step 5** Change your disk cache folder to point to the cache file location.

The cache file location is usually C:\ProgramFiles\Netscape\Users*yourname*\cache. The *yourname* segment of the file location is often the same as the user name.

---

## 1.7.6 Slow CTC Operation or Login Problems

**Symptom** You experience slow CTC operation or have problems logging into CTC.

Table 1-3 describes the potential cause of the symptom and the solution.

*Table 1-3 Slow CTC Operation or Login Problems*

| Possible Problem | Solution |
|---|---|
| The CTC cache file might be corrupted or might need to be replaced. | Search for and delete cache files. This operation forces the ONS 15454 to download a new set of Java archive (JAR) files to your computer hard drive. Complete the "Delete the CTC Cache File Automatically" procedure on page 1-43 or the "Delete the CTC Cache File Manually" procedure on page 1-44. |
| Insufficient heap memory allocation. | Increase the heap size if you are using CTC to manage more than 50 nodes concurrently. See the "Set the CTC_HEAP and CTC_MAX_PERM_SIZE_HEAP Environment Variables for Windows" procedure on page 1-40 or the "Set the CTC_HEAP and CTC_MAX_PERM_SIZE_HEAP Environment Variables for Solaris" procedure on page 1-41.<br><br>**Note** To avoid network performance issues, Cisco recommends managing a maximum of 50 nodes concurrently with CTC. To manage more than 50 nodes, Cisco recommends using Cisco Transport Manager (CTM). Cisco does not recommend running multiple CTC sessions when managing two or more large networks. |

## Delete the CTC Cache File Automatically

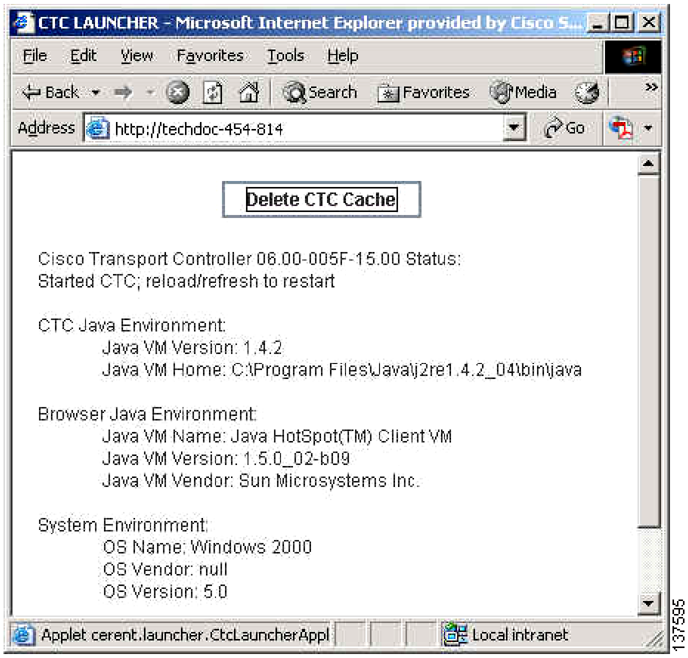
**Caution** All running sessions of CTC must be halted before deleting the CTC cache. Deleting the TC cache might cause any CTC running on this system to behave in an unexpected manner.

**Step 1** Enter an ONS 15454 IP address into the browser URL field. The initial browser window shows a **Delete CTC Cache** button.

**Step 2** Close all open CTC sessions and browser windows. The PC operating system does not allow you to delete files that are in use.

**Step 3** Click **Delete CTC Cache** in the initial browser window to clear the CTC cache. Figure 1-16 shows the Delete CTC Cache window.

*Figure 1-16 Deleting the CTC Cache*




## Delete the CTC Cache File Manually

**Caution** All running sessions of CTC must be halted before deleting the CTC cache. Deleting the CTC cache might cause any CTC running on this system to behave in an unexpected manner.

**Step 1** To delete the JAR files manually, from the Windows Start menu choose **Search > For Files or Folders**.

**Step 2** In the Search Results dialog box, enter **ctc*.jar** or **cms*.jar** in the Search for Files or Folders Named field and click **Search Now**.

**Step 3** Click the **Modified** column in the Search Results dialog box to find the JAR files that match the date when you downloaded the files from the TCC2/TCC2P.

**Step 4** Highlight the files and press the keyboard **Delete** key.

**Step 5** Click **Yes** in the Confirm dialog box.

## 1.7.7 Node Icon is Gray on CTC Network View

**Symptom** The CTC network view shows one or more node icons as gray in color and without a node name.

**Possible Cause** Different CTC releases do not recognize each other.

**Recommended Action** Correct the core version build as described in the "1.7.9 Different CTC Releases Do Not Recognize Each Other" section on page 1-46.

**Possible Cause** Username and password do not match.

**Recommended Action** Correct the username and password as described in the "1.7.10 Username or Password Do Not Match" section on page 1-47.

**Possible Cause** A lost DCC connection.

**Recommended Action** Usually accompanied by an embedded operations channel (EOC) alarm. Clear the EOC alarm and verify the DCC connection as described in the "EOC" alarm.

## 1.7.8 Java Runtime Environment Incompatible

**Symptom** The CTC application does not run properly.

**Possible Cause** The compatible Java 2 JRE is not installed.

**Recommended Action** The JRE contains the Java virtual machine, runtime class libraries, and Java application launcher that are necessary to run programs written in the Java programming language. The ONS 15454 CTC is a Java application. A Java application, unlike an applet, cannot rely completely on a web browser for installation and runtime services. When you run an application written in the Java programming language, you need the correct JRE installed. The correct JRE for each CTC software release is included on the Cisco ONS 15454 software CD. Complete the "Launch CTC to Correct the Core Version Build" procedure on page 1-46. If you are running multiple CTC software releases on a network, the JRE installed on the computer must be compatible with the different software releases. Table 1-4 shows JRE compatibility with ONS 15454 software releases.

*Table 1-4 JRE Compatibility*

| Software Release | JRE 1.2.2 Compatible | JRE 1.3 Compatible | JRE 1.4 Compatible |
|---|---|---|---|
| ONS 15454 R2.2.1 and earlier | Yes | No | No |
| ONS 15454 R2.2.2 | Yes | Yes | No |
| ONS 15454 R3.0 | Yes | Yes | No |
| ONS 15454 R3.1 | Yes | Yes | No |
| ONS 15454 R3.2 | Yes | Yes | No |
| ONS 15454 R3.3 | Yes | Yes | No |
| ONS 15454 R3.4 | No | Yes | No |

*Table 1-4 JRE Compatibility (continued)*

| Software Release | JRE 1.2.2 Compatible | JRE 1.3 Compatible | JRE 1.4 Compatible |
|---|---|---|---|
| ONS 15454 R4.0[1] | No | Yes | No |
| ONS 15454 R4.1 | No | Yes | No |
| ONS 15454 R4.5 | No | Yes | No |
| ONS 15454 R4.6 | No | Yes | Yes |
| ONS 15454 R4.7 | No | Yes | Yes |
| ONS 15454 R5.0 | No | Yes | Yes |
| ONS 15454 R6.0 | No | No | Yes |

1. Software R4.0 notifies you if an earlier JRE version is running on your PC or UNIX workstation.

### Launch CTC to Correct the Core Version Build

**Step 1** Exit the current CTC session and completely close the browser.

**Step 2** Start the browser.

**Step 3** Enter the ONS 15454 IP address of the node that reported the alarm. This can be the original IP address you logged in with or an IP address other than the original.

**Step 4** Log into CTC. The browser downloads the JAR file from CTC.

## 1.7.9 Different CTC Releases Do Not Recognize Each Other

**Symptom** Different CTC releases do not recognize each other. This situation is often accompanied by the INCOMPATIBLE-SW alarm.

**Possible Cause** The software loaded on the connecting workstation and the software on the TCC2/TCC2P card are incompatible.

**Recommended Action** This occurs when the TCC2/TCC2P software is upgraded but the PC has not yet upgraded the compatible CTC JAR file. It also occurs on login nodes with compatible software that encounter other nodes in the network that have a newer software version. Complete the "Launch CTC to Correct the Core Version Build" procedure on page 1-46.

**Note** Remember to always log into the ONS node with the latest CTC core version first. If you initially log into an ONS node running a CTC core version of 2.2 or lower and then attempt to log into another ONS node in the network running a higher CTC core version, the lower version node does not recognize the new node.

### Launch CTC to Correct the Core Version Build

**Step 1** Exit the current CTC session and completely close the browser.

**Step 2** Start the browser.

**Step 3** Enter the ONS 15454 IP address of the node that reported the alarm. This can be the original IP address you logged on with or an IP address other than the original.

**Step 4** Log into CTC. The browser downloads the JAR file from CTC.

## 1.7.10 Username or Password Do Not Match

**Symptom** A username/password mismatch often occurs concurrently with a NOT-AUTHENTICATED alarm.

**Possible Cause** The username or password entered does not match the information stored in the TCC2/TCC2P card.

**Recommended Action** All ONS nodes must have the same username and password created to display every ONS node in the network. You can also be locked out of certain ONS nodes on a network if your username and password were not created on those specific ONS nodes. For initial login to the ONS 15454, enter the CISCO15 user name in capital letters, click **Login**, and use the password **otbu+1**, which is case-sensitive.

Complete the "Verify Correct Username and Password" procedure on page 1-47. If the node has been configured for RADIUS authentication, the username and password are verified against the RADIUS server database rather than the security information in the local node database. For more information about RADIUS security, refer to the "Security Reference" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

### Verify Correct Username and Password

**Step 1** Ensure that your keyboard Caps Lock key is not turned on and affecting the case-sensitive entry of the username and password.

**Step 2** Contact your system administrator to verify the username and password.

**Step 3** Call Cisco Technical Support (1 800 553-2447) to have them enter your system and create a new user name and password.

## 1.7.11 DCC Connection Lost

**Symptom** DCC connection is lost. The node usually has alarms and the nodes in the network view have a gray icon. This symptom is usually accompanied by an EOC alarm.

**Possible Cause** A lost DCC connection.

**Recommended Action** Usually accompanied by an EOC alarm. Clear the EOC alarm and verify the DCC connection as described in the "EOC" alarm.

## 1.7.12 "Path in Use" Error When Creating a Circuit

**Symptom** While creating a circuit, you get a "Path in Use" error that prevents you from completing the circuit creation.

**Possible Cause** Another user has already selected the same source port to create another circuit.

**Recommended Action** CTC does not remove a card or port from the available list until a circuit is completely provisioned. If two users simultaneously select the same source port to create a circuit, the first user to complete circuit provisioning gets use of the port. The other user gets the "Path in Use" error. Cancel the circuit creation and start over, or click **Back** until you return to the initial circuit creation window. The source port that was previously selected no longer appears in the available list because it is now part of a provisioned circuit. Select a different available port and begin the circuit creation process again.

## 1.7.13 Calculate and Design IP Subnets

**Symptom** You cannot calculate or design IP subnets on the ONS 15454.

**Possible Cause** The IP capabilities of the ONS 15454 require specific calculations to properly design IP subnets.

**Recommended Action** Cisco provides a free online tool to calculate and design IP subnets. Go to http://www.cisco.com/techtools/ip_addr.html. For information about ONS 15454 IP capability, refer to the "Management Network Connectivity" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

# 1.8 Timing

This section provides solutions to common timing reference errors and alarms.

## 1.8.1 ONS 15454 Switches Timing Reference

**Symptom** Timing references switch when one or more problems occur.

**Possible Cause** The optical or building integrated timing supply (BITS) input is receiving loss of signal (LOS), loss of frame (LOF), or AIS alarms from its timing source.

**Possible Cause** The optical or BITS input is not functioning.

**Possible Cause** The synchronization status messaging (SSM) message is set to do not use for synchronization (DUS).

**Possible Cause** SSM indicates a Stratum 3 or lower clock quality.

**Possible Cause** The input frequency is off by more than 15 ppm.

**Possible Cause** The input clock wanders and has more than three slips in 30 seconds.

**Possible Cause** A bad timing reference existed for at least two minutes.

**Recommended Action** The ONS 15454 internal clock operates at a Stratum 3E level of accuracy. This gives the ONS 15454 a free-running synchronization accuracy of +/– 4.6 ppm and a holdover stability of less than 255 slips in the first 24 hours or 3.7 x $10^{-7}$/day, including temperature. ONS 15454 free-running synchronization relies on the Stratum 3 internal clock. Over an extended time period, using a higher quality Stratum 1 or Stratum 2 timing source results in fewer timing slips than a lower quality Stratum 3 timing source.

## 1.8.2 Holdover Synchronization Alarm

**Symptom** The clock is running at a different frequency than normal and the "HLDOVRSYNC" alarm appears.

**Possible Cause** The last reference input has failed.

**Recommended Action** The clock is running at the frequency of the last known-good reference input. This alarm is raised when the last reference input fails. See the "HLDOVRSYNC" alarm on page 2-54 for a detailed description.

**Note** The ONS 15454 supports holdover timing per Telcordia GR-436 when provisioned for external (BITS) timing.

## 1.8.3 Free-Running Synchronization Mode

**Symptom** The clock is running at a different frequency than normal and the "FRNGSYNC" alarm appears.

**Possible Cause** No reliable reference input is available.

**Recommended Action** The clock is using the internal oscillator as its only frequency reference. This occurs when no reliable, prior timing reference is available. See the "FRNGSYNC" alarm on page 2-44 for a detailed description.

## 1.8.4 Daisy-Chained BITS Not Functioning

**Symptom** You are unable to daisy chain the BITS sources.

**Possible Cause** Daisy-chained BITS sources are not supported on the ONS 15454.

**Recommended Action** Daisy-chained BITS sources cause additional wander buildup in the network and are therefore not supported. Instead, use a timing signal generator to create multiple copies of the BITS clock and separately link them to each ONS 15454.

## 1.8.5 Blinking STAT LED after Installing a Card

**Symptom** After installing a card, the STAT LED blinks continuously for more than 60 seconds.

**Possible Cause** The card cannot boot because it failed the Power On Shelf Test (POST) diagnostics.

**Recommended Action** The blinking STAT LED indicates that POST diagnostics are being performed. If the LED continues to blink for more than 60 seconds, the card has failed the POST diagnostics test and has failed to boot. If the card has truly failed, an "EQPT" alarm is raised against the slot number with an "Equipment Failure" description. Check the alarm tab for this alarm to appear for the slot where the card was installed. To attempt recovery, remove and reinstall the card and observe the card boot process. If the card fails to boot, replace the card. Complete the "Physically Replace a Card" procedure on page 2-154.

**Caution** Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Refer to the procedures in the "2.9.1 Protection Switching, Lock Initiation, and Clearing" section on page 2-149. For more information, refer to the "Maintain the Node" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

# 1.9 Fiber and Cabling

This section explains problems typically caused by cabling connectivity errors. It also includes instructions for crimping CAT-5 cable and lists the optical fiber connectivity levels.

## 1.9.1 Bit Errors Appear for a Traffic Card

**Symptom** A traffic card has multiple bit errors.

**Possible Cause** Faulty cabling or low optical-line levels.

**Recommended Action** Bit errors on line (traffic) cards usually originate from cabling problems or low optical-line levels. The errors can be caused by synchronization problems, especially if pointer justification (PJ) errors are reported. Moving cards into different error-free slots will isolate the cause. Use a test set whenever possible because the cause of the errors could be external cabling, fiber, or external equipment connecting to the ONS 15454. Troubleshoot low optical levels using the "1.9.2 Faulty Fiber-Optic Connections" section on page 1-51.

## 1.9.2 Faulty Fiber-Optic Connections

**Symptom** A card has multiple alarms and/or signal errors.

**Possible Cause** Faulty fiber-optic connections. Fiber connection problems usually occur in conjunction with alarms. Refer to the appropriate trouble-clearing procedure in Chapter 2, "Alarm Troubleshooting," to address them.

**Recommended Action** Refer to the appropriate trouble-clearing procedure in Chapter 2, "Alarm Troubleshooting," to address them.

**Possible Cause** Faulty CAT-5 cables.

**Recommended Action** Faulty CAT-5 cables can be the source of alarms and signal errors. Complete the "1.9.2.1 Crimp Replacement LAN Cables" section on page 1-52.

**Possible Cause** Faulty Gigabit Interface Converters (GBICs).

**Recommended Action** Faulty GBICs can be the source of alarms and signal errors. See the "1.9.2.2 Replace Faulty SFP or XFP Connectors" section on page 1-53.

**Warning** **Invisible laser radiation may be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments.** Statement 272

**Warning** **Laser radiation presents an invisible hazard, so personnel should avoid exposure to the laser beam. Personnel must be qualified in laser safety procedures and must use proper eye protection before working on this equipment.** Statement 300

### 1.9.2.1 Crimp Replacement LAN Cables

You can crimp your own LAN cables for use with the ONS 15454. Use a cross-over cable when connecting an ONS 15454 to a hub, LAN modem, or switch, and use a LAN cable when connecting an ONS 15454 to a router or workstation. Use CAT-5 cable RJ-45 T-568B, Color Code (100 Mbps), and a crimping tool. Figure 1-17 shows the wiring of an RJ-45 connector. Figure 1-18 shows a LAN cable layout, and Table 1-5 shows the cable pinouts. Figure 1-19 shows a cross-over cable layout, and Table 1-6 shows the cross-over pinouts.

*Figure 1-17 RJ-45 Pin Numbers*

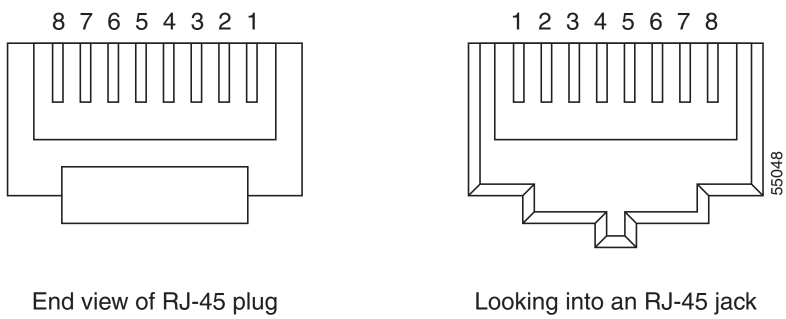



*Figure 1-18 LAN Cable Layout*

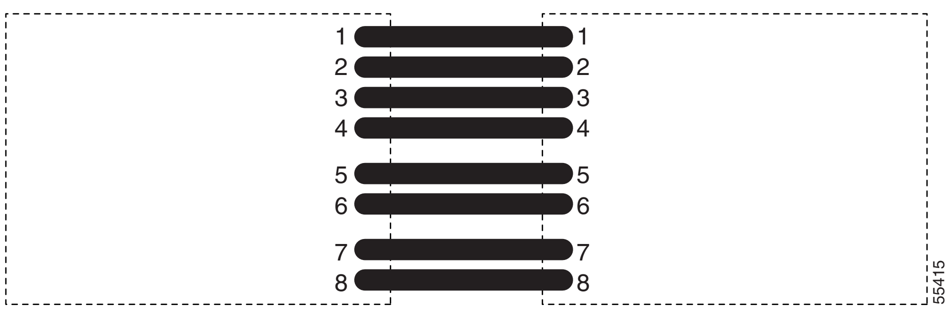



*Table 1-5 LAN Cable Pinout*

| Pin | Color | Pair | Name | Pin |
|---|---|---|---|---|
| 1 | white/orange | 2 | Transmit Data + | 1 |
| 2 | orange | 2 | Transmit Data – | 2 |
| 3 | white/green | 3 | Receive Data + | 3 |
| 4 | blue | 1 | — | 4 |
| 5 | white/blue | 1 | — | 5 |
| 6 | green | 3 | Receive Data – | 6 |
| 7 | white/brown | 4 | — | 7 |
| 8 | brown | 4 | — | 8 |

*Figure 1-19 Cross-Over Cable Layout*

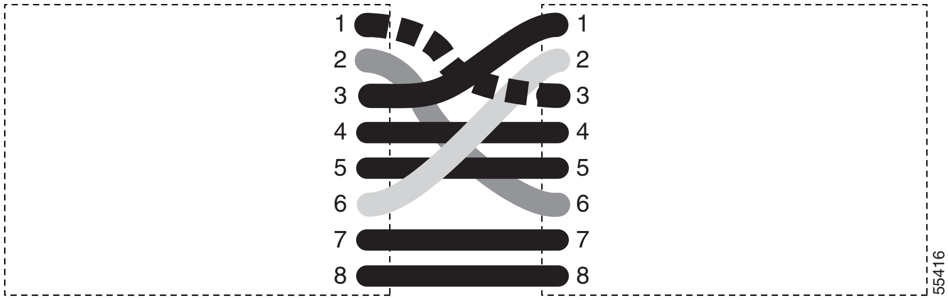



*Table 1-6 Cross-Over Cable Pinout*

| Pin | Color | Pair | Name | Pin |
|---|---|---|---|---|
| 1 | white/orange | 2 | Transmit Data + | 3 |
| 2 | orange | 2 | Transmit Data – | 6 |
| 3 | white/green | 3 | Receive Data + | 1 |
| 4 | blue | 1 | — | 4 |
| 5 | white/blue | 1 | — | 5 |
| 6 | green | 3 | Receive Data – | 2 |
| 7 | white/brown | 4 | — | 7 |
| 8 | brown | 4 | — | 8 |

**Note** Odd-numbered pins always connect to a white wire with a colored stripe.

## 1.9.2.2 Replace Faulty SFP or XFP Connectors

Small Form-factor Pluggables (SFPs) and 10-Gbps SFPs (called XFPs) are input/output devices that plug into some transponder and muxponder cards to link the port with the fiber-optic network. The type of SFP or XFP determines the maximum distance that traffic can travel from the card to the next network device. For a description of SFPs and XFPs and their capabilities, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*. SFPs and XFPs are hot-swappable and can be installed or removed while the card or shelf assembly is powered and running.

**Warning** **Class 1 laser product.** Statement 1008

**Warning** **Invisible laser radiation may be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments.** Statement 272

**Note** SFPs and XFPs must be matched on both ends by type: SX to SX, LX to LX, or ZX to ZX.

## Remove SFP or XFP Connectors

**Warning** **Invisible laser radiation may be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments.** Statement 272

**Step 1** Disconnect the network fiber cable from the SFP or XFP LC duplex connector.

**Step 2** Release the SFP or XFP from the slot by simultaneously squeezing the two plastic tabs on each side.

**Step 3** Slide the SFP out of the card slot. A flap closes over the SFP slot to protect the connector on the card.

## Install an SFP or XFP Connector

**Warning** **Class 1 laser product.** Statement 1008

**Warning** **Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard.** Statement 1056

**Step 1** Remove the SFP or XFP from its protective packaging.

**Step 2** Check the label to verify that you are using a compatible SFP or XFP for the card where you want to install the connector. Table 1-7 shows the compatible SFPs and XFPs.

**Caution** Only use SFPs/XFPs certified for use in Cisco ONSs. The qualified Cisco SFP/XFP pluggable module top assembly numbers (TANs) are provided in Table 1-7.

*Table 1-7 SFP/XFP Card Compatibility*

| Card | Compatible SFP/XFP (Cisco Product ID) | Cisco Top Assembly Number (TAN) |
|---|---|---|
| MXP_2.5G_10G (ONS 15454 SONET/SDH) | 15454-SFP-OC48-IR=<br>ONS-SE-2G-S1= | 10-1975-01<br>10-2017-01 |
| MXP_2.5G_10E (ONS 15454 SONET/SDH) | 15454-SFP-OC48-IR=<br>ONS-SE-2G-S1=<br>ONS-SE-2G-L2= | 10-1975-01<br>10-2017-01<br>10-2013-01 |
| MXP_MR_2.5G<br>MXPP_MR_2.5G | 15454-SFP-GE+-LX=<br>15454E-SFP-GE+-LX=<br>15454-SFP-GEFC-SX=<br>15454E-SFP-GEFC-S=<br>ONS-SE-GE-ZX= | 10-1832-03<br>10-1832-03<br>10-1833-01<br>10-1833-02 |

*Table 1-7 SFP/XFP Card Compatibility (continued)*

| Card | Compatible SFP/XFP (Cisco Product ID) | Cisco Top Assembly Number (TAN) |
|---|---|---|
| TXP_MR_2.5G (ONS 15454 SONET/SDH)<br>TXPP_MR_2.5G (ONS 15454 SONET/SDH) | 15454-SFP3-1-IR=<br>15454E-SFP-L.1.1=<br>15454-SFP12-4-IR=<br>15454E-SFP-L.4.1=<br>15454-SFP-OC48-IR=<br>15454E-SFP-L.16.1=<br>ONS-SE-2G-S1=<br>15454-SFP-200=<br>15454E-SFP-200=<br>15454-SFP-GEFC-SX=<br>15454E-SFP-GEFC-S=<br>15454-SFP-GE+-LX=<br>15454E-SFP-GE+-LX=<br>ONS-SE-2G-L2=<br>ONS-SE-GE-ZX= | 10-1828-01<br>10-1828-01<br>10-1976-01<br>10-1976-01<br>10-1975-01<br>10-1975-01<br>10-2017-01<br>10-1750-01<br>10-1750-01<br>10-1833-01<br>10-1833-02<br>10-1832-01<br>10-1832-02<br>10-2013-01 |
| TXP_MR_10E (ONS 15454 SONET/SDH) | ONS-XC-10G-S1 | 10-2012-01 |

**Step 3** Plug the LC duplex connector of the fiber into a Cisco-supported SFP or XFP.

**Step 4** If the new SFP or XFP has a latch, close the latch over the cable to secure it.

**Step 5** Plug the cabled SFP or XFP into the card port until it clicks.

To change the payload type of an SFP or XFP (called pluggable port modules [PPMs] in CTC), refer to the "Provision Transponder and Muxponder Cards" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

# 1.10 Power Supply Problems

This section explains problems related to loss of power or power supply low voltage.

**Symptom** Loss of power or low voltage, resulting in a loss of traffic and causing the LCD clock to reset to the default date and time.

**Possible Cause** Loss of power or low voltage.

**Possible Cause** Improperly connected power supply.

**Recommended Action** The ONS 15454 requires a constant source of DC power to properly function. Input power is –48 VDC. Power requirements range from –42 VDC to –57 VDC. A newly installed ONS 15454 that is not properly connected to its power supply does not operate. Power problems can be confined to a specific ONS 15454 or affect several pieces of equipment on the site. A loss of power or low voltage can result in a loss of traffic and causes the LCD clock on the ONS 15454 to default to January 1, 1970, 00:04:15. To reset the clock, in node view click the **Provisioning > General > General** tab and change the Date and Time fields. Complete the "Isolate the Cause of Power Supply Problems" procedure on page 1-56.

**Warning** **Only trained and qualified personnel should be allowed to install, replace, or service this equipment.** Statement 1030

**Warning** **During this procedure, wear grounding wrist straps to avoid ESD damage to the card. Do not directly touch the backplane with your hand or any metal tool, or you could shock yourself.** Statement 94

**Caution** Operations that interrupt power supply or short the power connections to the ONS 15454 are service-affecting.

## Isolate the Cause of Power Supply Problems

**Step 1** If a single ONS 15454 show signs of fluctuating power or power loss:

a. Verify that the –48 VDC #8 power terminals are properly connected to a fuse panel. These power terminals are located on the lower section of the backplane Electrical Interface Assembly (EIA) under the clear plastic cover.

b. Verify that the power cable is #10 AWG and in good condition.

c. Verify that the power cable connections are properly crimped. Stranded #10 AWG does not always crimp properly with Staycon type connectors.

d. Verify that 20-A fuses are used in the fuse panel.

e. Verify that the fuses are not blown.

f. Verify that a rack-ground cable attaches to the frame-ground terminal (FGND) on the right side of the ONS 15454 EIA. Connect this cable to the ground terminal according to local site practice.

g. Verify that the DC power source has enough capacity to carry the power load.

h. If the DC power source is battery-based:

- Check that the output power is high enough. Power requirements range from –40.5 VDC to –57 VDC.
- Check the age of the batteries. Battery performance decreases with age.
- Check for opens and shorts in batteries, which might affect power output.
- If brownouts occur, the power load and fuses might be too high for the battery plant.

**Step 2** If multiple pieces of site equipment show signs of fluctuating power or power loss:

a. Check the uninterruptible power supply (UPS) or rectifiers that supply the equipment. Refer to the UPS manufacturer’s documentation for specific instructions.

b. Check for excessive power drains caused by other equipment, such as generators.

c. Check for excessive power demand on backup power systems or batteries when alternate power sources are used.

# 1.11 Power Up Problems for Node and Cards

This section explains power up problems in a node or cards typically caused an improper power supply.

**Symptom** You are unable to power up a node or the cards in a node.

**Possible Cause** Improper power supply.

**Recommended Action** Refer to power information in the "Hardware Specifications" appendix in the *Cisco ONS 15454 DWDM Reference Manual*.

# 1.12 Network Level (Internode) Problems

The following network-level troubleshooting is discussed in this section:

- Fiber cut detection
- System restart after a fiber cut
- OCHNC circuit creation failure

**Note** In the following paragraphs, any reference to the OPT-BST card also includes the OPT-BST-L card.

Prior to following the procedures in this section, pay attention to the following information.

**Note** The automatic laser shutdown (ALS) function should only be disabled temporarily for installation or maintenance reasons. Activate ALS immediately after maintenance or installation.

The following warning applies to handling unterminated fibers when ALS is disabled:

**Warning** **Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard.** Statement 1056

## 1.12.1 Fiber Cut Detection

A fiber cut is one of the most disruptive faults for a DWDM system because more than one channel is potentially affected. Fault isolation must, therefore, be quick and effective.

In the Multi-Service Transport Platform (MSTP), a dedicated alarm is unambiguously associated with the detection of a fiber cut. The alarm is LOS (OTS or AOTS) and can be raised only by the two cards (OPT-BST and OSC-CSM) that directly interface to the span fiber.

**Note** Any reference to OPT-BST also refers to OPT-BST-L.

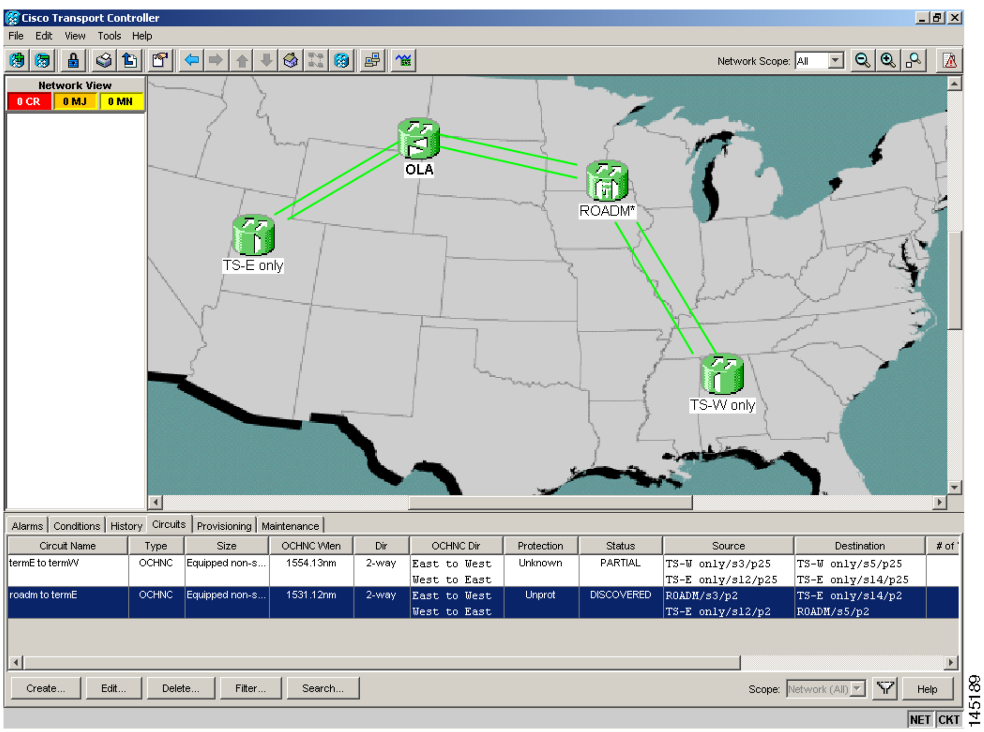
The LOS (OTS or AOTS) alarm is associated with the physical LINE-RX port of the OPT-BST and OSC-CSM cards (in CTC, identified by Port 5 on the OPT-BST and Port 4 on the OSC-CSM). LOS (OTS or AOTS) is the combination of the two alarms LOS-P (OTS or AOTS) (applies to channel payload) and LOS-O (applies to the OC-3 overhead OSC signal).

The simultaneous failure of both the active channel (C- or L-band) and the service channel (1510 nm) coming into the node is evidence of a fiber span issue, whereas either the LOS-P (OTS or AOTS) alarm alone or the LOS-O alarm alone can only be derived from different root causes.

**Note** When a fiber cut occurs, the actual conditions on the affected span (for example, alarms raised on both line directions) are strictly dependent on the network ALS setting. The network automatic laser shutdown (ALS) setting is a function of the ALS mode configured on the appropriate cards in the system (OPT-BST, OSC-CSM, and OSCM).

Different symptoms and scenarios can occur, according to the network ALS settings. Consider the linear network (four nodes) in Figure 1-20 as a reference. The scenarios are presented after the figure.

***Figure 1-20 Linear Network, With No Fiber Cut***




## 1.12.1.1 Scenario A

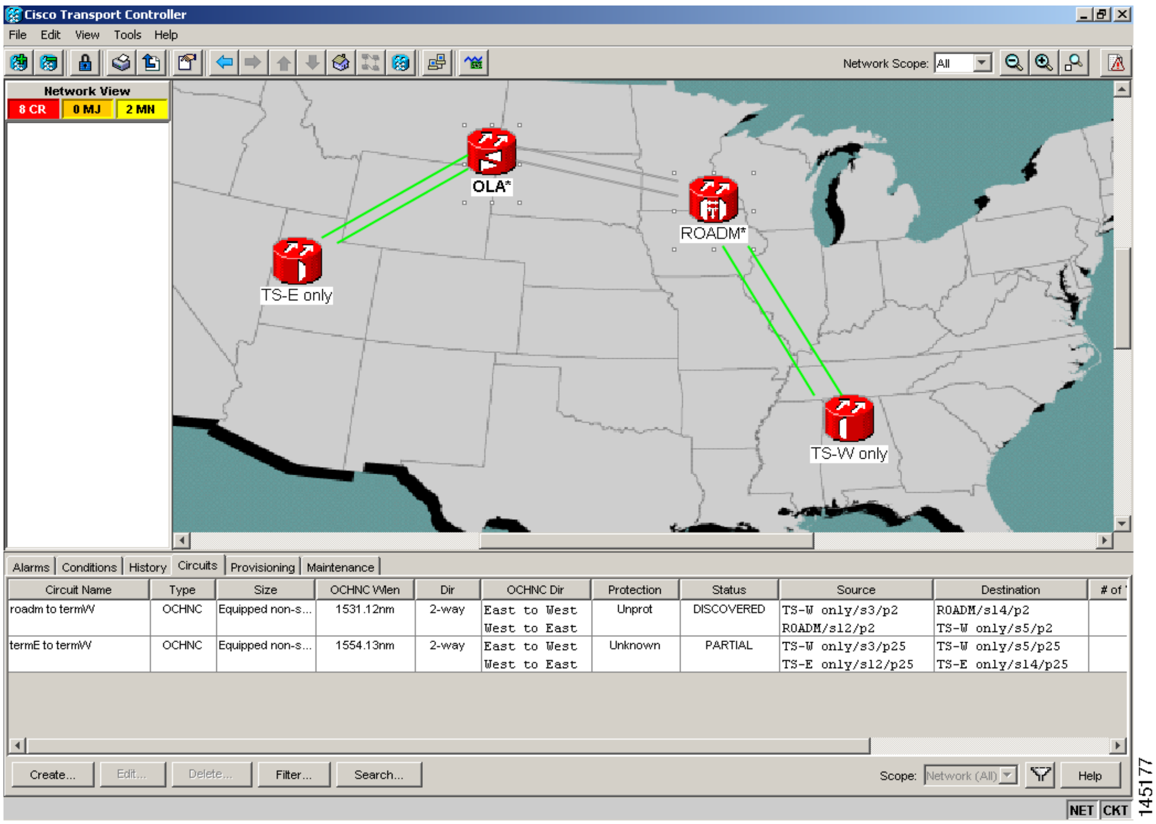
Scenario A has the following conditions:

- ALS Mode = Auto Restart on OPT-BST (+ OSCM) and OSC-CSM
- Fiber cut on the fiber between the OLA-TX node and the ROADM-RX node

The ALS protocol (refer to the “Network Optical Safety—Automatic Laser Shutdown” section in the “Network Reference” chapter of the *Cisco ONS 15454 DWDM Installation and Operation Guide*) is activated in the event of a fiber cut, resulting in the shutdown of optical power on both of the fibers belonging to the affected span, even if only one of the two fibers is cut.

The final fault condition of the network is shown in Figure 1-21.

***Figure 1-21 Fiber Cut with ALS MODE = Auto Restart***




In network view, both of the lines representing the span were formerly green and have now changed to gray. Notice also that the status of all the OCHNC circuits on the broken span have changed from Discovered to Partial.

In node view, the alarm panel of the two nodes (reconfigurable optical add/drop multiplexing [ROADM] and optical line amplification [OLA] in the example) show the LOS (AOTS) alarm on Port 4 of the OSC-CSM (see Figure 1-22) and the LOS (OTS) on Port 5 of the OPT-BST (see Figure 1-23).

*Figure 1-22 LOS Indication on the ROADM Node OSC-CSM*

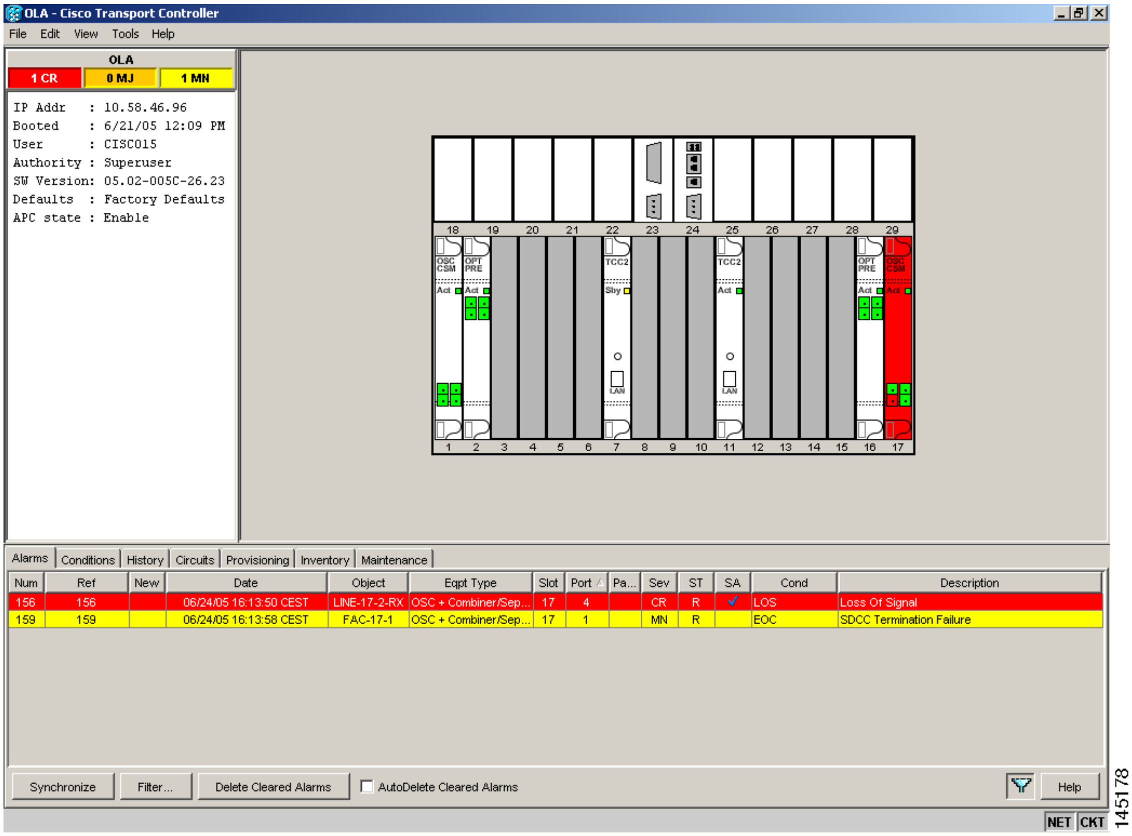
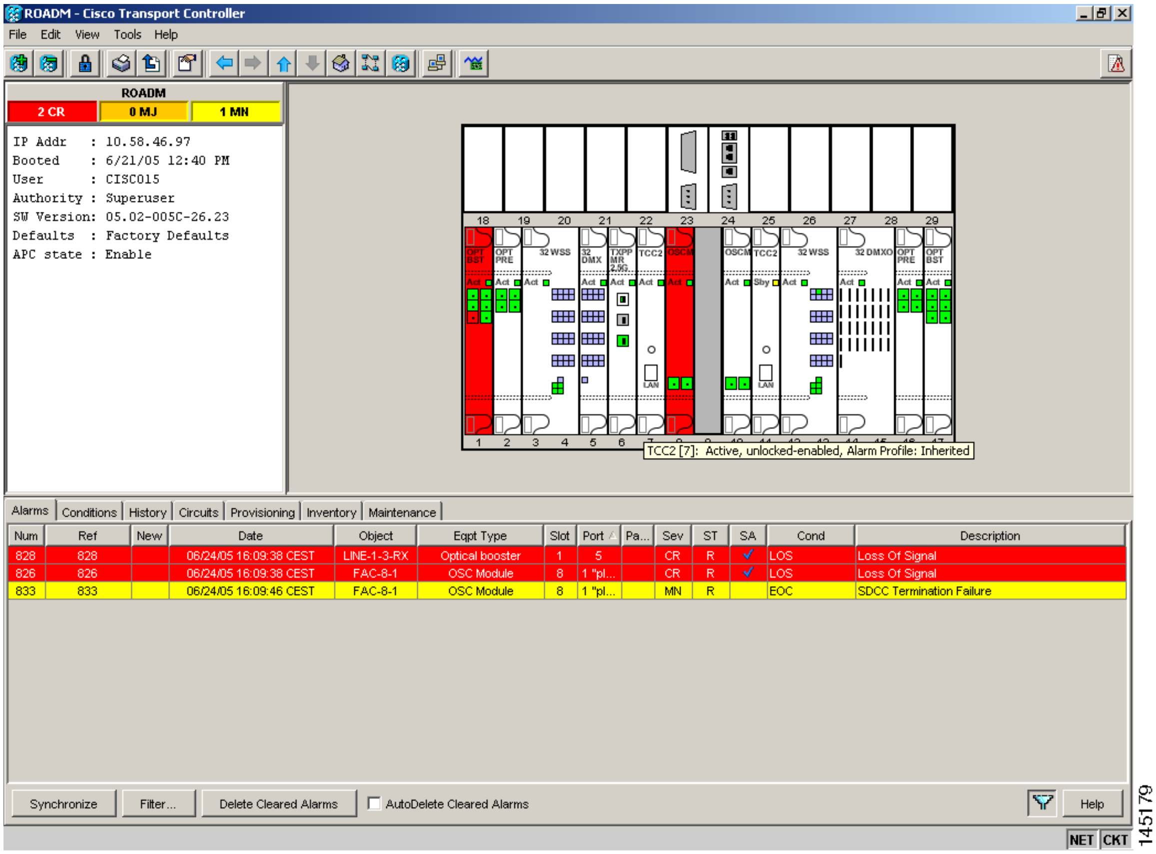


*Figure 1-23 LOS Indication on the OLA Node OPT-BST*



**Note** An EOC condition is always present on both nodes, because the optical service channel (OSC) link (to which the communication channel applies) is down.

**Note** For the OSCM card, only an LOS (OC-3) alarm is present at the SONET layer (Port 1).

### 1.12.1.2 Scenario B

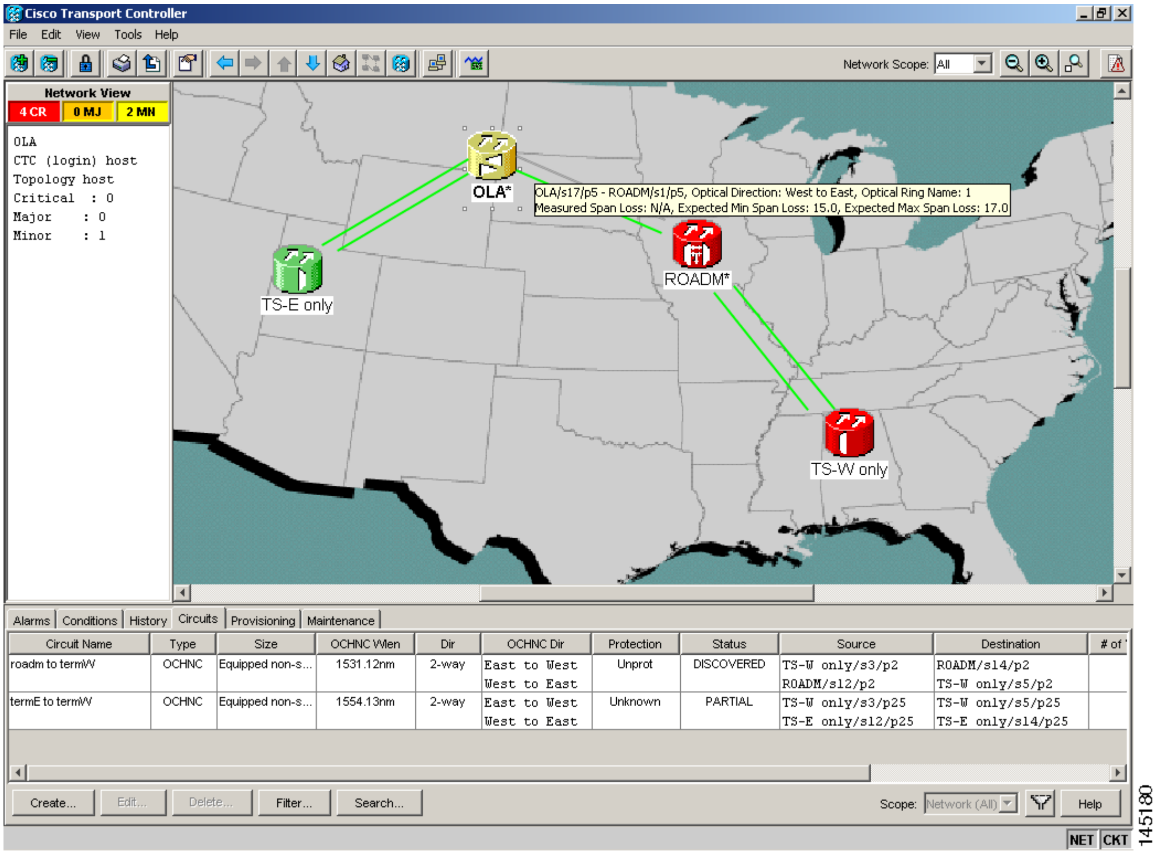
Scenario B has the following conditions:

- ALS Mode = DISABLE on OPT-BST (+ OSCM) and OSC-CSM
- Fiber cut on the fiber between the OLA-TX node and the ROADM-RX node

Because the ALS protocol is disabled, the signal is lost on only the affected fiber (power is not shut down on both fibers).

The LOS (OTS or AOTS) alarm is raised by the ROADM-RX node that was receiving the signal coming from the broken fiber. The final fault condition of the network is shown in Figure 1-24.

*Figure 1-24 Network View Fault Condition for Fiber Cut with ALS Mode Disabled*




In network view (Figure 1-24), only the actual affected fiber becomes gray, whereas the traffic (and OSC signal as well) on the good fiber is active and fault identification is immediate.

In node views (Figure 1-25 and Figure 1-26), the alarm panel of the receiving node (ROADM in this example) reports the LOS (OTS), while the transmitting node (OLA) reports only an EOC alarm.

*Figure 1-25 ROADM Node View with Fault Condition for ALS MODE Disabled*

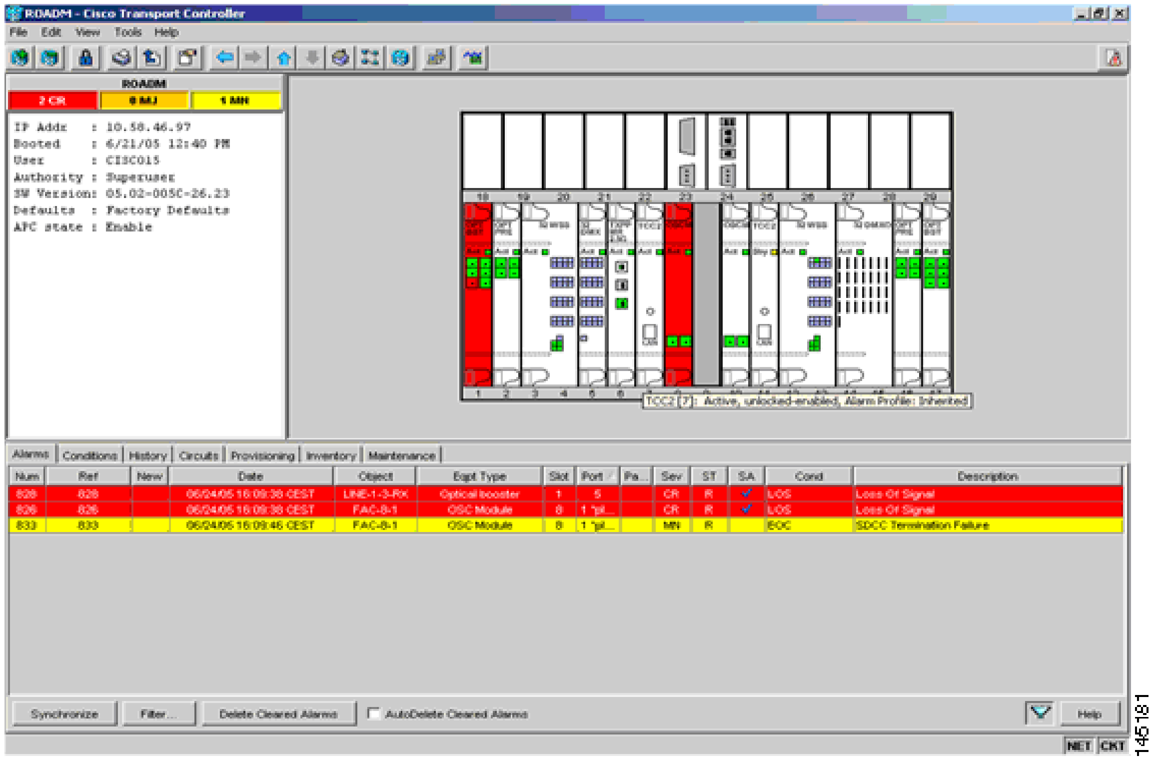
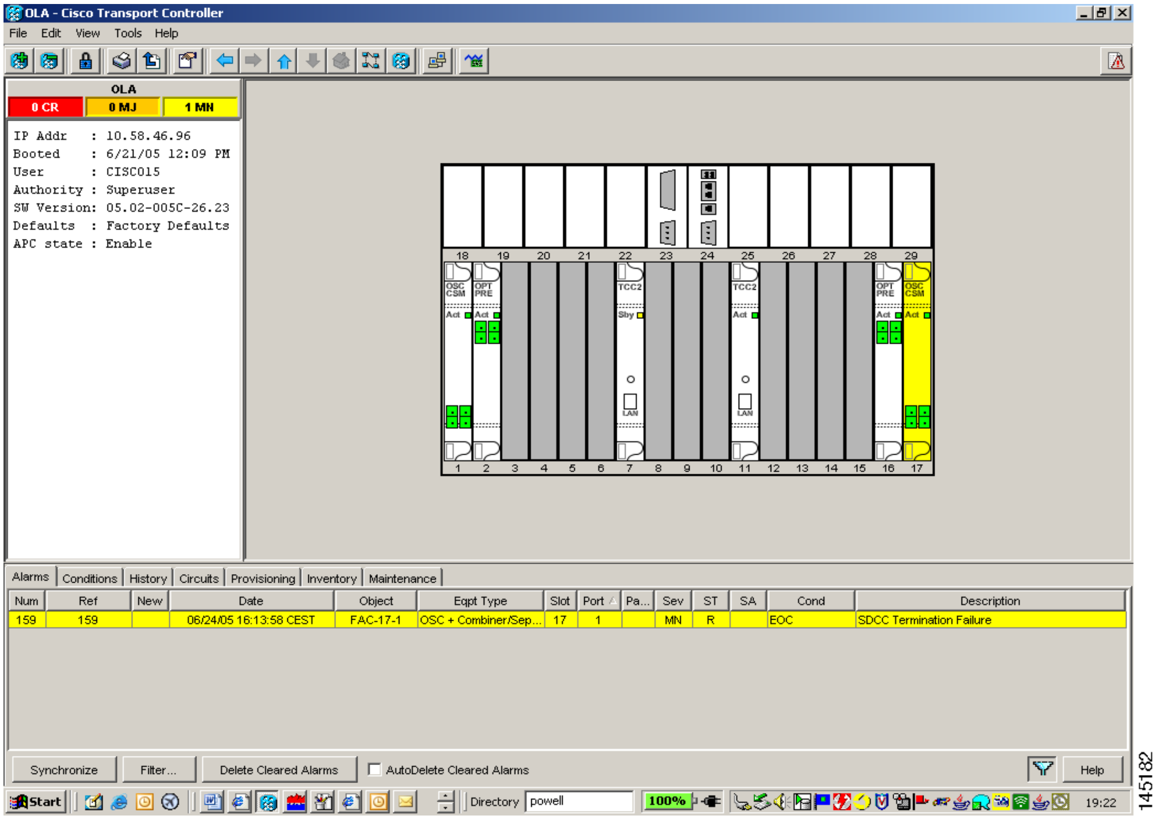


*Figure 1-26 OLA Node View with Fault Condition for ALS MODE Disabled*




In order to troubleshoot and eventually fix a fiber cut, follow the "Fix a Fiber Cut" procedure on page 1-64. The basic assumption is that the MSTP system was already installed and working correctly before the alarm condition occurred. For first installation or restart from a fiber cut, refer to 1.12.2 System Restart after a Fiber Cut, page 1-65.

## Fix a Fiber Cut

**Warning** **When the network ALS setting is DISABLE, optical power is still present at the damaged fiber. Before fixing the span, it is highly recommended that you shut down the amplifier and the OSC laser upstream of the fiber cut.**

**Step 1** Isolate the span affected by the fiber cut.

**a.** Go to CTC network view.

**b.** Identify the span connection that is gray.

**Step 2** Verify the alarm is valid, then perform the following steps for both DWDM nodes connected to the span identified in Step 1.

**a.** Double-click the card directly connected to the span (either the OPT-BST or the OSC-CSM).

**b.** Click the Alarms tab and verify that a LOS condition is present on the LINE-RX port. If the alarm is correctly reported, move to Step 3. If not, close the CTC application, delete the CTC cache and reopen the CTC connection.

c. Click the **Synchronize** button on the bottom left of the window.

> **Note** If the "gray" condition of the span persists, log into the Technical Support website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) to report a service-affecting problem.

**Step 3** If the network ALS setting on the DWDM nodes that you are troubleshooting is Auto Restart, continue with Step 4; if the network ALS setting is DISABLE, go to Step 5.

> **Note** The network ALS setting is a function of the ALS mode configured on the appropriate cards in the system (OPT-BST, OSC-CSM, and OSCM).

**Step 4** Isolate the fiber affected by the fiber cut. For the two fibers belonging to the span, identify the fiber belonging to the west-to-east (W–E) line direction:

a. Go into the upstream node and identify the OSCM or OSC-CSM card managing the OSC termination referring to the faulty span.

b. Double-click the card, then click the **Maintenance Panel** tab.

c. Force the OSC-TX laser to be active by setting the ALS Mode to **DISABLE**.

d. Go into the downstream node and verify if OSC power is being received.

- If a pair of OPT-BST + OSCM cards terminate the OSC connection, click the **Provisioning > Optical Line > Parameters** tabs, then verify that there is power for OSC-TX (port 4).
- If an OSC-CSM terminates the OSC connection, click the **Provisioning > Optical Line > Parameters** tabs, then verify that there is power for OSC-RX (port 6).

e. If no power is detected and the LOS (OC-3) alarm persists, go to Step 5; otherwise, the fiber under test is good. In this case, go to Step f to check the other fiber.

f. Repeat Steps a to d for the other fiber to verify that it is at fault.

**Step 5** Repair the identified broken fiber to restore the internode link.

## 1.12.2 System Restart after a Fiber Cut

When the network ALS setting is Auto Restart, the system automatically restarts after a fiber cut occurs. The MSTP system restart after a fiber cut is a fully automatic process regulated by a chronological sequence of steps including the OSC link built-in amplifiers restart and amplifier power control (APC) regulation.

The successful completion of system restart is strictly related to possible changes of the insertion loss value of the repaired span. A change in insertion loss is dependent on many factors, including the process of physically repairing the fiber, a change in fiber length after repair, and so on.

Four different scenarios related to span loss are presented in this section:

1. Span loss increased:

- Span loss change > 5 dBm
- OSC power value on the receiver < –42 dBm

2. Span loss increased:

- Span loss change > 5 dBm
- OSC power value on the receiver > –42 dBm

3. Span loss increased: 3 dBm < span loss change < 5 dBm
4. Span loss increased: span loss change < 3 dBm

**Note** It is also possible that span loss decreased, but this is unlikely. This condition does not prevent the MSTP system automatic restart process, but can lead (potentially) to issues downstream of the repaired span, for example, a Power Overload condition on the OSC receiver or on the Trunk-RX port of a TXP or MXP card.

These conditions are identified by specific alarms (see the "HI-RX-POWER" section of Chapter 2, "Alarm Troubleshooting" of the *DWDM Alarm and Troubleshooting Guide*).

The symptoms of the possible span loss scenarios (except for span loss decrease) are described in the following paragraphs. Refer to the linear network in Figure 1-20 during the discussion of the scenarios.

The basic assumption is that the network ALS feature (for feature details, refer to the "Network Optical Safety—Automatic Laser Shutdown" section in the *Cisco ONS 15454 DWDM Installation and Operation Guide*) is active (ALS Mode = Auto Restart on the OPT-BST [+ OSCM] and OSC-CSM). Given this assumption, the starting condition is as shown in Figure 1-21.

The system behavior when the network ALS Mode is DISABLE is a subcase that requires a manual restart after repairing a single fiber in only one line direction.

**Note** The network ALS feature is a function of the ALS Mode settings of the OPT-BST, OSCM, and OSC-CSM cards. For the network ALS Mode to be disabled, each of these cards must have its ALS Mode set to DISABLE.

### 1.12.2.1 Scenario 1: Span Loss Change > 5 dBm and OSC Power Value on the Receiver < –42 dBm

The following conditions are present in Scenario 1:

- In network view, both of the lines representing the span remain gray as long as the status of the OCHNC circuits relating to the repaired span remain Partial.
- In node view, the alarm panels of the two nodes (ROADM and OLA in this example) show the LOS (OTS or AOTS) condition on the LINE-RX port of the OPT-BST or OSC-CSM.
- An EOC condition is always present on both nodes because the OSC optical link is down due to an incoming power level lower than the optical sensitivity limit (–42 dBm). The system condition remains unchanged as illustrated in Figure 1-21.
- Every 100 seconds, the ALS protocol turns up the OSC TX laser in a pulse mode (pulse duration = 2 seconds), but the excessive loss on the span prevents the OSC link from synchronizing, and the MSTP system remains unoperational.

**Note** During the attempt to restart, a valid power value is reported by the OSC transmit card (in the example, the OSC-CSM in the OLA node), but on the OSC receive card (the OSCM in the ROADM node), the alarm condition persists.

### Corrective Action for Scenario 1

**Step 1** Follow these steps to verify the alarms for both DWDM nodes connected to the repaired span:

a. Double-click the card directly connected to the span (either the OPT-BST or the OSC-CSM).

b. Click the **Alarms** tab.

c. Verify that a LOS condition is present on the LINE-RX port.

d. Click the **Synchronize** button on the bottom left of the window.

e. If the alarm is correctly reported, move to Step 2. If not, close the CTC application and delete the CTC cache. Then reopen the CTC connection, and repeat Step 1.

**Note** If the gray color persists on the span, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) in order to report a service-affecting problem.

**Step 2** Isolate the fiber affected by the excessive insertion loss. For the two fibers belonging to the span, identify the one for the W–E line direction.

a. Go into the upstream node and identify the OSCM or OSC-CSM card that manages the OSC termination for the faulty span.

b. Double-click the card, then click the **Maintenance** tab.

c. Force the OSC-TX laser active by setting ALS Mode to **DISABLE**.

d. Go into the downstream node and verify the OSC Power level received.

- If a pair of OPT-BST + OSCM cards terminate the OSC connection, click the **Provisioning > Optical Line > Parameters** tabs, then verify that there is power for OSC-TX (Port 4).
- If an OSC-CSM terminates the OSC connection, click the **Provisioning > Optical Line > Parameters** tabs, then verify that there is power for OSC-RX (Port 6).
- If no power is detected and the LOS (OC-3) alarm persists, the faulty fiber has been identified, so go to Step 3.

e. If a power value greater than –42 dBm is detected, the fiber under test has been properly repaired. However, it is recommended that you check the new fiber Insertion Loss value.

- In node view, click the **Maintenance > DWDM > WDM Span Check** tabs.
- Retrieve the new value of fiber Insertion Loss of the repaired span.

**Note** The new value of the fiber Insertion Loss of this fiber after restoration must be less than 5 dB higher than the previous Insertion Loss value. If possible, try to recover the original value by making a better fiber splice. If this is not possible, use the new value (must be less than 5 dB higher than the previous value) and rerun Cisco MetroPlanner to revalidate the new condition.

**Step 3** For the two fibers belonging to the repaired span, identify one for the east to west (E–W) line direction.

**Step 4** Repeat the procedure starting at Step 2 for the E–W direction.

**Step 5** Clean the LINE-RX and LINE-TX connectors for the failing fiber identified in the previous steps.

**Step 6** If the problem persists, continue with Step 7. Otherwise, the corrective action is finished.

**Step 7** Repair the failing fiber again until the expected OSC link is reestablished.

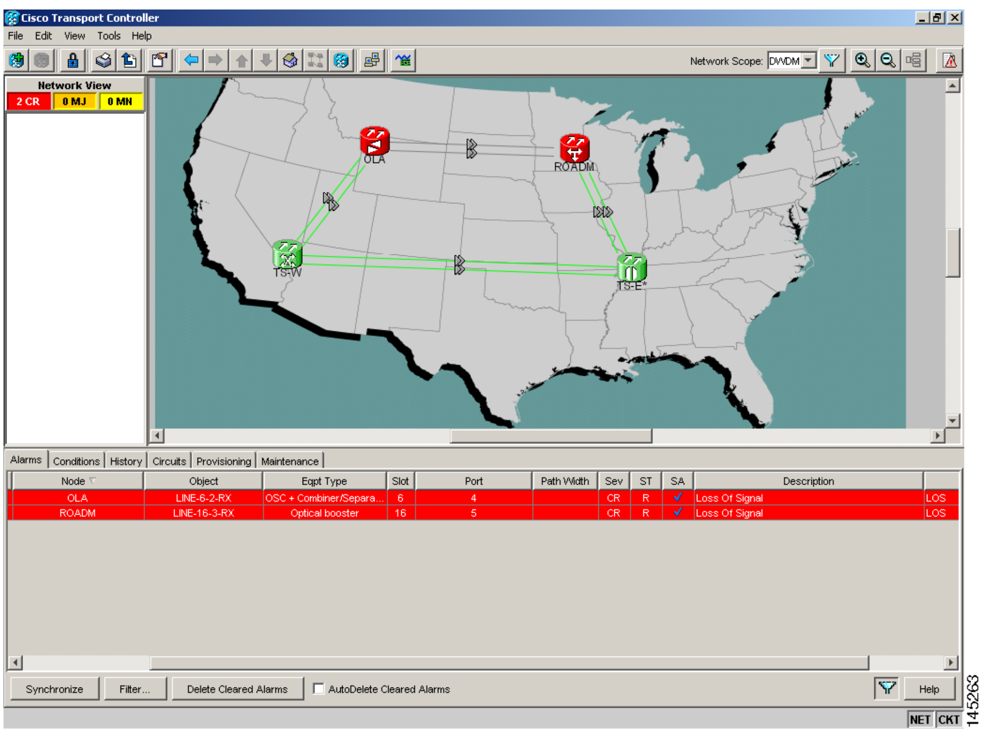
**Note** If the OSC link cannot be reestablished (either by splicing or replacing the fiber), and the new value of Span Loss cannot be modified, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

### 1.12.2.2 Scenario 2: Span Loss Change > 5 dBm and OSC Power Value on the Receiver > –42 dBm

In network view, both of the lines representing the span change to green; however, the status of the OCHNC circuits relating to the repaired span remains Partial, instead of Complete (due to the fiber cut).

This change is due to the fact the physical optical power value received by the OSC transceiver is above the sensitivity limit (–42 dBm) and consequently, the OSC optical link can be rebuilt, allowing the restoration of the Section DCC (SDCC) or multiplex section DCC (MS-DCC). The network view for this condition is shown in Figure 1-27.

*Figure 1-27 Network View for Span Loss Change > 5 dBm and OSC Power Value at Receiver > –42 dBm*




In node view, the EOC condition is cleared, but the alarm panels of the two nodes (ROADM and OLA in the example) continue to show LOS (OTS or AOTS) on the LINE-RX port of the OPT-BST or OSC-CSM.

The network ALS protocol keeps the OCHNC traffic down along the span because the new losses of the restored span can potentially affect the optical validation of the network design done by Cisco MetroPlanner.

### Corrective Action for Scenario 2

**Step 1** Verify the validity of the alarm. For both DWDM nodes connected to the repaired span:

a. Double-click the card directly connected with the span (either the OPT-BST or the OSC-CSM).

b. Click **Alarms**

c. Click the **Synchronize** button on the bottom left of the window.

d. Verify that a LOS condition is present on the LINE-RX port.

e. If the alarm is correctly reported, move to Step 3. If not, close the CTC application, delete the CTC cache, and open the CTC connection again. Then, go back to substep a.

> **Note** If the "gray condition" of the span persists, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

**Step 2** Repair the fiber.

**Step 3** Repair the fiber then measure the new Span Loss value.

a. In the node view of both nodes for the span, click the **Maintenance > DWDM > WDM Span Chec**k tabs.

b. Click **Retrieve Span Loss Values** to retrieve the latest loss data.

> **Note** The two values retrieved at each node level (west side and east side) refer to the two fibers coming into the node from the adjacent nodes, so they apply to different spans. To complete the measurement in Step 3, the appropriate values must be taken into account.

**Step 4** Compare the span measurements of Step 3 with the span losses values used during the network design with Cisco MetroPlanner.

**Step 5** For the two fibers belonging to the repaired span, identify the fiber for the W–E line direction and calculate the insertion loss variation. If the span loss change is greater than 3 dBm, continue with Step 6. If not, go to Step 9.

**Step 6** Clean the LINE-RX and LINE-TX connectors on the DWDM cards managing the fiber of the repaired span. If the problem persists, continue with Step 7.

**Step 7** If the alarm condition is still reported, it is recommended that the fiber be repaired again to reestablish the expected span loss value. If this is not possible and the new value of span loss cannot be modified, go to Step 8 to fix the system faulty condition.

**Step 8** Follow the signal flow into the network starting from the repaired fiber:

a. In the downstream node, identify the OPT-BST or OSC-CSM card that manages OSC and CHS detection.

b. In card view, click the **Provisioning > Optical Line > Optic Thresholds** tabs.

c. Click the **Alarms** radio button, then click **Refresh**.

d. Decrease the current OSC and CHS Fail Low thresholds by the same amount of the span loss change calculated in Step 5.

If an OPT-BST is present:

– CHS Fail Low threshold refers to Port 2.

- OSC Fail Low threshold refers to Port 4.

If an OSC-CSM is present:

- CHS Fail Low threshold refers to Port 3.
- OSC Fail Low threshold refers to Port 6.

**Step 9** For the two fibers belonging to the repaired span, identify the fiber for the east to west (E–W) line direction.

**Step 10** Repeat the procedure from Step 5 to Step 8 for the E–W direction.

**Step 11** If the LOS alarm has cleared, the system has restarted properly. However, because a span loss value significantly different is now present, we highly recommended that you complete the following procedure:

a. Go back to the Cisco MetroPlanner tool and open the network design configuration file.

b. Select **Installation Mode** to freeze the node layout and amplifier positioning.

c. Change the span value, inserting the new span loss that was measured in Step 3.

d. Run the Cisco MetroPlanner algorithm to validate the new design.

e. If the optical result indications (power, optical signal-to-noise ratio [OSNR], chromatic dispersion [CD], and so on) are all green, the repair procedure is complete. If not, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

If the LOS alarm is still present, continue with Step 12.

**Step 12** Go back to the card where the LOS alarm is active, and set the Optics Thresholds (see Step 8b) to the lowest value allowed.

If an OPT-BST is present:

- CHS Fail Low threshold must to be set to –30 dBm.
- OSC Fail Low threshold must to be set to –42 dBm.

If an OSC-CSM is present:

- CHS Fail Low threshold must to be set to –30 dBm.
- OSC Fail Low threshold must to be set to –40 dBm.

**Note** If the LOS alarm is still present, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

**Step 13** If the LOS alarm is has cleared, the system has restarted properly, but because a Span Loss value significantly different from the design is now present, we highly recommend that you complete the procedure described in Step 11.

### 1.12.2.3 Scenario 3: 3 dBm < Span Loss Change < 5 dBm

In network view, both the lines representing the span change to green after the rebuild of the OSC optical link and consequent restoration of the SDCC or MS-DCC. The EOC condition and the LOS alarms are cleared.

The network ALS protocol successfully restarts the amplifiers, which enables the OCHNC traffic restoration along the span.

The reactivation of the OCHNC circuits relating to the repaired span (the status changes from Partial to Complete) can lead to several final conditions that depend on the network topology and node layout.

The rebuilding of circuits automatically triggers the APC check mechanism (for details, refer to the "Automatic Power Control" section in the "Network Reference" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*). The APC check mechanism impacts the optical gain of the amplifiers (primarily the OPT-PRE card) and the VOA express attenuation for the optical add/drop multiplexing (OADM) cards. The APC application acts on the appropriate cards downstream of the repaired span (for each line direction), and attempts to compensate for the introduction of excess loss.

Because the loss increase exceeds the maximum variation (+/–3 dBm) for which APC is allowed to compensate, an APC-CORRECTION-SKIPPED condition is raised by the first node along the flow detecting the event. The condition panel of the impacted node (the ROADM, in this example) reports the APC-CORRECTION-SKIPPED condition and indicates the port or card to which it applies.

To correct Scenario 3:

**Step 1** Verify the alarm validity. For both DWDM nodes connected to the repaired span:

a. Double-click the card reporting the issue.

b. Click **Conditions**.

c. Click **Retrieve** and verify that an APC-CORRECTION-SKIPPED condition is present on an aggregate port.

d. If the alarm is correctly reported, go to Step 2. If not, close the CTC application, delete the CTC cache, and open the CTC connection again. Then, go to substep a.

**Note** If the discrepancy persists, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

**Step 2** Repair the fiber and measure the new Span Loss value after the fiber has been repaired.

a. In the node view of both nodes of the span, click the **Maintenance > DWDM > WDM Span Check** tabs.

b. Click **Retrieve Span Loss Values** to retrieve the latest loss data.

**Note** The two values retrieved at each node level (west side and east side) refer to the two fibers coming into the node from the adjacent nodes, so they apply to different spans. To complete the measurement in Step 3, the appropriate values must be taken into account.

**Step 3** Compare the span measurements of the previous step with the Span Losses values used during the network design with Cisco MetroPlanner.

**Step 4** For the two fibers belonging to the repaired span, identify the one for the W–E line direction. If the span loss change is greater than 3 dB, continue with Step 5. If not, go to Step 8.

**Step 5** Clean the LINE-RX and LINE-TX connectors of the DWDM cards that manage the fiber of the repaired span. If the problem persists, continue with Step 6. Otherwise, you are finished with the corrective action.

**Step 6** If the alarm condition is still reported, we recommend that you again repair the fiber to reestablish the expected span loss value. If this is not possible and the new value of Span Loss cannot be modified, move to Step 7 to fix the system faulty condition.

**Step 7** Follow the signal flow into the network starting from the repaired fiber.

**a.** In the first downstream node of the restored span (W–E), check whether a DWDM card reports the APC-CORRECTION-SKIPPED condition on a port applying to the W–E direction (see Step 2 for directions to do this).

**b.** If the answer is yes, retrieve the following values according to the card type.

- For OPT-PRE or OPT-BST cards: Click the **Provisioning > Optical Ampli. Line > Gain Setpoint** tabs
- For AD-xC-xx.x or AD-xB-xx.x cards: Click the **Provisioning > Optical Line > VOA Attenuation Reference** tabs.
- Go to Step 7f.

**c.** If the answer is no, go to Step 7d.

**d.** Move along the downstream nodes until a card with the APC-CORRECTION-SKIPPED condition for a W–E port is detected.

**e.** From that card, retrieve parameters according to Step 7b.

**f.** In the first downstream node of the restored span, go to the Circuits tab and identify all the OCHNC circuits passing through the repaired span.

**g.** Edit all the OCHNC circuits identified in Step 7f:

- Click the **Tools > Circuits > Set Circuit State** tabs.
- Change the Target Circuit Admin. State to **OOS DSBLD** (or, **locked, disabled**) and click **Apply**.

**h.** Go to the DWDM card for which the Gain or VOA Attenuation values were retrieved (the card can be either the one in substep Step 7b or Step 7e) and verify that the administrative state of the alarmed port is now OOS (locked).

**i.** If the alarmed port is not OOS (locked), go to the card view, click **Circuits**, and identify the remaining OCHNC circuits that are still active. Put the circuits in **OOS DSBLD** (or, **locked, disabled**) in order to reach the OOS (locked) administrative state on the alarmed port.

**j.** Wait for three minutes, then switch the administrative state of only one of the circuits selected in Step 7f and Step 7i back to **IS**, (unlocked).

**k.** After the network completes the restart phase, go to the formerly alarmed card and verify that the APC-CORRECTION-SKIPPED condition has cleared and a new Gain Setpoint or VOA Attenuation Reference (compare with Step 7b) has been provisioned.

**Note** The total variation of the above Gain Setpoint or VOA Attenuation Reference setpoint must be within approximately +/– 1 dBm of the Span Loss value measured in Step 2.

**l.** If the APC-CORRECTION-SKIPPED condition has cleared and the system has restarted properly, we highly recommend that you complete the following procedure due to the fact that a Span Loss value that is significantly different than the design is now present.

- Go back to the Cisco MetroPlanner tool and open the network design configuration file.
- Select Installation Mode to freeze the node layout and amplifier positioning.
- Change the span value, inserting the new Span Loss measured in Step 2.

- Run the Cisco MetroPlanner algorithm to validate the new design.
- If the optical result indications (power, OSNR, CD, and so on) are all green, the repair procedure is complete. If not, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

**Note** If the APC condition persists, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

**Step 8** For the two fibers belonging to the repaired span, identify the fiber for to the east to west (E–W) line direction.

**Step 9** Repeat the procedures from Step 5 to Step 7 for the E–W direction.

### 1.12.2.4 Scenario 4: Span Loss Change < 3 dB

In network view, both the lines that represent the span turn green after the rebuilding of the OSC optical link and consequent restoration of the SDCC or MS-DCC. The EOC condition and LOS alarms are cleared.

The network ALS protocol successfully completes the amplifier restart to enable OCHNC traffic restoration along the span.

The rebuilding of circuits automatically triggers the APC check mechanism (for details, refer to the "Automatic Power Control" section in the "Network Reference" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*). The APC check mechanism affects the optical gain of the amplifiers (primarily the OPT-PRE) and the VOA express attenuation for the OADM cards. The APC application acts on the "suitable" cards downstream of the repaired span (for each line direction), and attempts to compensate for the introduction of excess loss.

The APC operation is successfully completed if enough margin during the Cisco MetroPlanner network design phase has been taken into account. If not, the adjustment done by the APC application overcomes the range setting for a specific optical parameter in the first appropriate card along the flow and an APC-OUT-OF-RANGE condition is raised. The condition panel of the impacted node (the ROADM in the example) reports the APC-OUT-OF-RANGE condition and indicates the port or card to which it applies.

To correct Scenario 4:

**Step 1** Verify the alarm validity. For both DWDM nodes on the repaired span:

**a.** Double-click the card reporting the issue.

**b.** Click **Conditions**.

**c.** Click **Retrieve** and verify that an APC-OUT-OF-RANGE condition is present on an aggregate port.

**d.** If the alarm is correctly reported, go to Step 2. If not, close the CTC application, delete the CTC cache, and open the CTC connection again. Then, go to Step 1.

**Note** If the discrepancy persists, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

**Step 2** Repair the fiber and measure the new Span Loss value.

a. In the node view of both nodes for to the span, click the **Maintenance > DWDM > WDM Span Check** tabs.

b. Click **Retrieve Span Loss Values** to retrieve the latest loss data.

**Note** The two values retrieved at each node level (west side and east side) refer to the two fibers coming into the node from the adjacent nodes, so they apply to different spans. To complete the measurement in Step 3, the appropriate values must be taken into account.

**Step 3** Compare the span measurements done in Step 2 with the Span Losses values used during the network design with Cisco MetroPlanner.

**Step 4** For the two fibers belonging to the repaired span, identify the one for the W–E line direction.

- If the span loss change is greater than 1 dBm, continue with Step 5.
- If the span loss change is 1 dBm or less, move to Step 8.

**Step 5** Clean the LINE-RX and LINE-TX connectors of the DWDM cards that manage the fiber of the repaired span.

**Step 6** If the problem persists, continue with the next step. if not, you have finished the corrective action.

**Step 7** if the span loss change is greater than 1 dBm and the APC-OUT-OF-RANGE condition still exists, it is mandatory to again repair the fibers to reestablish the expected span loss value.

**Note** If it is not possible to reduce the span loss change to under 1 dBm through fiber repair, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem

**Step 8** For the two fibers belonging to the repaired span, identify the fiber for the east to west (E–W) line direction.

**Step 9** Repeat the procedure from Step 5 to Step 7 for the E–W direction.

## 1.12.3 OCHNC Circuits Creation Failure

OCHNC circuit creation is managed by the Cisco Wavelength Path Provisioning (WPP) network application. The WPP application helps prevent errors during new circuit activation (if the wavelength is already allocated in the path between source and destination) and also guarantees an appropriate time interval between one circuit activation and the next to enable proper amplifier gain regulation by APC.

WPP uses the network topology information carried by the OSC link among different nodes to identify the routing path of the optical wavelength (OCHNC circuits) from the source node to the destination node. WPP also enables the card ports of the OCHNC circuits by changing the administrative state from the default Out Of Service (OOS, or locked) state to the final In Service (IS), or unlocked state.

### 1.12.3.1 Prerequisites for Successful OCHNC Circuit Creation

The prerequisite conditions for successfully completed circuit creation are:

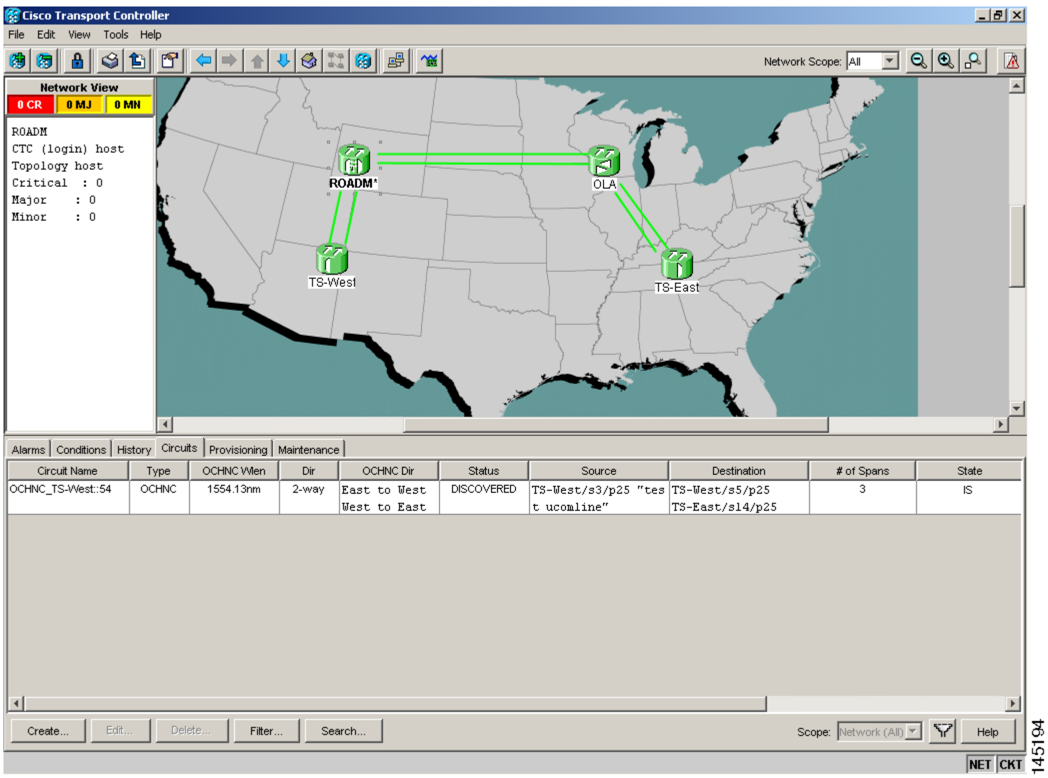
1. Internode: OSC link active among all DWDM nodes involved

2. Internode: APC enabled (or alternatively manually disabled by the user)
3. Intranode: Logical connections among cards created and provisioned on every node of the network (ANS completed)

OCHNC circuit creation is successfully completed when the CTC circuit table reports the situation shown in Figure 1-28.

- Circuit Status has turned to DISCOVERED.
- The # of spans field shows the correct number of hops among different nodes that the OCHNC circuit passes through to reach the final destination.
- Circuit State reports IS (unlocked).

***Figure 1-28 OCHNC Circuit Successfully Completed***

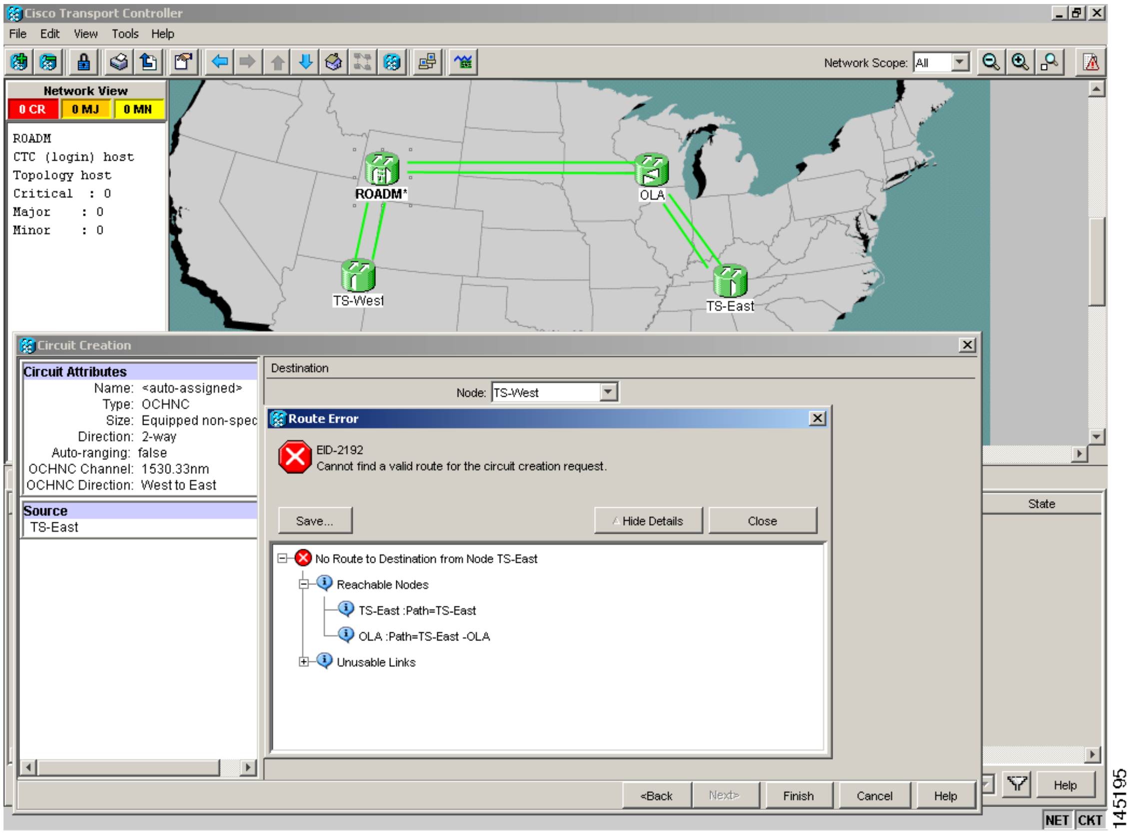



## 1.12.3.2 Conditions for OCHNC Circuit Creation Failure

If the OCHNC circuit creation fails**,** you will see one of the following conditions.

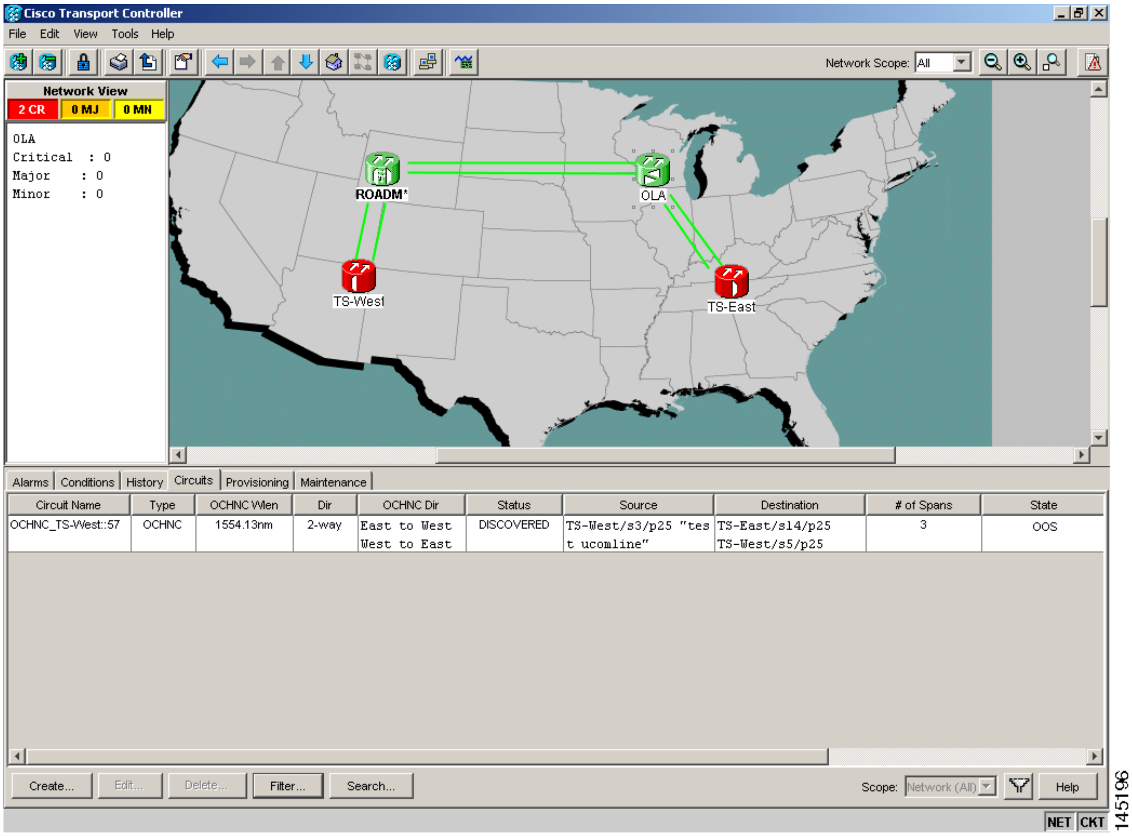
- If the WPP wizard cannot complete the circuit creation procedure, CTC displays the error message shown in Figure 1-29. In the message, click **Details** to see the partial connections that WPP can set up.Start troubleshooting the problem in the first node unreachable along the path.

*Figure 1-29 Partial Circuit*




- The circuit is successfully created and reported under the Circuits tab, the Status field turns to DISCOVERED, but the Circuit State is OOS (locked). The condition is shown in Figure 1-30.

*Figure 1-30 Circuit Discovered, State OSS*




- The OCHNC circuit is shown under the Circuits tab, but the Status field reports PARTIAL. This applies to a circuit successfully built-up when the network falls into scenarios 1. (OSC link fail) or 2. (APC disabled), described in "1.12.3.3 Scenarios for OCHNC Circuit Creation Failure" section on page 1-77.

The root cause identification for the preceding conditions are found in the prerequisite conditions described in "1.12.3.1 Prerequisites for Successful OCHNC Circuit Creation" section on page 1-74.

### 1.12.3.3 Scenarios for OCHNC Circuit Creation Failure

The most common scenarios for failure to create an OCHNC circuit are:

1. One (or more) of the span OSC links involving the OCHNC circuit has not been properly established. The WPP application prevents the creation of any circuit passing through the failing span. Prerequisite condition 1. of "1.12.3.1 Prerequisites for Successful OCHNC Circuit Creation" section on page 1-74 has not been met.
2. The APC application is internally disabled due to the presence of a Critical alarm somewhere in the network. As a consequence, no reliable information about the number of active channels can be shared among the nodes and the creation of any further OCHNC circuit is prevented until the faulty condition is fixed. Prerequisite condition 2. of "1.12.3.1 Prerequisites for Successful OCHNC Circuit Creation" section on page 1-74 has not been met.

3. One (or more) of the intranode connections between two DWDM cards associated with the circuit have not been properly created. Prerequisite condition 3. of 1.12.3.1 Prerequisites for Successful OCHNC Circuit Creation has not been met.
4. One (or more) of the intranode connections between two DWDM cards associated with the circuit has not been properly provisioned. This happens when ANS application has not run in one of the involved nodes or at least one port status after the ANS run has not been successfully configured (Fail-Out of Range alarm on the ANS panel). Prerequisite condition 3. of 1.12.3.1 Prerequisites for Successful OCHNC Circuit Creation has not been met.

To troubleshoot and eventually fix issues related to the faulty OCHNC circuit creation shown in Figure 1-29, the following procedure must be performed.

**Step 1** Verify OSC connectivity:

a. Go to network view and identify the MSTP nodes to which the OCHNC circuit applies.
b. Verify that all the OSC links connecting the MSTP nodes along the circuit path, from the source node to the destination node, are active (green line).

**Note** Bidirectional circuits have two possible nodes, depending on the line direction being considered.

Complete one of the following actions depending on OSC connectivity:

- If the OSC link is down, focus on the affected span and troubleshoot the issue (see 1.12.2 System Restart after a Fiber Cut, page 1-65).

**Note** If necessary, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

- If the OSC link is not down, continue with Step 2.

**Step 2** Verify APC status:

a. Go to node view on the MSTP node that is the source node for the circuit.
b. In the General Info box on the left, check the APC state (last row).
  - If the APC state is DISABLE - INTERNAL, choose the appropriate troubleshooting procedure according to Chapter 2, "Alarm Troubleshooting" of the *DWDM Alarm and Troubleshooting Guide*.

  **Note** If necessary, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

  - If the APC state is not DISABLE - INTERNAL, continue with Step 3.

**Step 3** Verify that the intranode connections have been built in:

a. Go to the node view on the MSTP node that is the source node for the circuit.
b. Click the **Provisioning > WDM-ANS > Connections** tabs.
c. Verify the all node connections have been created and that their state is Connected.

**Tip** To quickly verify the connections, click the **Calculate Connection** button and check to see if any new connections come up.

If some connections are missing, perform the proper procedure according to Chapter 3, "Turn Up a Node" in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Step 4** If necessary, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

# 1.13 Node Level (Intranode) Problems

Troubleshooting for node-level optical channel (OCH) VOA start-up failure is discussed in this section.

**Note** In the following paragraphs, a reference to the 32-WSS card also includes the 32-WSS-L card.

A dedicated VOA regulates the optical power for every single channel (single wavelength) inserted in the MSTP system through a 32-WSS, 32MUX-O, or AD-xC-xx.x card.

The final state for the VOAs is the power control working mode. In this mode, the attenuation that the VOA introduces is automatically set based on the feedback provided from a dedicated photodiode, so that a specific power setpoint value is reached and maintained.

Prior to following the procedures in this section, pay attention to the following information.

**Note** The ALS function should only be disabled temporarily for installation or maintenance reasons. Activate ALS immediately after maintenance or installation.

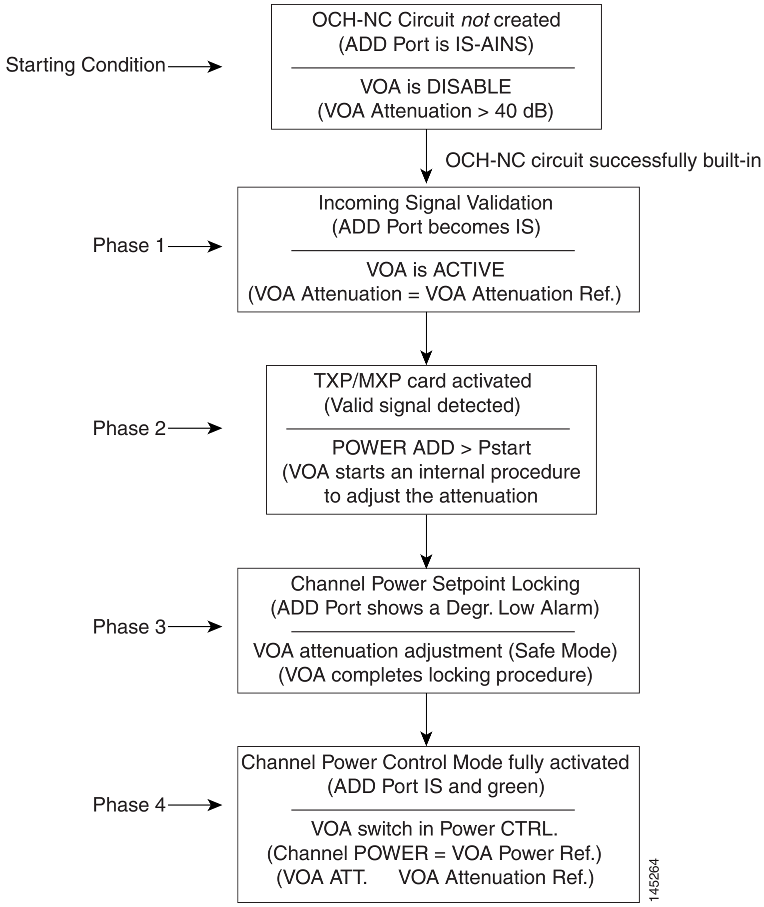
The following warning applies to handling unterminated fibers when ALS is disabled:

**Warning** **Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard.** Statement 1056

## 1.13.1 VOA Startup Phases

The final VOA condition is achieved through a startup procedure divided into the four sequential phases shown in Figure 1-31.

*Figure 1-31 VOA Startup Procedure*




Until the VOA has completed all the phases shown in Figure 1-31, the power control mode is not fully activated.

## 1.13.1.1 Phase 1: Incoming Signal Validation

The Incoming Signal Validation phase checks to see that the optical interface connection is valid and that the optical power level is appropriate.

Cisco MetroPlanner calculates the VOA Attenuation Reference value to allow only supported MSTP interfaces to overcome the power start-up (Pstart-up) acceptance level. (Refer to the "Network-Level Gain—Tilt Management of Optical Amplifiers" section in the "Network Reference" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.).

If the interface that is connected has a power value outside the allowed range, the Phase 1 check prevents OCHNC turn-up.

## 1.13.1.2 Phase 2: TXP/MXP Card Activated (Valid Signal Detected)

If Phase 1 indicates that the signal is valid, an automatic iterative attenuation adjustment on the VOA takes place to reach a power target on the photodiode downstream of the VOA.

**Note** The power setpoint is generated by Cisco MetroPlanner on a case-by-case basis. During the ANS run, the power target is provisioned on the VOA.

### 1.13.1.3 Phase 3: Channel Power Setpoint Locking

In Phase 3, the VOA is kept in a transient standby condition when a steady power value close enough to the final power setpoint has been reached (nominally 3 dBm lower).

The duration of the transient standby condition is three seconds (by default) and allows safe management of optical interfaces that have different signal rise time values or are undergoing a pulse startup procedure compliant with the ITU-T G664 recommendation.

### 1.13.1.4 Phase 4: Channel Power Control Mode Fully Activated

The VOA reaches the final attenuation condition that leads the power value that is read on the photodiode to the expected target value (VOA Power Reference). Simultaneously, the VOA operating mode switches to power control mode.

From this point on, any further adjustment of the VOA attenuation is triggered by a variation of the value read on the photodiode. The aim of these adjustments is to always keep the power value equal to the power setpoint, with +/– 0.5 dBm as the minimum adjustment increment.

## 1.13.2 VOA Failure Scenarios

Several conditions can stop the startup procedure at an intermediate step, blocking the VOA (and the circuit activation, as a consequence) from completing activation of the power control mode. The scenarios in this section portray those conditions.

Root-cause identification can be performed based on the alarm raised and the power reading on the photodiode associated with the VOA.

### 1.13.2.1 Scenario A: Optical Power Level of the Incoming Signal Lower Than Minimum Allowed by MSTP Supported Optical Interfaces

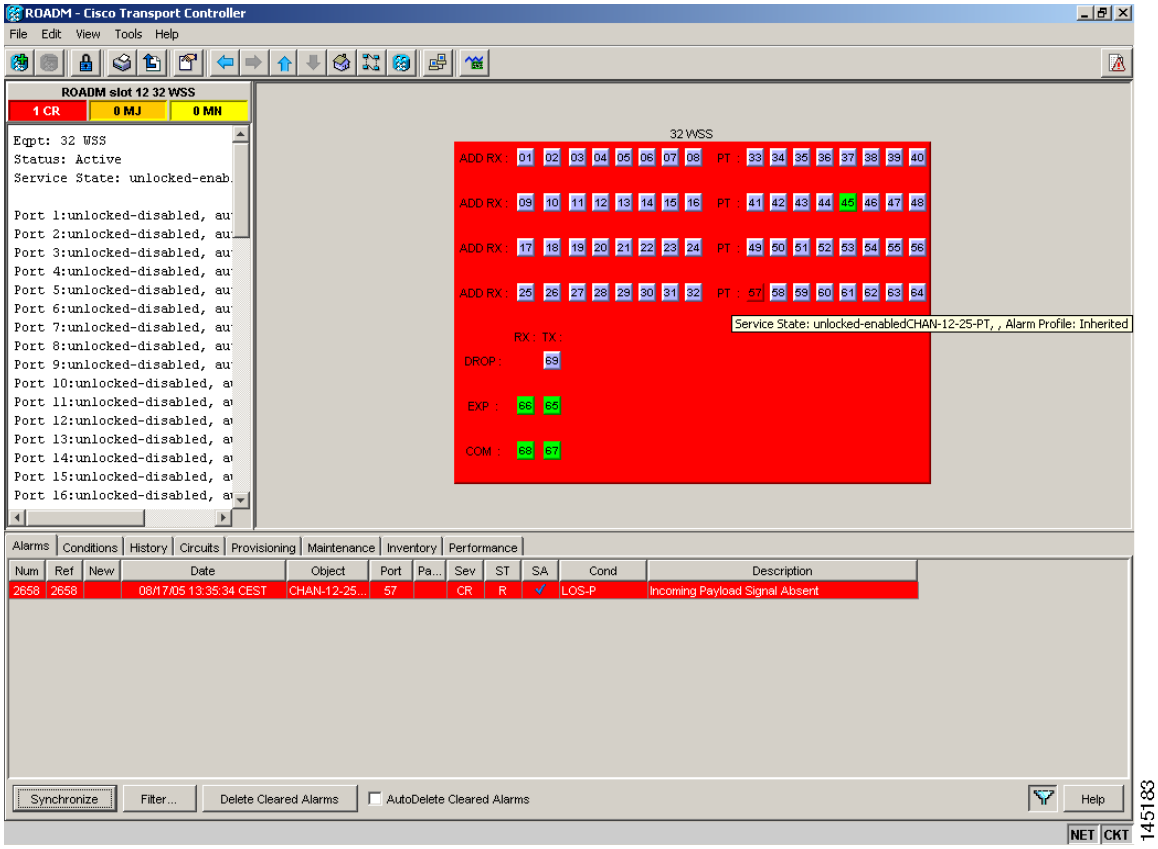
This scenario is for a condition where a TXP or MXP card is directly connected to a 32MUX-O or 32WSS card where power in is expressed as Pin < – 4.5 dBm.

If the incoming power level is lower than the minimum allowed, the startup procedure always stops at Phase 1 (see Figure 1-32). This is the case even if the final VOA Power Reference reported in CTC is reachable.

The final conditions that CTC reports are:

- A LOS-P (OCH layer) alarm on the port associated with the VOA (see Figure 1-32)
- A valid (different from the end of scale value of – 50 dBm) optical power value in the Power field, but the value for Power is less than – 33 dBm. (To view the Power field, in card view, click the **Provisioning > Parameters** tabs.)

*Figure 1-32 LOS-P Indication on the VOA Port*




Use the following procedure to troubleshoot and eventually fix issues related to the VOA start-up when the optical power level of the incoming signal is lower than the minimum allowed by the MSTP supported optical interfaces (32MUX-O and 32WSS cards).

**Step 1** Verify the alarm validity:

- **a.** Identify the DWDM nodes where the alarmed card is seated.
- **b.** Double-click the card (either the 32MUX-O or the 32WSS card).
- **c.** Click **Alarms**.
- **d.** Verify that a LOS-P alarm is present on the ADD-RX port.
- **e.** Click the **Synchronize** button in the bottom left of the window.
- **f.** If the alarm is correctly reported, move to Step 2. If not, close the CTC application, delete the CTC cache, and open the CTC connection again.

**Note** If the alarm inconsistency persists, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

**Step 2** f the alarmed card is a 32WSS, verify the incoming power level from the connected TXP, MXP, or line card. If the alarmed card is a 32MUX-O, go to Step 5.

a. Double-click the 32WSS card.

b. Click the **Provisioning** > **Optical Chn: Optical Connector X > Parameters** tabs to display the optical power physically coming into the 32WSS ADD-RX port.

> **Note** X is the number (1 to 4) of the appropriate multifiber push-on (MPO) connector that manages the alarmed channel (wavelength).

c. Identify the proper channel (wavelength) and read the Power ADD field.

d. If the Power ADD value is less than –4.5 dBm, go to Step 3. If not, click the **Provisioning** > **Optical Chn: Optical Connector X** > **Parameters** tabs.

> **Note** X is the number (1 to 4) of the appropriate multifiber MPO connector that manages the alarmed channel (wavelength).

e. Identify the correct row based on the **Type** field (the row must indicate Add in the type field).

f. Decrease the attenuation on the VOA to the minimum (0 dB) to enable channel startup. To perform this adjustment:

- Read the VOA Attenuation Ref value for the channel (wavelength).
- Enter into the VOA Attenuation Calib field the same value as that of the VOA Attenuation Ref field, but with the opposite sign (the algebraic sum of the two contributions must be equal to zero).
- Click **Apply**. If the LOS-P alarm persists, continue with this procedure. Otherwise, the problem has been corrected.

g. In card view, click **Circuits**.

h. Delete the OCHNC circuit that relates to the faulty channel.

i. Ensure that the corresponding ADD-RX service state port changes to **IS-AINS** (or unlocked, automaticInService) and that the color changes to grey (the LOS-P alarm should clear).

j. Recreate the OCHNC circuit and verify that the Status field reports DISCOVERED and that the state is IS (unlocked).

k. If the LOS-P alarm has not cleared, replace the 32WSS card (refer to the "Remove and Replace DWDM Cards" procedure in the "Add and Remove Cards and Nodes" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*). Before you replace the card, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

**Step 3** Because the actual power received by the 32WSS card is lower than expected, verify the correct behavior of the TXP, MXP, or line card connected to the 32WSS:

a. The TX laser must be active (trunk port is in **IS** [or, **unlocked**] state).

b. The wavelength provisioned must be the proper one.

c. The output power value must be within the expected range (refer to the "Specifications" appendix in the *Cisco ONS 15454 DWDM Installation and Operations Guide*). If the trunk port PM is not available through CTC, perform a manual measurement using a standard power meter.

d. If the TX laser is active, the wavelength is provisioned properly, and the output power value is in the correct range, go to Step 4. Otherwise, take the appropriate corrective action, including card replacement if the output power value is outside of the expected range (refer to the "Remove and Replace DWDM Cards" procedure in the "Add and Remove Cards and Nodes" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*. Replacing the card should correct the problem.)

**Step 4** If the TXP or MXP card behaves as expected, the only remaining root-cause is the fiber connection between the two cards:

a. Verify that the ADD_RX port of the alarmed 32WSS is connected to the TRUNK_TX port of the TXP or MXP card using an MPO-LC multifiber cable.

**Note** A patch-panel tray is normally used to manage fiber connections (for patch-panel cabling details, refer to the "Turn Up a Node" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*).

b. Check and clean the LC fiber fan-out according to site practice. The fiber numbers (1 to 8) must correspond to the wavelength managed.

c. If a patch panel is used, check and, if necessary, clean the LC-LC adapter. If necessary, replace any bad devices (maximum tolerance is 1 dB).

d. Pull out the LC connector from the TRUNK_TX port of the TXP or MXP card and clean the fiber according to site practice.

**Note** If no site practice exists for cleaning fibers, complete the procedure in the "Maintain the Node" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Note** If the alarm condition has not cleared, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

**Step 5** When the alarmed card is a 32MUX-O, the troubleshooting procedure should start from the TXP, MXP, or line card. Verify the correct behavior of the TXP, MXP, or line card connected to the 32MUX-O:

a. The TX laser must be active (trunk port is in **IS** [or unlocked] state).

b. The wavelength provisioned must be the proper one.

c. The output power value must be within the expected range (refer to the "Hardware Specifications" appendix in the *Cisco ONS 15454 DWDM Installation and Operations Guide*). If the trunk port PM is not available through CTC, perform a manual measurement using a standard power meter.

d. If the TX laser is active, the wavelength is provisioned properly, and the output power value is in the correct range, go to Step 6. Otherwise, take the appropriate corrective action, including card replacement if the output power value is outside of the expected range (refer to the "Remove and Replace DWDM Cards" procedure in the "Add and Remove Cards and Nodes" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*. Replacing the card should correct the problem.)

**Step 6** If the TXP or MXP card behaves as expected, check the fiber connection between the two cards:

a. The ADD_RX port of the alarmed 32MUX-O must be connected to the TRUNK_TX port of a TXP or MXP card using an MPO-LC multifiber cable.

> **Note** A patch-panel tray is normally used to manage fiber connections (for patch-panel cabling details, refer to the "Turn Up a Node" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*).

**b.** Check and clean the LC fiber fan-out according to site practice. The fiber numbers (1 to 8) must correspond to the wavelength managed.

**c.** If a patch panel is used, check and, if necessary, clean the LC-LC adapter.

**d.** If necessary, replace any bad devices (maximum tolerance is 1 dB).

**e.** Pull out the LC connector from the TRUNK_TX port of the TXP or MXP card and clean the fiber according to site practice.

> **Note** If no site practice exists for cleaning fibers, complete the procedure in the "Maintain the Node" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**f.** If the alarm condition persists, move to Step 7. Otherwise, the problem has been corrected.

**Step 7** Verify the correct behavior of the VOA inside the 32MUX-O card:

**a.** Double-click the 32MUX-O card.

**b.** Click **Circuits**.

- Delete the OCHNC circuit relating to the faulty channel.
- Ensure that the service state of the corresponding ADD-RX port changes to IS-AINS (or unlocked, automaticInService), and that the color turns grey (the LOS-P alarm should clear).

**c.** In card view, click the **Provisioning > Optical Chn: Optical Connector X > Parameters** tabs and identify the proper channel (wavelength).

> **Note** X refers to one of the 32-WSS connectors

**d.** Decrease the attenuation on the VOA to the minimum (0 dB) to enable channel startup. To perform this in field adjustment:

- Read the VOA Attenuation Ref value for the channel (wavelength).
- Enter the same value into the VOA Attenuation Calib field as that of the VOA Attenuation Ref field, but with the opposite sign (the algebraic sum of the two contributions must be equal to zero).
- Click **Apply**. If the LOS-P alarm persists, continue with this procedure. Otherwise, the problem has been corrected.

**e.** Click **Circuits**.

**f.** Recreate the OCHNC circuit and verify that Circuit Status field reports DISCOVERED and the state is IS (unlocked).

**g.** If the LOS-P alarm has not cleared, replace the 32MUX-O card (refer to the "Remove and Replace DWDM Cards" procedure in the "Add and Remove Cards and Nodes" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*). Before you replace the card, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem).

## 1.13.2.2 Scenario B: Optical Power Level of the Incoming Signal Lower Than Expected

In some cases, the pass-through channels on the 32WSS card or the optical bypass channels on the 32MUX-O card are at a power level that is lower than expected. The incoming power level can be lower than expected for several reasons. A few examples are:

- Dirty connections
- Excessive span loss
- Wrong amplifier gain setting

When the power is lower than expected, the start-up procedure can stop at Phase 1, Phase 2, or Phase 3 (see Figure 1-31). The point at which the start-up procedure stops depends on the amount of power missing.

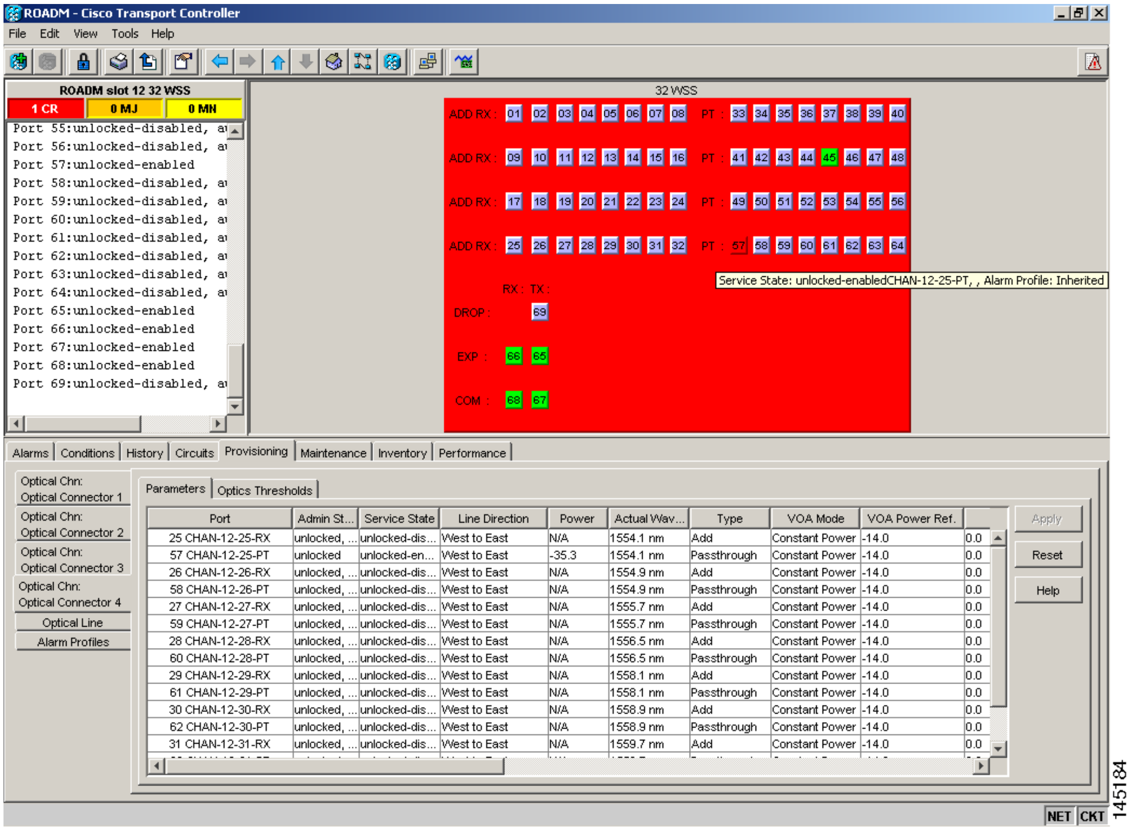
Given that delta power is the amount of optical power missing compared to the expected value, two final conditions for Scenario B can be identified, conditions B1 and B2.

### 1.13.2.2.1 Condition B1—Delta Power > 6 dB (LOS-P Alarm)

When the optical power is greater than 6 dB lower than the expected value, the final VOA Power Reference setpoint value is definitively not reachable and even Phase 1 of the start-up procedure cannot be properly completed. As a consequence, the final condition reported in CTC is the same as that of Scenario A:

- A LOS-P (OCH layer) alarm is present on the port associated with the VOA.
- A valid (different from the end of scale value of – 50 dBm) optical power value can be read in the Power field, but the value for Power is less than – 33 dBm (see Figure 1-33). (To access this value, in card view, click the **Provisioning > Parameters** tabs.)

*Figure 1-33 Power Level of Incoming Signal Less than –33 dBm*



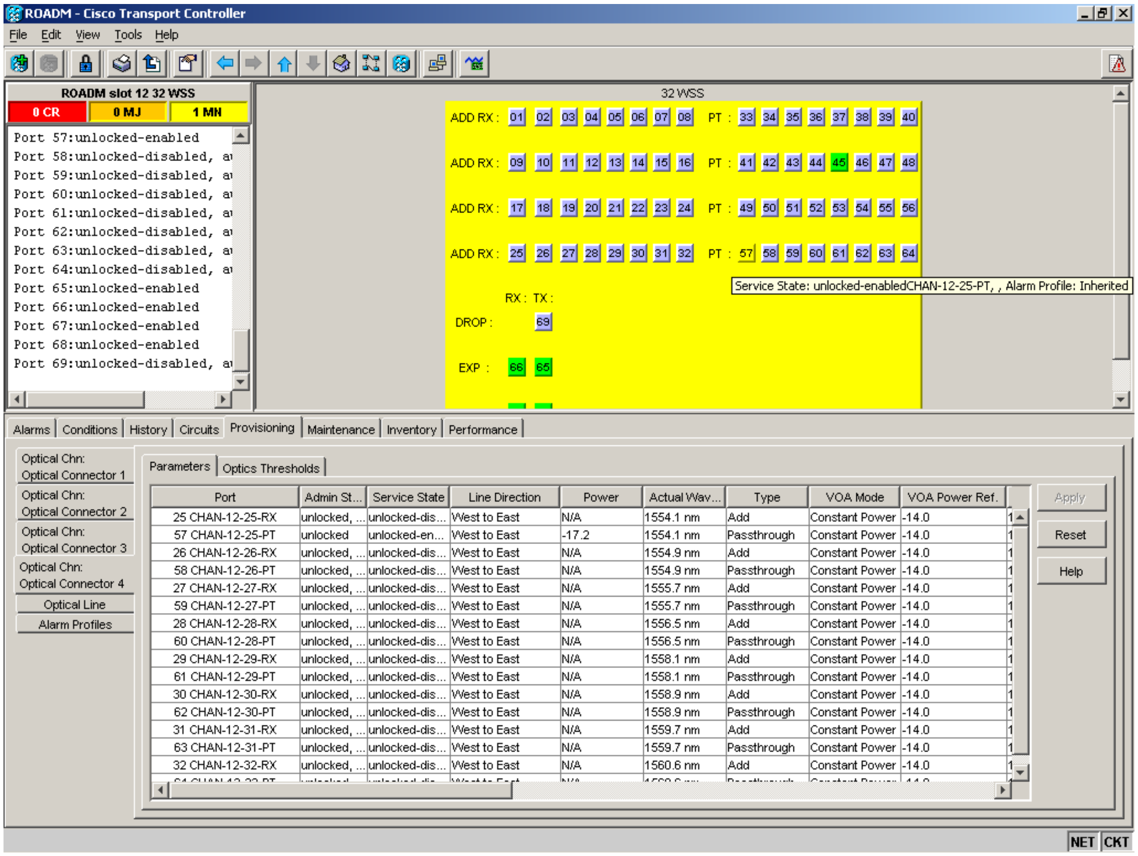

## 1.13.2.2.2 Condition B2—Delta Power < 6 dB (OPWR-LowDEGrade Alarm)

When the optical power is less than 6 dB lower than the expected value, even if a valid incoming signal is present, the final VOA Power Reference setpoint value that is reported in the CTC is not reachable and the VOA startup procedure is stopped at Phase 3.

The final conditions that CTC reports are:

- An OPWR-LowDEGrade (OCH layer) alarm is present on the port associated with the VOA.
- A valid (different from the end of scale value of –50 dBm) optical power value can be read in the Power field, but the value is (VOA Power Ref – 6 dBm) < Power < VOA Power Ref (see Figure 1-34). To access this value, in card view, click the **Provisioning > Parameters** tabs.

*Figure 1-34 Optical Power Less than 6 dB Lower than Expected*




145185

### 1.13.2.2.3 Corrective Actions for Scenario B (Optical Power Level of Incoming Signal Lower than Expected)

When the optical power level of the incoming signal is lower than expected for the pass-through channels on the 32WSS or the optical bypass channels on the 32MUX-O card, use the following procedure to troubleshoot and eventually fix issues related to VOA start-up:

According to the final conditions reported by the card (either LOS-P alarm for condition B1 or OPWR-LowDEGrade for condition B2), two troubleshooting procedures are suggested.

If condition B1 (see "1.13.2.2.1 Condition B1—Delta Power > 6 dB (LOS-P Alarm)" section on page 1-86) results in an LOS-P alarm, compete the following procedure:

**Step 1** Verify the alarm validity:

**a.** Identify the DWDM nodes where the alarmed card is located.

**b.** Double-click the card (either the 32MUX-O or the 32WSS card).

**c.** Click **Alarms**.

**d.** Verify that a LOS-P alarm is present on the ADD-RX port.

**e.** Click the **Synchronize** button at the bottom left of the window.

**f.** If the alarm is correctly reported, move to Step 2. If not, close the CTC application, delete the CTC cache, and open the CTC connection again.

> **Note** If the alarm inconsistency persists, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

**Step 2** In card view, click **Circuits** and retrieve the node, card, and port information for the alarmed channel from the Source field of the OCHNC circuit. Then follow the procedures of Step 3 (32MUX-O, 32WSS, or AD-xC-xx.x card) or Step 4 (TXP, MXP, or line card) as appropriate.

**Step 3** Verify the correct behavior of the far-end DWDM card (32MUX-O, 32WSS, or AD-xC-xx.x) that manages the channel (wavelength):

a. Verify that the power value coming in on the ADD_RX port is correct.
   - In card view, click the **Provisioning > Optical Chn: Optical Connector X > Parameters** tabs.

   > **Note** X is number (1 to 4) of the proper multifiber MPO connector that manages the alarmed channel (wavelength).

   - The Power field value must be the same as that in the VOA Power Ref field. If not, take the appropriate corrective actions according to the alarm raised at the RX-ADD port.

**Step 4** Verify the correct behavior of the TXP, MXP, or line card that is the signal source of the channel (wavelength) that is alarmed:

a. The TX laser must be active (trunk port is in IS [unlocked] state).
b. The wavelength provisioned must be the proper one.
c. The output power value must be within the expected range (refer to the "Hardware Specifications" appendix in the *Cisco ONS 15454 DWDM Installation and Operations Guide*). If the trunk port PM is not available through CTC (for example, TXP_MR_2.5G), perform a manual measurement using a standard power meter.

**Step 5** If the cards referenced in Step 3 and Step 4 are operating properly, go to Step 6. If not, take the appropriate corrective actions according to the alarm raised on the card. See the appropriate procedure for the alarm in Chapter 2, "Alarm Troubleshooting" of the *DWDM Alarm and Troubleshooting Guide*.

**Step 6** If the alarmed card is a 32MUX-O, go to Step 9**.**

**Step 7** If the alarmed card is a 32WSS, continue with the following steps:

a. Double-click the card.
b. Click the **Provisioning > Optical Chn: Optical Connector X > Parameters** tabs.

   > **Note** X is number (1 to 4) of the proper multifiber MPO connector that manages the alarmed channel (wavelength).

c. Identify the correct row based in the Type field (the row must indicate Passthrough in the type field).
d. Decrease the attenuation on the VOA to the minimum (0 dB) to enable channel startup. To perform this in field adjustment:
   - Read the VOA Attenuation Ref value for the channel (wavelength).
   - Enter the same value into the VOA Attenuation Calib field as that of the VOA Attenuation Ref field, but with the opposite sign (the algebraic sum of the two contributions must be equal to zero).

- Click **Apply**. If the LOS-P alarm persists, continue with this procedure. Otherwise, the problem has been corrected.

e. Click **Circuits**.

f. Delete the OCHNC circuit for the faulty channel.

g. Ensure that the service state of the corresponding ADD-RX port changes to IS-AINS (or unlocked, automaticInService) and that the color changes to grey (LOS-P alarm should clear).

h. Recreate the OCHNC circuit and verify that Circuit Status field reports DISCOVERED and the state is IS (unlocked).

i. If the LOS-P alarm has not cleared, continue with Step 8. Otherwise, the problem has been corrected.

**Step 8** To unambiguously pinpoint the root cause of the alarm, verify the proper cabling of the EXP_RX port (which is the common input port for all the pass-through channels) on the 32WSS card:

a. The EXP_RX port of the alarmed 32WSS must be connected to the EXP_TX port of the coupled 32WSS card on the opposite side of the node.

b. Pull out the LC connector from the EXP_RX port of the 32WSS and clean the fiber according to site practice.

c. Pull out the LC connector from the EXP_TX port of the coupled 32WSS and clean that connector also.

d. Verify that the fiber attenuation is within the specifications (maximum tolerance is 1 dB).

e. If necessary, replace any bad fibers.

**Note** If no site practice exists for cleaning fibers, complete the procedure in the "Maintain the Node" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

f. If the alarm condition persists even after the checking and fixing the fibers, replace the 32WSS card (refer to the "Remove and Replace DWDM Cards" procedure in the "Add and Remove Cards and Nodes" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*). Before replacing the card, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem).

**Step 9** Verify the correct behavior of the VOA inside the 32MUX-O card:

a. Double-click the 32MUX-O card.

b. Click **Circuits**.

c. Delete the OCHNC circuit for the faulty channel.

d. Ensure that the service state of the corresponding ADD-RX port changes to IS-AINS (or unlocked, automaticInService) and that the color changes to grey (LOS-P alarm should clear).

e. Click the **Provisioning > Optical Chn: Optical Connector X > Parameters** tabs and identify the proper channel (wavelength).

**Note** *X* is number (1 to 4) of the proper multifiber MPO connector that manages the alarmed channel (wavelength).

f. Decrease the attenuation on the VOA to the minimum (0 dB) to enable channel startup. To perform this in field adjustment:

- Read the VOA Attenuation Ref value for the channel (wavelength).
- Enter the same value into the VOA Attenuation Calib field as that of the VOA Attenuation Ref field, but with the opposite sign (the algebraic sum of the two contributions must be equal to zero).
- Click the **Apply** button. If the LOS-P alarm persists, continue with this procedure. Otherwise, the problem has been corrected.

**g.** Click **Circuits**.

**h.** Recreate the OCHNC circuit and verify that Circuit Status field reports DISCOVERED and the state is IS (unlocked).

**i.** If the LOS-P alarm has not cleared, continue with Step 10. Otherwise, the problem has been corrected.

**Step 10** To unambiguously pinpoint the root cause of the alarm, verify the proper cabling of the alarmed ADD_RX port on the 32MUX-O card:

**a.** The ADD_RX port of the alarmed 32MUX-O must be connected to the DROP_TX port of the coupled 32DMX-O card on the opposite side of the node using two MPO-LC multifiber cables.

**Note** A patch-panel tray is normally used to manage fiber connections (for patch-panel cabling details, refer to the "Turn Up a Node" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*).

**b.** Verify that the power value coming out of DROP_TX port of the coupled 32DMX-O card is correct:

- In card view, click the **Provisioning > Optical Chn: Optical Connector X > Parameters** tabs.

  **Note** *X* is number (1 to 4) of the proper multi-fibers MPO connector that manages the alarmed channel (wavelength).

- The Power field value must be the same as that in the VOA Power Ref field. If it is not, take the appropriate corrective action for the alarm according to Chapter 2, "Alarm Troubleshooting.".

**c.** Check and clean the LC fiber fan-out according to site practice. The fiber numbers (1 to 8) must correspond to the wavelength managed.

**d.** Repeat Step c for the MPO-LC multifiber cable coming out of the DROP_TX port of the coupled 32DMX-O card.

**e.** Check and, if necessary, clean the LC-LC adapter.

**f.** If necessary, replace and bad devices (maximum tolerance is 1 dB).

**Note** If no site practice exists for cleaning fibers, complete the procedure in the "Maintain the Node" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**g.** If the alarm condition persists even after the cabling is checked or fixed, replace the 32MUX-O card (refer to the "Remove and Replace DWDM Cards" procedure in the "Add and Remove Cards and Nodes" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*. Before replacing the card, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem).

If condition B2 (see "1.13.2.2.2 Condition B2—Delta Power < 6 dB (OPWR-LowDEGrade Alarm)" section on page 1-87) results in an OPWR-LowDEGrade alarm, compete the following procedure:

---

**Step 1** Verify the alarm validity:

a. Identify the DWDM node where the alarmed card is located.

b. Double-click the card (either the 32MUX-O or the 32WSS card).

c. Click **Alarms**.

d. Verify that an Optical Power Degrade Low (OPWR-LDEG) alarm is present on the ADD-RX port.

e. Click the **Synchronize** button at the bottom left of the window.

f. If the alarm is correctly reported, goto Step 2. If not, close the CTC application, delete the CTC cache, and open the CTC connection again.

> **Note** If the alarm inconsistency persists, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

**Step 2** In card view, click **Circuits** and retrieve the node, card, and port information for the alarmed channel from the Source field of the OCHNC circuit. Then, follow the procedures in Step 3 (for 32MUX-O, 32WSS, or AD-xC-xx.x cards) or Step 4 (for TXP, MXP, or line cards) as appropriate.

**Step 3** Verify the correct behavior of the far-end DWDM card (32MUX-O, 32WSS, or AD-xC-xx.x) that manages the channel (wavelength). To do this, verify that the power value coming in on the ADD_RX port is correct:

a. In card view, click the **Provisioning > Optical Chn: Optical Connector X > Parameters** tabs.

> **Note** X is number (1 to 4) of the proper multi-fibers MPO connector that manages the alarmed channel (wavelength).

b. The Power field value must be the same as that in the VOA Power Ref field. If it is not, take the appropriate corrective action for the alarm according to Chapter 2, "Alarm Troubleshooting" in the *DWDM Alarm and Troubleshooting Guide*.

**Step 4** Verify the correct behavior of the TXP, MXP, or line card that is the signal source of the channel (wavelength) that is alarmed:

a. The TX laser must be active (trunk port is in IS [unlocked] state).

b. The wavelength provisioned must be the proper one.

c. The output power value must be within the expected range (refer to the "Hardware Specifications" appendix in the *Cisco ONS 15454 DWDM Installation and Operations Guide*). If the trunk port PM is not available through CTC, perform a manual measurement using a standard power meter.

**Step 5** If the cards referenced in Step 3 and Step 4 are operating properly, go to Step 6. If not, take the appropriate corrective actions according to the alarm raised on the card (see Chapter 2, "Alarm Troubleshooting" in the *DWDM Alarm and Troubleshooting Guide)*.

**Step 6** If the alarmed card is a 32MUX-O card, go to Step 8.

**Step 7** If the alarmed card is a 32WSS card, verify the proper cabling of the EXP_RX port (common input port for all pass-through channels) on the 32WSS card:

a. Verify that the EXP_RX port of the alarmed 32WSS is connected to the EXP_TX port of the coupled 32WSS card on the opposite side of the node.

b. Pull out the LC connector from the EXP_RX port of the 32WSS card and clean the fiber according to site practice.

c. Pull out the LC connector from the EXP_TX port of the coupled 32WSS card and clean its connector also.

d. Verify that the fiber attenuation is within the specifications (maximum tolerance is 1 dB).

e. If necessary, replace any bad fibers.

**Note** If no site practice exists for cleaning fibers, complete the procedure in the "Maintain the Node" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Note** If the alarm condition persists even after the cabling check/fixing, the root cause could be related to a network issue and a more accurate analysis of the signal flow is needed according to the actual system topology. If necessary, call Cisco TAC (1 800 553-2447) for help.

**Step 8** Verify the proper cabling of the alarmed ADD_RX port on the 32MUX-O card:

a. Verify that the ADD_RX port of the alarmed 32MUX-O is connected to the DROP_TX port of the coupled 32DMX-O card on the opposite side of the node, using two MPO-LC multifiber cables.

**Note** A patch-panel tray is normally used to manage fiber connections (for patch-panel cabling details, refer to the "Turn Up a Node" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*).

b. Verify that the power value coming out of the DROP_TX port of the coupled 32DMX-O card is correct:

- In card view, click the **Provisioning > Optical Chn: Optical Connector X > Parameters** tabs.

  **Note** *X* is number (1 to 4) of the proper multifiber MPO connector that manages the alarmed channel (wavelength).

- The Power field value must be the same as that in the VOA Power Ref field. If it is not, take the appropriate corrective action for the alarm according to Chapter 2, "Alarm Troubleshooting."

c. Check (the number 1 to 8 must correspond with the wavelength managed) and clean the LC fan-out according to site practice.

d. Repeat Step c for the MPO-LC multifiber cable coming out of the DROP_TX port of the coupled 32DMX-O card.

e. Check and, if necessary, clean the LC-LC adapter used.

f. If necessary, replace any bad devices (maximum tolerance is 1 dB).

**Note** If no site practice exists for cleaning fibers, complete the procedure in the "Maintain the Node." chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Note** If the alarm condition persists even after the cable check and repair procedures, the root cause could be related to a network issue and a more accurate analysis of the signal flow is needed according with the actual system topology. If necessary, call Cisco TAC (1 800 553-2447) for help.

### 1.13.2.3 Scenario C: Optical Drop Power Level Lower Than Expected

This scenario describes the condition in which the optical power at the 32DMX-O drop channels is lower than expected. The 32DMX-O card is equipped with a VOA for each wavelength, and each VOA manages the power for one dropped wavelength.

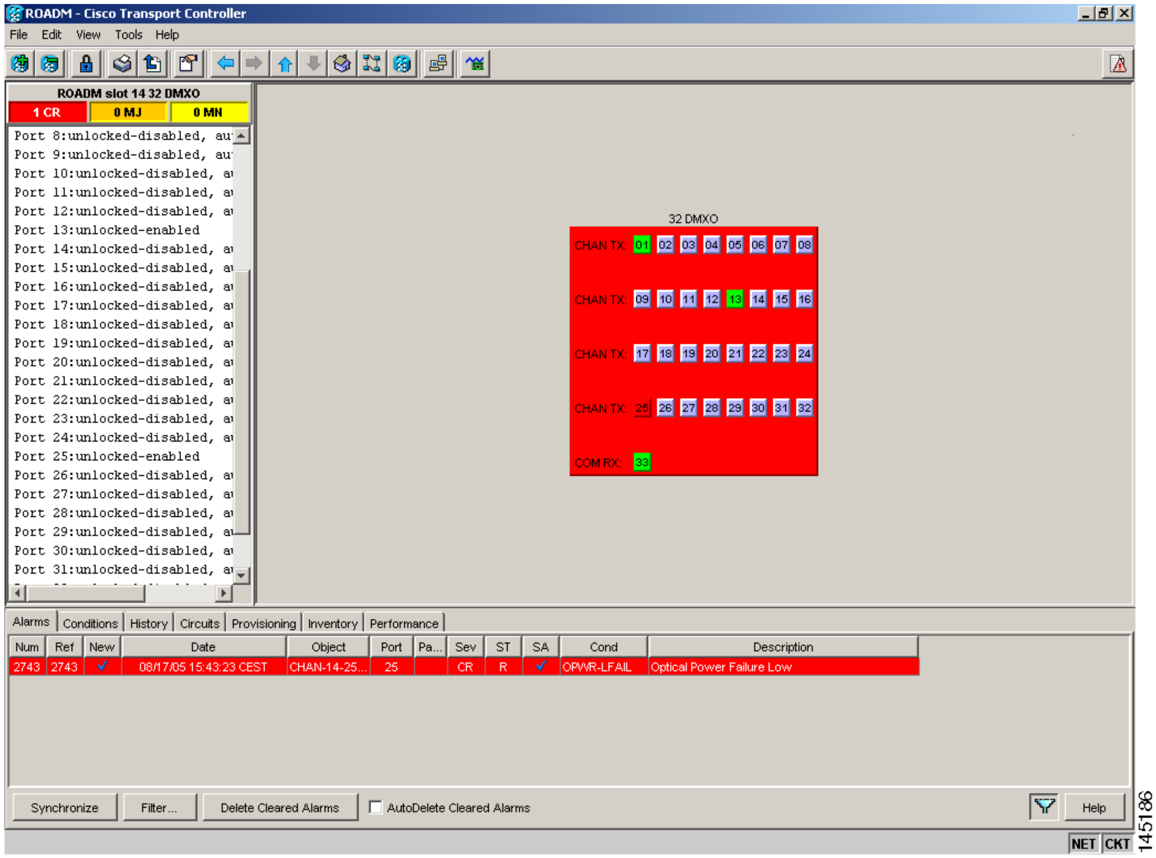
The failing scenarios during the OCHNC turn-up and consequent VOA startup are the same as those described in the "1.13.2.2 Scenario B: Optical Power Level of the Incoming Signal Lower Than Expected" section on page 1-86. The only difference is the type of alarm that is raised when the condition exists in which delta power is greater than 6 dB.

#### 1.13.2.3.1 Condition C1—Delta Power > 6 dB Lower than Expected

When the optical power on the dropped channel is greater than 6 dB lower that the value expected, the final VOA Power Reference setpoint value is definitively not reachable. As a consequence, the final conditions reported in CTC are as follows:

- An **OPWR-LFAIL** (OCH layer) alarm is present on the port associated with the VOA (see Figure 1-35).
- A valid (different from the end of scale value of – 50 dBm) optical power value can be read in the CTC Power field, but the Power value is less than – 33 dBm. (To view this value in card view, click the **Provisioning > Parameters** tabs.)

*Figure 1-35 Optical Drop Power Greater than 6 dB Lower than Expected*



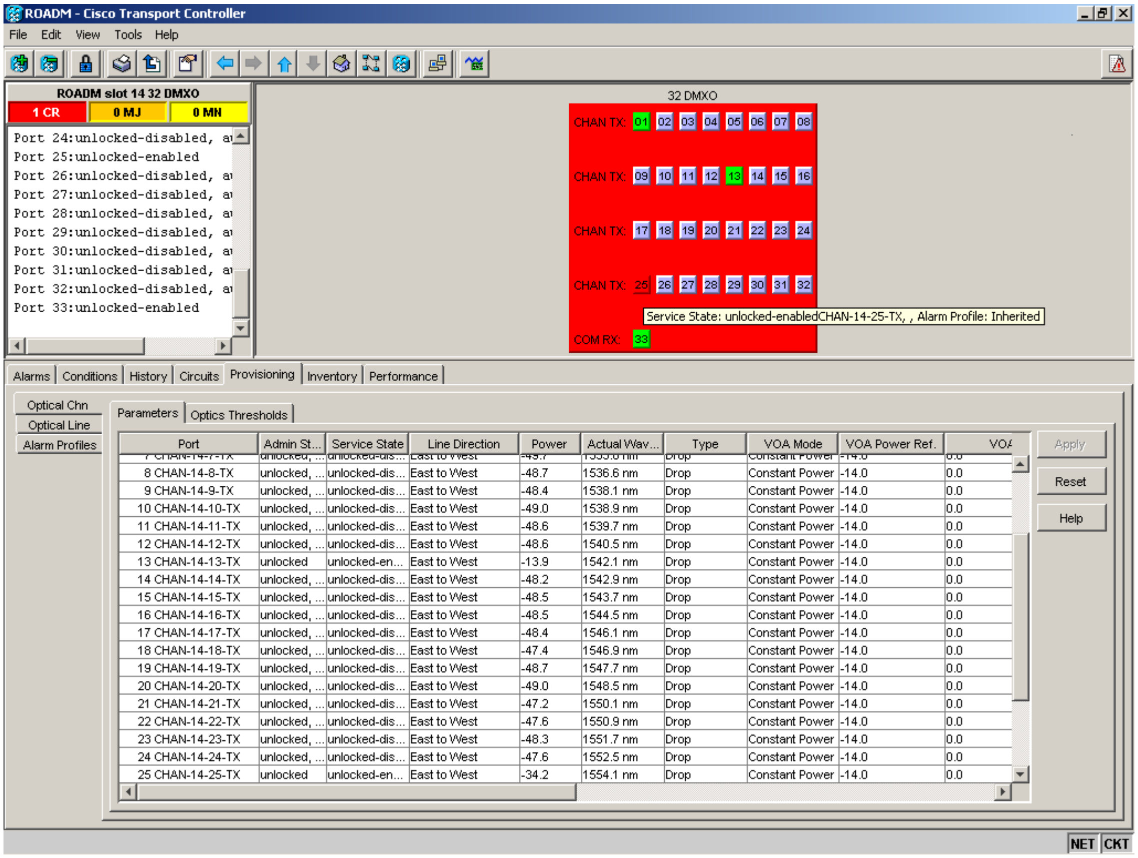

### 1.13.2.3.2 Condition C2—Delta Power < 6 dB Lower than Expected

If the delta power is less than 6 dB lower than expected, the final conditions reported in CTC are the same as those reported for ConditionB2 (see 1.13.2.2.2 Condition B2—Delta Power < 6 dB (OPWR-LowDEGrade Alarm), page 1-87):

- An OPWR-LowDEGrade (OCH layer) alarm is present on the port associated with the VOA.
- A valid (different from the end of scale value of – 50dBm) optical power value can be read in the CTC Power field, but the value is (VOA Power Ref – 6 dBm) < Power < VOA Power Ref (Figure 1-34). To view this value in card view, click the **Provisioning > Parameters** tabs.).

A dirty connection or excessive loss of the incoming span are among the possible reasons that can lead to a fault condition. They are the most common and affect all wavelengths, whereas an excessive amplifier gain tilt or a wavelength misconfiguration on the far-end TXP or MXP card can lead to condition where only a single wavelength fails, such as the one (Channel 25) shown in Figure 1-36.

*Figure 1-36 Optical Drop Power Less than 6 dB Lower than Expected*




145187

#### 1.13.2.3.3 Corrective Action for Scenario C (Optical Power Level of Incoming Signal Lower than Expected)

If condition C1 (see "1.13.2.3.1 Condition C1—Delta Power > 6 dB Lower than Expected" section on page 1-94) results in an LOS-P alarm, compete the following procedure:

---

**Step 1** Verify the alarm validity:

**a.** Identify the DWDM nodes where the alarmed card is located.

**b.** Double-click the 32DMX-O card.

**c.** Click **Alarms**.

**d.** Verify that a LOS-P alarm is present on the CHAN-TX port.

**e.** Click the **Synchronize** button at the bottom left of the window.

**f.** If the alarm is correctly reported, move to Step 2. If not, close the CTC application, delete the CTC cache, and open the CTC connection again.

---

**Note** If the alarm inconsistency persists, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

---

**Step 2** Verify the correct behavior of the far-end DWDM card (32MUX-O, 32WSS, AD-xC-xx.x) that manages the channel (wavelength), and the TXP, MXP, or line card that is the signal source of the channel (wavelength) alarmed:

a. Click **Circuits** and retrieve the node, card, and port information for the alarmed channel from the Source field of the OCHNC circuit.

b. For the far-end DWDM card, verify that the power value coming in the ADD_RX port is correct:

- In card view, click the **Provisioning > Optical Chn: Optical Connector X > Parameters** tabs.

**Note** *X* is number (1 to 4) of the proper multifiber MPO connector that manages the alarmed channel (wavelength).

- The Power field value must be the same of VOA Power Ref field. If not, take the appropriate corrective actions according to Chapter 2, "Alarm Troubleshooting."

c. For the corresponding TXP, MXP, or line card connected, verify the following:

- The TX laser is active (the trunk port is in IS [unlocked] state).
- The wavelength provisioned is the proper one.

d. The output power value must be within the expected range (refer to the "Hardware Specifications" appendix in the *Cisco ONS 15454 DWDM Installation and Operations Guide*). If the trunk port PM is not available through CTC (for example, TXP_MR_2.5G), perform a manual measurement using a standard power meter.

e. If everything in Step 2 is correct, go to Step 3. If not, take the appropriate corrective actions according to Chapter 2, "Alarm Troubleshooting."

**Step 3** Verify the correct behavior of the VOA inside the 32DMX-O card:

a. Double-click the 32DMX-O card.

b. Click **Circuits**.

c. Delete the OCHNC circuit for the faulty channel.

d. Ensure that the service state of the corresponding CHAN-TX port changes to IS-AINS (or unlocked, automaticInService) and the color changes to grey (LOS-P alarm should clear).

e. Click the **Provisioning > Optical Chn: Optical Connector X > Parameters** tabs and identify the proper channel (wavelength).

**Note** *X* is number (1 to 4) of the proper multifiber MPO connector that manages the alarmed channel (wavelength).

f. Decrease the attenuation on the VOA to the minimum (0 dB) to enable channel startup. To perform this in field adjustment:

- Read the **VOA Attenuation Ref** value for the channel (wavelength).
- Enter the same value into the VOA Attenuation Calib field as that in the VOA Attenuation Ref field, but with the opposite sign (the algebraic sum of the two contributions must be equal to zero).
- Click **Apply**.

g. Click **Circuits**.

h. Recreate the OCHNC circuit and verify that Circuit Status field reports DISCOVERED and the state is IS (unlocked).

i. If the LOS-P alarm has not cleared, continue with Step 4. If it has cleared, you are finished.

**Step 4** To unambiguously pinpoint the root cause of the alarm, verify the proper cabling of the COM-RX port (common input port for all the drop channels) of the alarmed 32DMX-O card:

a. Verify that the COM_RX port of the alarmed 32DMX-O is connected either to the DROP_TX port of a 32WSS card or to the COM_TX port of an OPT-PRE, OPT-BST, or OSC-CSM card, depending on the actual node layout.

b. Pull out the LC connector from the COM_RX port of the 32DMX-O card and clean the fiber according to site practice.

c. Pull out the LC connector from the COM_TX or DROP_TX port of the connected DWDM card and clean the fiber according to site practice.

d. Verify that the fiber attenuation is within the specifications (maximum tolerance is 1 dB).

e. If necessary, replace any bad fibers.

> **Note** If no site practice exists for cleaning fibers, complete the procedure in the "Maintain the Node" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

f. If the alarm condition persists even after the cabling has been checked and fixed, replace the 32DMX-O card (refer to the "Remove and Replace DWDM Cards" procedure in the "Add and Remove Cards and Nodes" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*. Before replacing the card, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem).

If condition C2 (see "1.13.2.3.2 Condition C2—Delta Power < 6 dB Lower than Expected" section on page 1-95) results in an OPWR-LowDEGrade alarm, compete the following procedure:

---

**Step 1** Verify the alarm validity:

a. Identify the DWDM nodes where the alarmed card is seated.

b. Double-click the 32DMX-O card.

c. Click **Alarms**.

d. Verify that an Optical Power Degrade Low Loss of incoming Payload (OPWR-LDEG) alarm is present on the CHAN-TX port.

e. Click the **Synchronize** button at the bottom left of the window.

f. If the alarm is correctly reported, move to Step 2. If not, close the CTC application, delete the CTC cache, and open the CTC connection again.

> **Note** If the alarm inconsistency persists, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

**Step 2** Verify the correct behavior of the far-end DWDM card (32MUX-O, 32WSS, or AD-xC-xx.x) that manages the channel (wavelength) and the TXP, MXP, or line card that is the signal source of the channel (wavelength) alarmed.

a. Click **Circuits** and retrieve the node, card, and port information for to the alarmed channel from the Source field of the OCHNC circuit.

b. For the far-end DWDM card, verify that the power value coming in on the ADD_RX port is correct:

- In card view, click the **Provisioning > Optical Chn: Optical Connector X > Parameters** tabs.

**Note** *X* is number (1 to 4) of the proper multifiber MPO connector that manages the alarmed channel (wavelength).

- The Power field value must be the same of VOA Power Ref field. If not, take the appropriate corrective actions according to Chapter 2, "Alarm Troubleshooting."

c. For the corresponding TXP, MXP, or line card connected, verify the following:

- The TX laser is active (the trunk port is in IS [unlocked] state).
- The wavelength provisioned is the proper one.

d. The output power value must be within the expected range (refer to the "Hardware Specifications" appendix in the *Cisco ONS 15454 DWDM Installation and Operations Guide*). If the trunk port PM is not available through CTC, perform a manual measurement using a standard power meter.

e. If everything in Step 2 is correct, move to Step 3. If not, take the appropriate corrective actions according to Chapter 2, "Alarm Troubleshooting."

**Step 3** Verify the proper cabling of the COM-RX port (the common input port for all of the drop channels) of the alarmed 32DMX-O:

a. Verify that the COM_RX port of the alarmed 32DMX-O is connected either to the DROP_TX port of a 32WSS card or to the COM_TX port of an OPT-PRE, OPT-BST, or OSC-CSM, depending on the actual node layout.

b. Pull out the LC connector from the COM_RX port of the 32DMX-O card and clean the fiber according to site practice.

c. Pull out the LC connector from the COM_TX or DROP_TX port of the connected DWDM card and clean the fiber according to site practice.

d. Verify that the fiber attenuation is within the specifications (maximum tolerance is 1 dB).

e. If necessary, replace any bad fibers.

**Note** If no site practice exists for cleaning fibers, complete the procedure in the "Maintain the Node" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

f. If the alarm condition persists even after the cabling has been checked and fixed, the root cause could be related to a network issue and a more accurate analysis of the signal flow is needed according to the actual system topology. If necessary, call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.


# Alarm Troubleshooting

**Note** The terms "Unidirectional Path Switched Ring" and "UPSR" may appear in Cisco literature. These terms do not refer to using Cisco ONS 15xxx products in a unidirectional path switched ring configuration. Rather, these terms, as well as "Path Protected Mesh Network" and "PPMN," refer generally to Cisco's path protection feature, which may be used in any topological network configuration. Cisco does not recommend using its path protection feature in any particular topological network configuration.

This chapter gives a description, severity, and troubleshooting procedure for each commonly encountered dense wavelength division multiplexing (DWDM) alarm and condition—whether for trunk or client—used in the Cisco ONS platforms. Tables 2-1 through 2-5 provide lists of DWDM alarms organized by severity. Table 2-6 on page 2-5 provides a list of alarms organized alphabetically. Table 2-7 gives definitions of all DWDM alarm logical objects, which are the basis of the alarm profile list in Table 2-8 on page 2-9.

An alarm's troubleshooting procedure applies to both the Cisco Transport Controller (CTC) and Transaction Language One (TL1) version of that alarm. If the troubleshooting procedure does not clear the alarm, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call the Cisco Technical Assistance Center (1 800 553-2447).

For more information about alarm profiles, refer to the "Manage Alarms" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For a comprehensive list of all conditions and instructions for using TL1 commands, refer to the *Cisco SONET TL1 Command Guide* .

**Note** In this chapter, "ONS 15454" refers to both the SONET and SDH (ETSI) versions of the platform.

## 2.1 Alarm Indexes by Default Severity

The following tables group DWDM alarms and conditions by their default severities in the ONS system system. These severities are the same whether they are reported in the CTC Alarms window severity (SEV) column or in TL1.

**Note** The CTC default alarm profile contains some alarms or conditions that are not currently implemented but are reserved for future use.

**Note** The CTC default alarm profile in some cases contains two severities for one alarm (for example, MJ/MN). The ONS system platform default severity comes first (in this example, MJ), but the alarm can be demoted to the second severity in the presence of a higher-ranking alarm. This is in accordance with Telcordia GR-474.

## 2.1.1 Critical Alarms (CR)

Table 2-1 alphabetically lists Critical (CR) DWDM alarms.

*Table 2-1 Critical DWDM Alarm List*

| | | |
|---|---|---|
| AWG-FAIL (OTS) | LOF (TRUNK) | OPWR-HFAIL (AOTS, OCH, OMS, OTS) |
| AWG-OVERTEMP (OTS) | LOM (TRUNK) | OPWR-LFAIL (AOTS, OCH, OMS, OTS) |
| BKUPMEMP (EQPT) | LOS (2R) | OTUK-LOF (TRUNK) |
| EQPT (AICI-AEP, AICI-AIE, EQPT, PPM) | LOS (ESCON) | OTUK-TIM (TRUNK) |
| EQPT-MISS (FAN) | LOS (ISC) | PORT-ADD-PWR-FAIL-HI (OCH) |
| GAIN-HFAIL (AOTS) | LOS (OTS) | PORT-ADD-PWR-FAIL-LOW (OCH) |
| GAIN-LFAIL (AOTS) | LOS (TRUNK) | PORT-FAIL (OCH) |
| GE-OOSYNC (FC, GE, ISC) | MEA (EQPT) | TIM (TRUNK) |
| GE0OOSYNC (TRUNK) | MEA (PPM) | VOA-HFAIL (AOTS, OCH, OMS, OTS) |
| HITEMP (NE) | MFGMEM (AICI-AEP, AICI-AIE, AIP, BPLANE, FAN, PPM) | VOA-LFAIL (AOTS, OCH, OMS, OTS) |
| IMPROPRMVL (EQPT, PPM) | — | — |

## 2.1.2 Major Alarms (MJ)

Table 2-2 alphabetically lists Major (MJ) DWDM alarms.

*Table 2-2 Major DWDM Alarm List*

| | | |
|---|---|---|
| BAT-FAIL (PWR) | EHIBATVG (PWR) | OPTNTWMIS (NE) |
| CARLOSS (EQPT) | ELWBATVG (PWR) | OUT-OF-SYNC (ISC) |
| CARLOSS (FC) | FEC-MISM (TRUNK) | PEER-NORESPONSE (EQPT) |
| CARLOSS (GE) | HIBATVG (PWR) | PTIM (TRUNK) |
| CARLOSS (ISC) | LASERBIAS-FAIL (AOTS) | RING-ID-MIS (OSC-RING) |
| CARLOSS (TRUNK) | LWBATVG (PWR) | SIGLOSS (FC, GE, ISC, TRUNK) |
| CARLOSS (EQPT) | MEM-GONE (EQPT) | SYNCLOSS (FC, GE, ISC, TRUNK) |
| DSP-COMM-FAIL (TRUNK) | ODUK-TIM-PM (TRUNK) | SYSBOOT (NE) |

## 2.1.3 Minor Alarms (MN)

Table 2-3 alphabetically lists Minor (MN) DWDM alarms.

*Table 2-3 Minor DWDM Alarm List*

| | | |
|---|---|---|
| AUTORESET (EQPT) | INCOMPATIBLE-SW (SYSTEM) | PORT-ADD-PWR-DEG-LOW (OCH) |
| AWG-DEG (OTS) | LASERBIAS-DEG (AOTS, OTS) | PROTNA (EQPT) |
| BPV (BITS) | LASEREOL (OCN/STMN) | PROV-MISMATCH (PPM) |
| CASETEMP-DEG (AOTS) | LASERTEMP-DEG (AOTS) | PWR-FAIL-A (EQPT) |
| DISCONNECTED (SYSTEM) | LOF (BITS) | PWR-FAIL-B (EQPT) |
| DUP-NODENAME (NE) | LOGBUFR90 (SYSTEM) | PWR-FAIL-RET-A (EQPT) |
| EOC (TRUNK) | LOGBUFROVFL (SYSTEM) | PWR-FAIL-RET-B (EQPT) |
| EOC-L (TRUNK) | LO-LASERBIAS (EQPT, OCN/STMN, PPM) | SFTWDOWN (EQPT) |
| EXCCOL (EQPT) | LO-LASERTEMP (EQPT, OCN/STMN, PPM) | SH-INS-LOSS-VAR-DEG-HIGH (OTS) |
| EXT (ENVALRM) | LO-RXPOWER (2R, ESCON, FC, GE, ISC, OCN/STMN, TRUNK) | SH-INS-LOSS-VAR-DEG-LOW (OTS) |
| FIBERTEMP-DEG (AOTS) | LOS (BITS) | SNTP-HOST (NE) |
| GAIN-HDEG (AOTS) | LOS-O (OCH, OMS, OTS) | SSM-FAIL (TRUNK) |
| GAIN-LDEG (AOTS) | LO-TXPOWER (2R, EQPT, ESCON, FC, GE, ISC, OCN/STMN, PPM, TRUNK) | SYNCPRI (EXT-SREF, NE-SREF) |
| GCC-EOC (TRUNK) | MEM-LOW (EQPT) | SYNCSEC (EXT-SREF, NE-SREF) |
| HI-LASERBIAS (2R, EQPT, ESCON, FC, GE, ISC, OCN/STMN, PPM, TRUNK) | NOT-AUTHENTICATED (SYSTEM) | SYNCTHIRD (EXT-SREF, NE-SREF) |
| HI-LASERTEMP (EQPT, OCN/STMN, PPM) | OPWR-HDEG (AOTS, OCH, OMS, OTS) | TIM-MON (TRUNK) |
| HITEMP (EQPT, NE) | OPWR-LDEG (AOTS, OCH, OMS, OTS) | UNREACHABLE-TARGET-POWER (OCH) |
| HI-RXPOWER (2R, ESCON, FC, GE, ISC, OCN/STMN, TRUNK) | OTUK-IAE (TRUNK) | VOA-HDEG (AOTS, OCH, OMS, OTS) |
| HI-TXPOWER (2R, EQPT, ESCON, FC, GE, ISC, OCN/STMN, PPM, TRUNK) | PORT-ADD-PWR-DEG-HI (OCH) | VOA-LDEG (AOTS, OCH, OMS, OTS) |
| INCOMPATIBLE-SEND-PDIP (SYSTEM) | — | — |

## 2.1.4 NA Conditions

Table 2-4 alphabetically lists Not Alarmed (NA) DWDM conditions.

*Table 2-4 NA DWDM Conditions List*

| | | |
|---|---|---|
| ALS (2R, AOTS, ESCON, FC, GE, ISC, OCN/STMN, TRUNK) | LPBKFACILITY (ISC) | SSM-DUS (TRUNK) |
| AMPLI-INIT (AOTS) | LPBKTERMINAL (ESCON) | SSM-LNC (TRUNK) |
| APC-CORRECTION-SKIPPED (AOTS, OCH, OMS, OTS) | LPBKTERMINAL (FC) | SSM-OFF (TRUNK) |
| APC-DISABLED (NE) | LPBKTERMINAL (GE) | SSM-PRC (TRUNK) |
| APC-END (NE) | LPBKTERMINAL (ISC) | SSM-PRS (TRUNK) |
| APC-OUT-OF-RANGE (AOTS, OCH, OMS, OTS) | MAN-REQ (EQPT) | SSM-RES (TRUNK) |
| AS-CMD (2R, AOTS, BPLANE, EQPT, ESCON, FC, GE, ISC, NE, OCH, OCN/STMN, OMS, OTS, PPM, PWR, TRUNK) | MANRESET (EQPT) | SSM-SMC (TRUNK) |
| AS-MT (2R, AOTS, EQPT, ESCON, FC, GE, ISC, OCH, OCN/STMN, OMS, OTS, PPM, TRUNK) | MANSWTOINT (NE-SREF) | SSM-ST2 (TRUNK) |
| AWG-WARM-UP (OTS) | MANSWTOPRI (EXT-SREF, NE-SREF) | SSM-ST3 (TRUNK) |
| FAILTOSW (2R, EQPT, ESCON, FC, GE, ISC, OCN/STMN, TRUNK) | MANSWTOSEC (EXT-SREF, NE-SREF) | SSM-ST3E (TRUNK) |
| FORCED-REQ-SPAN (2R, ESCON, FC, GE, ISC, OCN/STMN, TRUNK) | MANSWTOTHIRD (EXT-SREF, NE-SREF) | SSM-ST4 (TRUNK) |
| FRCDSWTOINT (NE-SREF) | MANUAL-REQ-SPAN (2R, ESCON, FC, GE, ISC, OCN/STMN, TRUNK) | SSM-STU (TRUNK) |
| FRCDSWTOPRI (EXT-SREF, NE-SREF) | OCHNC-INC (OCHNC-CONN) | SSM-TNC (TRUNK) |
| FRCDSWTOSEC (EXT-SREF, NE-SREF) | ODUK-SD-PM (TRUNK) | SWTOPRI (EXT-SREF, NE-SREF) |
| FRCDSWTOTHIRD (EXT-SREF, NE-SREF) | ODUK-SF-PM (TRUNK) | SWTOSEC (EXT-SREF, NE-SREF) |
| FRNGSYNC (NE-SREF) | OPEN-SLOT (EQPT) | SWTOTHIRD (EXT-SREF, NE-SREF) |
| FSTSYNC (NE-SREF) | OSRION (AOTS, OTS) | SYNC-FREQ (TRUNK) |
| HI-CCVOLT (BITS) | OTUK-SD (TRUNK) | TEMP-MISM (NE) |
| HLDOVRSYNC (NE-SREF) | OTUK-SF (TRUNK) | UNC-WORD (TRUNK) |
| INTRUSION-PSWD (NE) | OUT-OF-SYNC (FC, GE, TRUNK) | VOLT-MISM (PWR) |
| LASER-APR (AOTS) | PARAM-MISM (AOTS, OCH, OMS, OTS) | WKSWPR (2R, EQPT, ESCON, FC, GE, ISC) |
| LOCKOUT-REQ (2R, EQPT, ESCON, FC, GE, ISC, OCN/STMN, TRUNK) | SD (TRUNK) | WKSWPR (TRUNK) |
| LPBKFACILITY (ESCON) | SF (TRUNK) | WTR (2R, EQPT, ESCON, FC, GE, ISC) |

*Table 2-4 NA DWDM Conditions List (continued)*

| | | |
|---|---|---|
| LPBKFACILITY (FC) | SHUTTER-OPEN (OTS) | WTR (TRUNK) |
| LPBKFACILITY (GE) | SQUELCHED (2R, ESCON, FC, GE, ISC, OCN/STMN, TRUNK) | — |

## 2.1.5 NR Conditions

Table 2-5 alphabetically lists Not Reported (NR) DWDM conditions.

*Table 2-5 NR DWDM Conditions List*

| | | |
|---|---|---|
| AIS (TRUNK) | ODUK-4-AIS-PM (TRUNK) | ODUK-OCI-PM (TRUNK) |
| ODUK-1-AIS-PM (TRUNK) | ODUK-AIS-PM (TRUNK) | OTUK-AIS (TRUNK) |
| ODUK-2-AIS-PM (TRUNK) | ODUK-BDI-PM (TRUNK) | OTUK-BDI (TRUNK) |
| ODUK-3-AIS-PM (TRUNK) | ODUK-LCK-PM (TRUNK) | RFI (TRUNK) |

# 2.2 Alarms and Conditions Listed By Alphabetical Entry

Table 2-6 alphabetically lists all ONS DWDM alarms and conditions.

*Table 2-6 Alphabetical List of DWDM Alarms and Condition s*

| | | |
|---|---|---|
| AIS (TRUNK) | LASERBIAS-FAIL (AOTS) | OTUK-LOF (TRUNK) |
| ALS (2R, AOTS, ESCON, FC, GE, ISC, OCN/STMN, TRUNK) | LASEREOL (OCN/STMN) | OTUK-SD (TRUNK) |
| AMPLI-INIT (AOTS) | LASERTEMP-DEG (AOTS) | OTUK-SF (TRUNK) |
| APC-CORRECTION-SKIPPED (AOTS, OCH, OMS, OTS) | LOCKOUT-REQ (2R, EQPT, ESCON, FC, GE, ISC, OCN/STMN, TRUNK) | OTUK-TIM (TRUNK) |
| APC-DISABLED (NE) | LOF (BITS) | OUT-OF-SYNC (FC, GE, ISC, TRUNK) |
| APC-END (NE) | LOF (TRUNK) | PARAM-MISM (AOTS, OCH, OMS, OTS) |
| APC-OUT-OF-RANGE (AOTS, OCH, OMS, OTS) | LOGBUFR90 (SYSTEM) | PEER-NORESPONSE (EQPT) |
| AS-CMD (2R, AOTS, BPLANE, EQPT, ESCON, FC, GE, ISC, NE, OCH, OCN/STMN, OMS, OTS, PPM, PWR, TRUNK) | LOGBUFROVFL (SYSTEM) | PORT-ADD-PWR-DEG-HI (OCH) |
| AS-MT (2R, AOTS, EQPT, ESCON, FC, GE, ISC, OCH, OCN/STMN, OMS, OTS, PPM, TRUNK) | LO-LASERBIAS (EQPT, OCN/STMN, PPM) | PORT-ADD-PWR-DEG-LOW (OCH) |
| AUTORESET (EQPT) | LO-LASERTEMP (EQPT, OCN/STMN, PPM) | PORT-ADD-PWR-FAIL-HI (OCH) |

*Table 2-6 Alphabetical List of DWDM Alarms and Condition s (continued)*

| | | |
|---|---|---|
| AWG-DEG (OTS) | LOM (TRUNK) | PORT-ADD-PWR-FAIL-LOW (OCH) |
| AWG-FAIL (OTS) | LO-RXPOWER (2R, ESCON, FC, GE, ISC, OCN/STMN, TRUNK) | PORT-FAIL (OCH) |
| AWG-OVERTEMP (OTS) | LOS (2R) | PROTNA (EQPT) |
| AWG-WARM-UP (OTS) | LOS (BITS) | PROV-MISMATCH (PPM) |
| BAT-FAIL (PWR) | LOS (ESCON) | PTIM (TRUNK) |
| BKUPMEMP (EQPT) | LOS (ISC) | PWR-FAIL-A (EQPT) |
| BPV (BITS) | LOS (OTS) | PWR-FAIL-B (EQPT) |
| CARLOSS (EQPT) | LOS (TRUNK) | PWR-FAIL-RET-A (EQPT) |
| CARLOSS (FC) | LOS-O (OCH, OMS, OTS) | PWR-FAIL-RET-B (EQPT) |
| CARLOSS (GE) | LOS-P (AOTS, OMS,OTS) | RFI (TRUNK) |
| CARLOSS (ISC) | LOS-P (OCH) | RING-ID-MIS (OSC-RING) |
| CARLOSS (TRUNK) | LOS-P (TRUNK) | SD (TRUNK) |
| CASETEMP-DEG (AOTS) | LO-TXPOWER (2R, EQPT, ESCON, FC, GE, ISC, OCN/STMN, PPM, TRUNK) | SF (TRUNK) |
| CARLOSS (EQPT) | LPBKFACILITY (ESCON) | SFTWDOWN (EQPT) |
| DISCONNECTED (SYSTEM) | LPBKFACILITY (FC) | SH-INS-LOSS-VAR-DEG-HIGH (OTS) |
| DSP-COMM-FAIL(TRUNK) | LPBKFACILITY (GE) | SH-INS-LOSS-VAR-DEG-LOW (OTS) |
| DSP-FAIL (TRUNK) | LPBKFACILITY (ISC) | SHUTTER-OPEN (OTS) |
| DUP-IPADDR (NE) | LPBKFACILITY (TRUNK) | SIGLOSS (FC, GE, ISC, TRUNK) |
| DUP-NODENAME (NE) | LPBKTERMINAL (ESCON) | SYNCLOSS (FC, GE, ISC, TRUNK) |
| EHIBATVG (PWR) | LPBKTERMINAL (FC) | SNTP-HOST (NE) |
| ELWBATVG (PWR) | LPBKTERMINAL (GE) | SQUELCHED (2R, ESCON, FC, GE, ISC, OCN/STMN, TRUNK) |
| EOC (TRUNK) | LPBKTERMINAL (ISC) | SSM-DUS (TRUNK) |
| EOC-L (TRUNK) | LPBKTERMINAL (TRUNK) | SSM-FAIL (TRUNK) |
| EQPT (AICI-AEP, AICI-AIE, EQPT, PPM) | LWBATVG (PWR) | SSM-LNC (TRUNK) |
| EQPT-MISS (FAN) | MAN-REQ (EQPT) | SSM-OFF (TRUNK) |
| EXCCOL (EQPT) | MANRESET (EQPT) | SSM-PRC (TRUNK) |
| EXT (ENVALRM) | MANSWTOINT(NE-SREF) | SSM-PRS (TRUNK) |
| FAILTOSW (2R, EQPT, ESCON, FC, GE, ISC, OCN/STMN, TRUNK) | MANSWTOPRI (EXT-SREF, NE-SREF) | SSM-RES (TRUNK) |
| FEC-MISM (TRUNK) | MANSWTOSEC (EXT-SREF, NE-SREF) | SSM-SMC (TRUNK) |
| FIBERTEMP-DEG (AOTS) | MANSWTOTHIRD (EXT-SREF, NE-SREF) | SSM-ST2 (TRUNK) |
| FORCED-REQ-SPAN (2R, ESCON, FC, GE, ISC, OCN/STMN, TRUNK) | MANUAL-REQ-SPAN (2R, ESCON, FC, GE, ISC, OCN/STMN, TRUNK) | SSM-ST3 (TRUNK) |

*Table 2-6 Alphabetical List of DWDM Alarms and Condition s (continued)*

| | | |
|---|---|---|
| FRCDSWTOINT (NE-SREF) | MEA (EQPT) | SSM-ST3E (TRUNK) |
| FRCDSWTOPRI (EXT-SREF, NE-SREF) | MEA (FAN) | SSM-ST4 (TRUNK) |
| FRCDSWTOSEC (EXT-SREF, NE-SREF) | MEA (PPM) | SSM-STU (TRUNK) |
| FRCDSWTOTHIRD (EXT-SREF, NE-SREF) | MEM-GONE (EQPT) | SSM-TNC (TRUNK) |
| FRNGSYNC (NE-SREF) | MEM-LOW (EQPT) | SWTOPRI (EXT-SREF, NE-SREF) |
| FSTSYNC (NE-SREF) | MFGMEM (AICI-AEP, AICI-AIE, AIP, BPLANE, FAN, PPM) | SWTOSEC (EXT-SREF, NE-SREF) |
| GAIN-HDEG (AOTS) | NOT-AUTHENTICATED (SYSTEM) | SWTOTHIRD (EXT-SREF, NE-SREF) |
| GAIN-HFAIL (AOTS) | OCHNC-INC (OCHNC-CONN) | SYNC-FREQ (TRUNK) |
| GAIN-LDEG (AOTS) | ODUK-1-AIS-PM (TRUNK) | SYNCPRI (EXT-SREF, NE-SREF) |
| GAIN-LFAIL (AOTS) | ODUK-2-AIS-PM (TRUNK) | SYNCSEC (EXT-SREF, NE-SREF) |
| GCC-EOC (TRUNK) | ODUK-3-AIS-PM (TRUNK) | SYNCTHIRD (EXT-SREF, NE-SREF) |
| GE-OOSYNC (FC, GE, ISC) | ODUK-4-AIS-PM (TRUNK) | SYSBOOT (NE) |
| GE-OOSYNC (TRUNK) | ODUK-AIS-PM (TRUNK) | TEMP-MISM (NE) |
| HIBATVG (PWR) | ODUK-BDI-PM (TRUNK) | TIM (TRUNK) |
| HI-CCVOLT (BITS) | ODUK-LCK-PM (TRUNK) | TIM-MON (TRUNK) |
| HI-LASERBIAS (2R, EQPT, ESCON, FC, GE, ISC, OCN/STMN, PPM, TRUNK) | ODUK-OCI-PM (TRUNK) | UNC-WORD (TRUNK) |
| HI-LASERTEMP (QPT, OCN/STMN, PPM) | ODUK-SD-PM (TRUNK) | UNREACHABLE-TARGET-POWER (OCH) |
| HI-RXPOWER (2R, ESCON, FC, GE, ISC, OCN/STMN, TRUNK) | ODUK-SF-PM (TRUNK) | UT-COMM-FAIL (TRUNK) |
| HITEMP (EQPT, NE) | ODUK-TIM-PM (TRUNK) | UT-FAIL (TRUNK) |
| HI-TXPOWER (2R, EQPT, ESCON, FC, GE, ISC, OCN/STMN, PPM, TRUNK) | OPEN-SLOT (EQPT) | VOA-HDEG (AOTS, OCH, OMS, OTS) |
| HLDOVRSYNC (NE-SREF) | OPTNTWMIS (NE) | VOA-HFAIL (AOTS, OCH, OMS, OTS) |
| I-HITEMP (NE) | OPWR-HDEG (AOTS, OCH, OMS, OTS) | VOA-LDEG (AOTS, OCH, OMS, OTS) |
| IMPROPRMVL (EQPT, PPM) | OPWR-HFAIL (AOTS, OCH, OMS, OTS) | VOA-LFAIL (AOTS, OCH, OMS, OTS) |
| INCOMPATIBLE-SEND-PDIP (SYSTEM) | OPWR-LDEG (AOTS, OCH, OMS, OTS) | VOLT-MISM (PWR) |
| INCOMPATIBLE-SW (SYSTEM) | OPWR-LFAIL (AOTS, OCH, OMS, OTS) | WKSWPR (2R, EQPT, ESCON, FC, GE, ISC) |
| INTRUSION-PSWD (NE) | OSRION (AOTS, OTS) | WKSWPR (TRUNK) |
| INVMACADR (AIP) | OTUK-AIS (TRUNK) | WTR (2R, EQPT, ESCON, FC, GE, ISC) |
| LASER-APR (AOTS) | OTUK-BDI (TRUNK) | WTR (TRUNK) |
| LASERBIAS-DEG (AOTS, OTS) | OTUK-IAE (TRUNK) | WVL-MISMATCH (TRUNK) |

# 2.3 Alarm Logical Objects

Alarm logical objects names are part of the organization system used in the CTC alarm profile list. These objects are the software entities that alarms or conditions are raised against and are used to distinguish one kind of alarm—such an equipment alarm (EQPT)—from another, such as a optical transport overhead (OTS).

An alarm can appear in multiple entries if it is raised against multiple objects. For example, the loss of signal (LOS) alarm can be raised against the OTS as well as the trunk object. Therefore, both OTS: LOS and TRUNK: LOS could appear in the list.

Alarm profile list objects are defined in Table 2-7.

*Table 2-7 Logical Object Definitions Applicable to DWDM Alarms*

| Logical Object | Definition |
|---|---|
| **2R** | Reshape and retransmit (used for transponder [TXP] cards). |
| **AICI-AEP** | Alarm Interface Controller–International/alarm expansion panel. A combination term that refers to this platform’s AIC-I card. |
| **AICI-AIE** | Alarm Interface Controller-International/Alarm Interface Extension. A combination term that refers to this platform's AIC-I card. |
| **AIP** | Alarm Interface Panel. |
| **AOTS** | Amplified optical transport section. |
| **BITS** | Building integrated timing supply incoming references (BITS-1, BITS-2). |
| **BPLANE** | The backplane. |
| **ENVALRM** | An environmental alarm port. |
| **EQPT** | A card, its physical objects, and its logical objects as they are located in any of the eight noncommon card slots. The EQPT object is used for alarms that refer to the card itself and all other objects on the card including ports, lines, synchronous transport signals (STS), and Virtual Tributaries (VT). EQPT alarms also apply specifically to various platforms and are addressed in each of these documentation sets. |
| **ESCON** | Enterprise System Connection fiber optic technology, referring to the following TXP cards: TXP_MR_2.5G, TXPP_MR_2.5G. |
| **EXT-SREF** | BITS outgoing references (SYNC-BITS1, SYNC-BITS2). |
| **FAN** | Fan-tray assembly. |
| **FC** | Fibre Channel data transfer architecture, referring to the following muxponder (MXP) or TXP cards: MXP_MR_2.5G, MXPP_MR_2.5G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E. |
| **GE** | Gigabit Ethernet, referring to the following MXP or TXP cards: MXP_MR_2.5G, MXPP_MR_2.5G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, TXP_MR_10G. |
| **ISC** | Inter-service channel, referring to TXPP_MR_2.5G and TXP_MR_2.5G cards. |
| **NE** | The entire network element. |
| **NE-SREF** | The timing status of the NE. |
| **OCH** | The optical channel, referring to DWDM cards. |

*Table 2-7 Logical Object Definitions Applicable to DWDM Alarms (continued)*

| Logical Object | Definition |
|---|---|
| **OCN** | An OC-N line on an OC-N card, referring to the optical clients. |
| **OCHNC-CONN** | The optical channel network connection, referring to DWDM cards. |
| **OMS** | Optical multiplex section. |
| **OSC-RING** | Optical service channel ring. |
| **OTS** | Optical transport section. |
| **PPM** | Pluggable port module (PPM, also called a Small Form-factor Pluggable, or SFP), referring to MXP and TXP cards. |
| **PWR** | Power equipment. |
| **STMN** | An OC-N line on an OC-N card. |
| **SYSTEM** | Pertaining to the CTC software system itself; not always visible in the interface. |
| **TRUNK** | The optical or DWDM card carrying the high-speed signal; referring to MXP or TXP cards. |

# 2.4 Alarm List by Logical Object Type

Table 2-8 lists all ONS system Release 6.0 DWDM-related alarms and logical objects as they are given in the system alarm profile. The list entries are organized by logical object name and then by alarm or condition name. Where appropriate, the alarm entries also contain troubleshooting procedures.

**Note** In a mixed network containing different types of nodes (for example, ONS 15310-CL, ONS 15454, and ONS 15600), the initially displayed alarm list in the Provisioning > Alarm Profiles > Alarm Profile Editor tab lists all conditions that are applicable to all nodes in the network. However, when you load the default severity profile from a node, only applicable alarms will display severity levels. Nonapplicable alarms can display “use default” or “unset.”

*Table 2-8 Alarm List by Logical Object*

| | | |
|---|---|---|
| 2R: ALS | FC: SIGLOSS | OTS: AWG-FAIL |
| 2R: AS-CMD | FC: SYNCLOSS | OTS: AWG-OVERTEMP |
| 2R: AS-MT | FC: SQUELCHED | OTS: AWG-WARM-UP |
| 2R: FAILTOSW | FC: WKSWPR | OTS: LASERBIAS-DEG |
| 2R: FORCED-REQ-SPAN | FC: WTR | OTS: LOS |
| 2R: HI-LASERBIAS | GE: ALS | OTS: LOS-O |
| 2R: HI-RXPOWER | GE: AS-CMD | OTS: LOS-P |
| 2R: HI-TXPOWER | GE: AS-MT | OTS: OPWR-HDEG |
| 2R: LOCKOUT-REQ | GE: CARLOSS | OTS: OPWR-HFAIL |
| 2R: LO-RXPOWER | GE: FAILTOSW | OTS: OPWR-LDEG |
| 2R: LOS | GE: FORCED-REQ-SPAN | OTS: OPWR-LFAIL |
| 2R: LO-TXPOWER | GE: GE-OOSYNC | OTS: OSRION |

*Table 2-8 Alarm List by Logical Object (continued)*

| | | |
|---|---|---|
| 2R: MANUAL-REQ-SPAN | GE: HI-LASERBIAS | OTS: PARAM-MISM |
| 2R: SQUELCHED | GE: HI-RXPOWER | OTS: SH-INS-LOSS-VAR-DEG-HIGH |
| 2R: WKSWPR | GE: HI-TXPOWER | OTS: SH-INS-LOSS-VAR-DEG-LOW |
| 2R:WTR | GE: LOCKOUT-REQ | OTS: SHUTTER-OPEN |
| AICI-AEP: EQPT | GE: LO-RXPOWER | OTS: VOA-HDEG |
| AICI-AEP: MFGMEM | GE: LO-TXPOWER | OTS: VOA-HFAIL |
| AICI-AIE: EQPT | GE: LPBKFACILITY | OTS: VOA-LDEG |
| AICI-AIE: MFGMEM | GE: LPBKTERMINAL | OTS: VOA-LFAIL |
| AIP: INVMACADR | GE: MANUAL-REQ-SPAN | PPM: AS-CMD |
| AIP: MEA | GE: OUT-OF-SYNC | PPM: AS-MT |
| AIP: MFGMEM | GE: SIGLOSS | PPM: EQPT |
| AOTS: ALS | GE: SYNCLOSS | PPM: HI-LASERBIAS |
| AOTS: AMPLI-INIT | GE: SQUELCHED | PPM: HI-LASERTEMP |
| AOTS: APC-CORRECTION-SKIPPED | GE: WKSWPR | PPM: HI-TXPOWER |
| AOTS: APC-OUT-OF-RANGE | GE: WTR | PPM: IMPROPRMVL |
| AOTS: AS-CMD | ISC: ALS | PPM: LO-LASERBIAS |
| AOTS: AS-MT | ISC: AS-CMD | PPM: LO-LASERTEMP |
| AOTS: CASETEMP-DEG | ISC: AS-MT | PPM: LO-TXPOWER |
| AOTS: FIBERTEMP-DEG | ISC: CARLOSS | PPM: MEA |
| AOTS: GAIN-HDEG | ISC: FAILTOSW | PPM: MFGMEM |
| AOTS: GAIN-HFAIL | ISC: FORCED-REQ-SPAN | PPM: PROV-MISMATCH |
| AOTS: GAIN-LDEG | ISC: GE-OOSYNC | PWR: AS-CMD |
| AOTS: GAIN-LFAIL | ISC: HI-LASERBIAS | PWR: BAT-FAIL |
| AOTS: LASER-APR | ISC: HI-RXPOWER | PWR: EHIBATVG |
| AOTS: LASERBIAS-DEG | ISC: HI-TXPOWER | PWR: ELWBATVG |
| AOTS: LASERBIAS-FAIL | ISC: LOCKOUT-REQ | PWR: HIBATVG |
| AOTS: LASERTEMP-DEG | ISC: LO-RXPOWER | PWR: LWBATVG |
| AOTS: LOS-P | ISC: LOS | PWR: VOLT-MISM |
| AOTS: OPWR-HDEG | ISC: LO-TXPOWER | STMN: ALS |
| AOTS: OPWR-HFAIL | ISC: LPBKFACILITY | STMN: AS-CMD |
| AOTS: OPWR-LDEG | ISC: LPBKTERMINAL | STMN: AS-MT |
| AOTS: OPWR-LFAIL | ISC: MANUAL-REQ-SPAN | STMN: FAILTOSW |
| AOTS: OSRION | ISC: OUT-OF-SYNC | STMN: FORCED-REQ-SPAN |
| AOTS: PARAM-MISM | ISC: SIGLOSS | STMN: HI-LASERBIAS |
| AOTS: VOA-HDEG | ISC: SYNCLOSS | STMN: HI-LASERTEMP |
| AOTS: VOA-HFAIL | ISC: SQUELCHED | STMN: HI-RXPOWER |

*Table 2-8 Alarm List by Logical Object (continued)*

| | | |
|---|---|---|
| AOTS: VOA-LDEG | ISC: WKSWPR | STMN: HI-TXPOWER |
| AOTS: VOA-LFAIL | ISC: WTR | STMN: LASEREOL |
| BITS: BPV | NE: APC-DISABLED | STMN: LOCKOUT-REQ |
| BITS: HI-CCVOLT | NE: APC-END | STMN: LO-LASERBIAS |
| BITS: LOF | NE: AS-CMD | STMN: LO-LASERTEMP |
| BITS: LOS | NE: DUP-IPADDR | STMN: LO-RXPOWER |
| BPLANE: AS-CMD | NE: DUP-NODENAME | STMN: LO-TXPOWER |
| BPLANE: MFGMEM | NE: HITEMP | STMN: MANUAL-REQ-SPAN |
| ENVALRM: EXT | NE: I-HITEMP | STMN: SQUELCHED |
| EQPT: AS-CMD | NE: INTRUSION-PSWD | SYSTEM: DISCONNECTED |
| EQPT: AS-MT | NE: OPTNTWMIS | SYSTEM: INCOMPATIBLE-SEND-PDIP |
| EQPT: AUTORESET | NE: SNTP-HOST | SYSTEM: INCOMPATIBLE-SW |
| EQPT: BKUPMEMP | NE: SYSBOOT | SYSTEM: LOGBUFR90 |
| EQPT: CARLOSS | NE: TEMP-MISM | SYSTEM: LOGBUFROVFL |
| EQPT: CARLOSS | NE-SREF: FRCDSWTOINT | SYSTEM: NOT-AUTHENTICATED |
| EQPT: EQPT | NE-SREF: FRCDSWTOPRI | TRUNK: AIS |
| EQPT: EXCCOL | NE-SREF: FRCDSWTOSEC | TRUNK: ALS |
| EQPT: FAILTOSW | NE-SREF: FRCDSWTOTHIRD | TRUNK: AS-CMD |
| EQPT: HI-LASERBIAS | NE-SREF: FRNGSYNC | TRUNK: AS-MT |
| EQPT: HI-LASERTEMP | NE-SREF: FSTSYNC | TRUNK: CARLOSS |
| EQPT: HITEMP | NE-SREF: HLDOVRSYNC | TRUNK: DSP-COMM-FAIL |
| EQPT: HI-TXPOWER | NE-SREF: MANSWTOINT | TRUNK: DSP-FAIL |
| EQPT: IMPROPRMVL | NE-SREF: MANSWTOPRI | TRUNK: EOC |
| EQPT: LOCKOUT-REQ | NE-SREF: MANSWTOSEC | TRUNK: EOC-L |
| EQPT: LO-LASERBIAS | NE-SREF: MANSWTOTHIRD | TRUNK: FAILTOSW |
| EQPT: LO-LASERTEMP | NE-SREF: SWTOPRI | TRUNK: FEC-MISM |
| EQPT: LO-TXPOWER | NE-SREF: SWTOSEC | TRUNK: FORCED-REQ-SPAN |
| EQPT: MAN-REQ | NE-SREF: SWTOTHIRD | TRUNK: GCC-EOC |
| EQPT: MANRESET | NE-SREF: SYNCPRI | TRUNK: GE-OOSYNC |
| EQPT: MEA | NE-SREF: SYNCSEC | TRUNK: HI-LASERBIAS |
| EQPT: MEM-GONE | NE-SREF: SYNCTHIRD | TRUNK: HI-RXPOWER |
| EQPT: MEM-LOW | OCH: APC-CORRECTION-SKIPPED | TRUNK: HI-TXPOWER |
| EQPT: OPEN-SLOT | OCH: APC-OUT-OF-RANGE | TRUNK: LOCKOUT-REQ |
| EQPT: PEER-NORESPONSE | OCH: AS-CMD | TRUNK: LOF |
| EQPT: PROTNA | OCH: AS-MT | TRUNK: LOM |
| EQPT: PWR-FAIL-A | OCH: LOS-O | TRUNK: LO-RXPOWER |

*Table 2-8 Alarm List by Logical Object (continued)*

| | | |
|---|---|---|
| EQPT: PWR-FAIL-B | OCH: LOS-P | TRUNK: LOS |
| EQPT: PWR-FAIL-RET-A | OCH: OPWR-HDEG | TRUNK: LOS-P |
| EQPT: PWR-FAIL-RET-B | OCH: OPWR-HFAIL | TRUNK: LO-TXPOWER |
| EQPT: SFTWDOWN | OCH: OPWR-LDEG | TRUNK: LPBKFACILITY |
| EQPT: WKSWPR | OCH: OPWR-LFAIL | TRUNK: LPBKTERMINAL |
| EQPT: WTR | OCH: PARAM-MISM | TRUNK: MANUAL-REQ-SPAN |
| ESCON: ALS | OCH: PORT-ADD-PWR-DEG-HI | TRUNK: ODUK-1-AIS-PM |
| ESCON: AS-CMD | OCH: PORT-ADD-PWR-DEG-LOW | TRUNK: ODUK-2-AIS-PM |
| ESCON: AS-MT | OCH: PORT-ADD-PWR-FAIL-HI | TRUNK: ODUK-3-AIS-PM |
| ESCON: FAILTOSW | OCH: PORT-ADD-PWR-FAIL-LOW | TRUNK: ODUK-4-AIS-PM |
| ESCON: FORCED-REQ-SPAN | OCH: PORT-FAIL | TRUNK: ODUK-AIS-PM |
| ESCON: HI-LASERBIAS | OCH: UNREACHABLE-TARGET-POWER | TRUNK: ODUK-BDI-PM |
| ESCON: HI-RXPOWER | OCH: VOA-HDEG | TRUNK: ODUK-LCK-PM |
| ESCON: HI-TXPOWER | OCH: VOA-HFAIL | TRUNK: ODUK-OCI-PM |
| ESCON: LOCKOUT-REQ | OCH: VOA-LDEG | TRUNK: ODUK-SD-PM |
| ESCON: LO-RXPOWER | OCH: VOA-LFAIL | TRUNK: ODUK-SF-PM |
| ESCON: LOS | OCHNC-CONN: OCHNC-INC | TRUNK: ODUK-TIM-PM |
| ESCON: LO-TXPOWER | OCN: ALS | TRUNK: OTUK-AIS |
| ESCON: LPBKFACILITY | OCN: AS-CMD | TRUNK: OTUK-BDI |
| ESCON: LPBKTERMINAL | OCN: AS-MT | TRUNK: OTUK-IAE |
| ESCON: MANUAL-REQ-SPAN | OCN: FAILTOSW | TRUNK: OTUK-LOF |
| ESCON: SQUELCHED | OCN: FORCED-REQ-SPAN | TRUNK: OTUK-SD |
| ESCON: WKSWPR | OCN: HI-LASERBIAS | TRUNK: OTUK-SF |
| ESCON: WTR | OCN: HI-LASERTEMP | TRUNK: OTUK-TIM |
| EXT-SREF: FRCDSWTOPRI | OCN: HI-RXPOWER | TRUNK: OUT-OF-SYNC |
| EXT-SREF: FRCDSWTOSEC | OCN: HI-TXPOWER | TRUNK: PTIM |
| EXT-SREF: FRCDSWTOTHIRD | OCN: LASEREOL | TRUNK: RFI |
| EXT-SREF: MANSWTOPRI | OCN: LOCKOUT-REQ | TRUNK: SD |
| EXT-SREF: MANSWTOSEC | OCN: LO-LASERBIAS | TRUNK: SF |
| EXT-SREF: MANSWTOTHIRD | OCN: LO-LASERTEMP | TRUNK: SIGLOSS |
| EXT-SREF: SWTOPRI | OCN: LO-RXPOWER | TRUNK: SYNCLOSS |
| EXT-SREF: SWTOSEC | OCN: LO-TXPOWER | TRUNK: SQUELCHED |
| EXT-SREF: SWTOTHIRD | OCN: MANUAL-REQ-SPAN | TRUNK: SSM-DUS |
| EXT-SREF: SYNCPRI | OCN: SQUELCHED | TRUNK: SSM-FAIL |
| EXT-SREF: SYNCSEC | OMS: APC-CORRECTION-SKIPPED | TRUNK: SSM-LNC |
| EXT-SREF: SYNCTHIRD | OMS: APC-OUT-OF-RANGE | TRUNK: SSM-OFF |

*Table 2-8 Alarm List by Logical Object (continued)*

| | | |
|---|---|---|
| FAN: EQPT-MISS | OMS: AS-CMD | TRUNK: SSM-PRC |
| FAN: MEA | OMS: AS-MT | TRUNK: SSM-PRS |
| FAN: MFGMEM | OMS: LOS-O | TRUNK: SSM-RES |
| FC: ALS | OMS: LOS-P | TRUNK: SSM-SMC |
| FC: AS-CMD | OMS: OPWR-HDEG | TRUNK: SSM-ST2 |
| FC: AS-MT | OMS: OPWR-HFAIL | TRUNK: SSM-ST3 |
| FC: CARLOSS | OMS: OPWR-LDEG | TRUNK: SSM-ST3E |
| FC: FAILTOSW | OMS: OPWR-LFAIL | TRUNK: SSM-ST4 |
| FC: FORCED-REQ-SPAN | OMS: PARAM-MISM | TRUNK: SSM-STU |
| FC: GE-OOSYNC | OMS: VOA-HDEG | TRUNK: SSM-TNC |
| FC: HI-LASERBIAS | OMS: VOA-HFAIL | TRUNK: SYNC-FREQ |
| FC: HI-RXPOWER | OMS: VOA-LDEG | TRUNK: TIM |
| FC: HI-TXPOWER | OMS: VOA-LFAIL | TRUNK: TIM-MON |
| FC: LOCKOUT-REQ | OSC-RING: RING-ID-MIS | TRUNK: UNC-WORD |
| FC: LO-RXPOWER | OTS: APC-CORRECTION-SKIPPED | TRUNK: UT-COMM-FAIL |
| FC: LO-TXPOWER | OTS: APC-OUT-OF-RANGE | TRUNK: UT-FAIL |
| FC: LPBKFACILITY | OTS: AS-CMD | TRUNK: WKSWPR |
| FC: LPBKTERMINAL | OTS: AS-MT | TRUNK: WTR |
| FC: MANUAL-REQ-SPAN | OTS: AWG-DEG | TRUNK: WVL-MISMATCH |
| FC: OUT-OF-SYNC | — | — |

# 2.5 Trouble Notifications

The ONS system reports trouble by utilizing standard alarm and condition characteristics, standard severities following the rules in Telcordia GR-253-CORE, and graphical user interface (GUI) state indicators.These notifications are described in the following paragraphs.

The ONS DWDM system uses standard Telcordia categories to characterize levels of trouble. The system reports trouble notifications as alarms and status or descriptive notifications (if configured to do so) as conditions in the CTC Alarms window. Alarms typically signify a problem that the user needs to remedy, such as a loss of signal. Conditions do not necessarily require troubleshooting.

## 2.5.1 Alarm Characteristics

The ONS DWDM uses standard alarm entities to identify what is causing trouble. All alarms stem from hardware, software, environment, or operator-originated problems whether or not they affect service. Current alarms for the network, CTC session, node, or card are listed in the Alarms tab. (In addition, cleared alarms are also found in the History tab.)

### 2.5.2 Condition Characteristics

Conditions include any problem detected on an ONS system shelf. They can include standing or transient notifications. A snapshot of all current raised, standing conditions on the network, node, or card can be retrieved in the CTC Conditions window or using TL1's set of RTRV-COND commands. (In addition, some but not all cleared conditions are also found in the History tab.)

For a comprehensive list of all conditions, refer to the *Cisco SONET TL1 Command Guide* .

### 2.5.3 Severities

The ONS DWDM system uses Telcordia GR-474-CORE standard severities for alarms and conditions: Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), and Not Reported (NR). These are described as follows:

- A Critical (CR) alarm generally indicates severe, Service-Affecting (SA) trouble that needs immediate correction. Loss of traffic on an STS-1, which can hold 28 DS-1 circuits, would be a Critical (CR), Service-Affecting (SA) alarm.
- A Major (MJ) alarm is a serious alarm, but the trouble has less impact on the network. For example, loss of traffic on more than five DS-1 circuits is Critical (CR), but loss of traffic on one to four DS-1 circuits is Major (MJ).
- Minor (MN) alarms generally are those that do not affect service. For example, the automatic protection switching (APS) byte failure (APSB) alarm indicates that line terminating equipment (LTE) detects a byte failure on the signal that could prevent traffic from properly executing a traffic switch.
- Not Alarmed (NA) conditions are information indicators, such as for free-run synchronization state (FRNGSYNC) or a forced-switch to primary (FRCSWTOPRI) timing event. They could or could not require troubleshooting, as indicated in the entries.
- Not Reported (NR) conditions occur as a secondary result of another event. For example, the alarm indication signal (AIS), with severity NR, is inserted by a downstream node when an LOS (CR or MJ) alarm occurs upstream. These conditions do not in themselves require troubleshooting, but are to be expected in the presence of primary alarms.

Severities can be customized for an entire network or for single nodes, from the network level down to the port level by changing or downloading customized alarm profiles. These custom severities are subject to the standard severity-demoting rules given in Telcordia GR-474-CORE and shown in the 2.5.4 Service Effect section. Procedures for customizing alarm severities are located in the "Manage Alarms" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

### 2.5.4 Service Effect

Service-Affecting (SA) alarms—those that interrupt service—could be Critical (CR), Major (MJ), or Minor (MN) severity alarms. Service-Affecting (SA) alarms indicate service is affected. Non-Service-Affecting (NSA) alarms always have a Minor (MN) default severity.

### 2.5.5 States

The Alarms or History tab State (ST) column indicate the disposition of the alarm or condition as follows:

- A raised (R) event is one that is active.
- A cleared (C) event is one that is no longer active.
- A transient (T) event is one that is automatically raised and cleared in CTC during system changes such as user login, logout, loss of connection to node view, etc. Transient events do not require user action. These are listed in Chapter 3, "Transients Conditions."

## 2.6 Safety Summary

This section covers safety considerations designed to ensure safe operation of the ONS system. Personnel should not perform any procedures in this chapter unless they understand all safety precautions, practices, and warnings for the system equipment. Some troubleshooting procedures require installation or removal of cards; in these instances users should pay close attention to the following caution.

**Caution** Hazardous voltage or energy could be present on the backplane when the system is operating. Use caution when removing or installing cards.

Some troubleshooting procedures require installation or removal of OC-192 cards; in these instances users should pay close attention to the following warnings.

**Warning** **On the OC-192 card, the laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. The laser is off when the safety key is off (labeled 0).** Statement 293

**Warning** **Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard.** Statement 1056

**Warning** **Use of controls, adjustments, or performing procedures other than those specified could result in hazardous radiation exposure.** Statement 1057

**Warning** **Class 1 laser product.** Statement 1008

**Warning** **Do not reach into a vacant slot or chassis while you install or remove a module or a fan. Exposed circuitry could constitute an energy hazard.** Statement 206

**Warning** **The power supply circuitry for the equipment can constitute an energy hazard. Before you install or replace the equipment, remove all jewelry (including rings, necklaces, and watches). Metal objects can come into contact with exposed power supply wiring or circuitry inside the DSLAM equipment. This could cause the metal objects to heat up and cause serious burns or weld the metal object to the equipment.** Statement 207

# 2.7 Alarm Procedures

This section list alarms alphabetically and includes some conditions commonly encountered when troubleshooting alarms. The severity, description, and troubleshooting procedure accompany each alarm and condition.

**Note** When you check the status of alarms for cards, ensure that the alarm filter icon in the lower right corner of the GUI is not indented. If it is, click it to turn it off. When you are done checking for alarms, you can click the alarm filter icon again to turn filtering back on. For more information about alarm filtering, refer to the "Manage Alarms" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Note** When checking alarms, ensure that alarm suppression is not enabled on the card or port. For more information about alarm suppression, refer to the "Manage Alarms" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide.*

## 2.7.1 AIS

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

Logical Objects: TRUNK

The Alarm Indication Signal (AIS) condition indicates that this node is detecting an alarm indication signal in the incoming signal SONET overhead.

Generally, any AIS is a special SONET signal that communicates to the receiving node when the transmit node does not send a valid signal. AIS is not considered an error. It is raised by the receiving node on each input when it detects the AIS instead of a real signal. In most cases when this condition is raised, an upstream node is raising an alarm to indicate a signal failure; all nodes downstream from it only raise some type of AIS. This condition clears when you resolved the problem on the upstream node.

### Clear the AIS Condition

**Step 1** Determine whether there are alarms such as LOS on the upstream nodes and equipment or if there are OOS,MT (or Locked,maintenance), or OOS,DSBLD ports.

**Step 2** Clear the upstream alarms using the applicable procedures in this chapter.

**Step 3** If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.2 ALS

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Objects: 2R, AOTS, ESCON, FC, GE, ISC, OCN/STMN, TRUNK

The Automatic Laser Shutdown (ALS) condition occurs when an amplifier card (OPT-BST or OPT-PRE) is switched on. The turn-on process lasts approximately nine seconds, and the condition clears after approximately 10 seconds.

**Note** ALS is an informational condition and does not require troubleshooting.

## 2.7.3 AMPLI-INIT

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: AOTS

The Amplifier Initialized condition occurs when an amplifier card (OPT-BST or OPT-PRE) is not able to calculate gain. This condition typically accompanies the "APC-DISABLED" alarm on page 2-18.

**Note** For basic information about amplifier cards, refer to the "Card Reference" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For information about changing their settings, refer to the "Change DWDM Card Settings" chapter. For information abut gain, refer to the "Network Reference" chapter.

### Clear the AMPLI-INIT Condition

**Step 1** Complete the "Delete a Circuit" procedure on page 2-155 on the most recently created circuit.

**Step 2** Recreate this circuit using the procedures in the "Create Channels and Circuits" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Step 3** If the condition does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

## 2.7.4 APC-CORRECTION-SKIPPED

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Objects: AOTS, OCH, OMS, OTS

The Automatic Power Control (APC) Correction Skipped condition occurs when the actual power level of a DWDM channel exceeds the expected setting by 3 dBm or more. APC compares actual power levels with previous power levels every hour or after any channel allocation is performed. If the power difference to be compensated by APC exceeds the range of + 3 dBm or –3 dBm compared with the previous value set, APC is designed not to correct the level and the APC-CORRECTION-SKIPPED condition is raised.

There is no operator action to resolve this condition. It stays raised until the power level problem is resolved and APC obtains a normal reading. For more information about APC, refer to the "Network Reference" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*, and the "1.12.2 System Restart after a Fiber Cut" section on page 1-65.

## 2.7.5 APC-DISABLED

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: NE

The APC Disabled condition occurs when the information related to the number of DWDM channels is not reliable. The condition can occur when any of the following related alarms also occur: the "AMPLI-INIT" condition on page 2-17, the "EQPT" alarm on page 2-37, the "IMPROPRMVL" alarm on page 2-55, or the "MEA (EQPT)" alarm on page 2-90. If the condition occurs with the creation of the first circuit, delete and recreate the circuit. (Refer to the "Create Channels and Circuits" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide* for information about this.) For more information about APC, refer to the "Network Reference" chapter.

### Clear the APC-DISABLED Condition

**Step 1** Complete the appropriate procedure to clear the main alarm:

- Clear the EQPT Alarm, page 2-37
- Clear the IMPROPRMVL Alarm, page 2-56
- Clear the MEA (EQPT) Alarm, page 2-90

**Step 2** If the condition does not clear, complete the "Delete a Circuit" procedure on page 2-155 and then recreate it using procedures in the "Create Channels and Circuits" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Step 3** If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.6 APC-END

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: NE

The APC Terminated on Manual Request condition is raised when APC terminates after it is manually launched from CTC or TL1. APC-END is an informational condition that is raised and cleared spontaneously by the system and is not visible in the CTC Condition window. It is visible only by retrieving it in the Conditions or History tabs. For more information about APC, refer to the "Network Reference" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Note** APC-END is an informational condition and does not require troubleshooting.

## 2.7.7 APC-OUT-OF-RANGE

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Objects: AOTS, OCH, OMS, OTS

The APC Out of Range condition is raised on amplifier cards (OPT-PRE and OPT-BST); demultiplexer cards (32DMX) having a single variable optical attenuator (VOA); and optical add/drop multiplexer cards (AD-1C-xx.x, AD-2C-xx.x, AD-4C-xx.x, AD-1B-xx.x, and AD-4B-xx.x) when the requested gain or attenuation setpoint cannot be set because it exceeds the port parameter range. For example, this condition is raised when APC attempts to set the OPT-BST gain higher than 20 dBm (the card's maximum setpoint) or to set the attenuation on the express VOA lower than 0 dBm (its minimum setpoint).

**Note** For general information about DWDM cards, refer to the "Card Reference" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For information about changing their settings, refer to the "Change DWDM Card Settings" chapter. For more information about APC, refer to the "Network Reference" chapter.

### Clear the APC-OUT-OF-RANGE Condition

**Step 1** There are various root causes for the APC-OUT-OF-RANGE condition. To determine the correct root cause, complete the network-level troubleshooting procedures located in Chapter 1, "General Troubleshooting."

**Step 2** If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.8 AS-CMD

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Objects: 2R, AOTS, BPLANE, EQPT, ESCON, FC, GE, ISC, NE, OCH, OCN/STMN, OMS, OTS, PPM, PWR, TRUNK

The Alarms Suppressed by User Command condition applies to the network element (NE object), backplane (BPLANE object), a single MXP or TXP card, or a port on one of these cards. It occurs when alarms are suppressed for that object and its subordinate objects. For example, suppressing alarms on a card also suppresses alarms on its ports.

**Note** For more information about suppressing alarms, refer to the "Manage Alarms" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Note** This condition is not raised for multiservice transport platform (MSTP) cards such as amplifiers, multiplexers, or demultiplexers.

## Clear the AS-CMD Condition

**Step 1** For all nodes, in node view, click the **Conditions** tab.

**Step 2** Click **Retrieve**. If you have already retrieved conditions, look under the Object column and Eqpt Type column and note what entity the condition is reported against, such as a port, slot, or shelf.

- If the condition is reported against a slot and card, alarms were either suppressed for the entire card or for one of the ports. Note the slot number and continue with Step 3.
- If the condition is reported against the backplane, go to Step 7.
- If the condition is reported against the NE object, go to Step 8.

**Step 3** Determine whether alarms are suppressed for a port and if so, raise the suppressed alarms:

a. Double-click the card to open the card view.

b. Click the **Provisioning > Alarm Profiles > Alarm Behavior** tabs and complete one of the following substeps:

   - If the Suppress Alarms column check box is checked for a port row, deselect it and click **Apply**.
   - If the Suppress Alarms column check box is not checked for a port row, from the View menu choose **Go to Previous View**.

**Step 4** If the AS-CMD condition is reported for a card and not an individual port, in node view click the **Provisioning > Alarm Profiles > Alarm Behavior** tabs.

**Step 5** Locate the row number for the reported card slot.

**Step 6** Click the **Suppress Alarms** column check box to deselect the option for the card row.

**Step 7** If the condition is reported for the backplane, the alarms are suppressed for cards such as the ONS 15454 AIP that are not in the optical or electrical slots. To clear the alarm, complete the following steps:

a. In node view, click the **Provisioning > Alarm Profiles > Alarm Behavior** tabs.

b. In the backplane row, uncheck the **Suppress Alarms** column check box.

c. Click **Apply**.

**Step 8** If the condition is reported for the shelf, cards and other equipment are affected. To clear the alarm, complete the following steps:

a. In node view, click the **Provisioning > Alarm Profiles > Alarm Behavior** tabs if you have not already done so.

b. Click the **Suppress Alarms** check box located at the bottom of the window to deselect the option.

c. Click **Apply**.

**Step 9** If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.9 AS-MT

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Objects: 2R, AOTS, EQPT, ESCON, FC, GE, ISC, OCH, OCN/STMN, OMS, OTS, PPM, TRUNK

The Alarms Suppressed for Maintenance Command condition applies to MXP or TXP cards and occurs when a client or trunk port is placed in the Out-of-Service and Management, Maintenance (OOS-MA,MT service state for loopback testing operations.

### Clear the AS-MT Condition

**Step 1** Complete the "Clear an MXP or TXP Card Loopback Circuit" procedure on page 2-156.

**Step 2** If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.10 AUTORESET

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: EQPT

The Automatic System Reset alarm occurs when you change an IP address or perform any other operation that causes an automatic card-level reboot.

AUTORESET typically clears after a card reboots (up to ten minutes). If the alarm does not clear, complete the following procedure.

### Clear the AUTORESET Alarm

**Step 1** Determine whether there are additional alarms that could have triggered an automatic reset. If there are, troubleshoot these alarms using the applicable section of this chapter.

**Step 2** If the card automatically resets more than once a month with no apparent cause, complete the "Physically Replace a Card" procedure on page 2-154.

**Step 3** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.11 AWG-DEG

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: OTS

The Arrayed Waveguide Gratings (AWG) Degrade alarm occurs when a 32MUX-O, 32WSS-O, 32DMX-O, or 32DMX card heater-control circuit degrades. The heat variance can cause slight wavelength drift. The card does not need to be replaced immediately, but it should be at the next opportunity.

**Note** For General information about 32MUX-O, 32WSS-O, 32DMX-O and 32DMX cards, refer to the "Card Reference" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For more information about changing their settings, refer to the "Change DWDM Card Settings" chapter.

### Clear the AWG-DEG Alarm

**Step 1** For the alarmed 32MUX-O, 32WSS-O, 32DMX-O, or 32DMX card, complete the "Physically Replace a Card" procedure on page 2-154 at the next opportunity.

**Step 2** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.12 AWG-FAIL

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: OTS

The AWG Failure alarm occurs when a 32MUX-O, 32WSS-O, 32DMX-O, or 32DMX card heater-control circuit completely fails. The circuit failure disables wavelength transmission. The card must be replaced to restore traffic.

**Note** For general information about 32MUX-O, 32WSS-O, 32DMX-O and 32DMX cards, refer to the "Card Reference" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For information about changing their settings, refer to the "Change DWDM Card Settings" chapter.

### Clear the AWG-FAIL Alarm

**Step 1** For the alarmed 32MUX-O, 32WSS-O, 32DMX-O, or 32DMX card, complete the "Physically Replace a Card" procedure on page 2-154.

**Step 2** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) to report a Service-Affecting (SA) problem.

## 2.7.13 AWG-OVERTEMP

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: OTS

The AWG Over Temperature alarm is raised if a 32MUX-O, 32WSS-O, 32DMX-O, or 32DMX card having an AWG-FAIL alarm is not replaced and its heater-control circuit temperature exceeds 212 degrees F (100 degrees C). The card goes into protect mode and the heater is disabled.

**Note** For general information about these cards, refer to the "Card Reference" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For information about changing their settings, refer to the "Change DWDM Card Settings" chapter.

### Clear the AWG-OVERTEMP Alarm

**Step 1** Complete the "Clear the AWG-FAIL Alarm" procedure on page 2-22.

**Step 2** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) to report a Service-Affecting (SA) problem.

## 2.7.14 AWG-WARM-UP

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: OTS

The AWG Warm-Up condition occurs when a 32MUX-O, 32WSS-O, 32DMX-O, or 32DMX card heater-control circuit is attaining its operating temperature during startup. The condition lasts approximately 10 minutes but can vary somewhat from this period due to environmental temperature.

**Note** AWG-WARM-UP is an informational condition and does not require troubleshooting.

## 2.7.15 BAT-FAIL

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: PWR

The Battery Fail alarm occurs when one of the two power supplies (A or B) is not detected. This could be because the supply is removed or is not operational. The alarm does not distinguish between the individual power supplies, so onsite information about the conditions is necessary for troubleshooting.

### Clear the BAT-FAIL Alarm

**Step 1** At the site, determine which battery is not present or operational.

**Step 2** Remove the power cable from the faulty supply. For procedures, refer to the "Install the Shelf and Common Control Cards" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*. Reverse the power cable installation procedure.

**Step 3** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

## 2.7.16 BKUPMEMP

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: EQPT

The Primary Nonvolatile Backup Memory Failure alarm refers to a problem with the TCC2/TCC2P flash memory. The alarm occurs when the TCC2/TCC2P is in use and has one of four problems:

- Flash manager fails to format a flash partition.
- Flash manager fails to write a file to a flash partition.
- Problem at the driver level.
- Code volume fails cyclic redundancy checking (CRC, which is a method to verify for errors in data transmitted to the TCC2/TCC2P).

The BKUPMEMP alarm can also cause the "EQPT" alarm, page 2-37. If the EQPT alarm is caused by BKUPMEMP, complete the following procedure to clear the BKUPMEMP and the EQPT alarm.

**Caution** A software update on a standby TCC2/TCC2P can take up to 30 minutes.

### Clear the BKUPMEMP Alarm

**Step 1** Verify that both TCC2/TCC2Ps are powered and enabled by confirming lighted ACT/SBY LEDs on the TCC2/TCC2Ps.

**Step 2** Determine whether the active or standby TCC2/TCC2P has the alarm.

**Step 3** If both TCC2/TCC2Ps are powered and enabled, reset the TCC2/TCC2P where the alarm is raised. If the card is the active TCC2/TCC2P, complete the "Reset an Active TCC2/TCC2P Card and Activate the Standby Card" procedure on page 2-152. If the card is the standby TCC2/TCC2P:

a. Right-click the standby TCC2/TCC2P in CTC.

b. Choose **Reset Card** from the shortcut menu.

c. Click **Yes** in the Are You Sure dialog box. The card resets, the FAIL LED blinks on the physical card.

d. Wait ten minutes to verify that the card you reset completely reboots.

**Step 4** If the TCC2/TCC2P you reset does not reboot successfully, or the alarm has not cleared, call Cisco TAC (1 800 553-2447). If the Cisco TAC technician tells you to reseat the card, complete the "Remove and Reinsert (Reseat) the Standby TCC2/TCC2P Card" procedure on page 2-153. If the Cisco TAC technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Card" procedure on page 2-154.

# 2.7.17 BPV

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: BITS

The 64K Clock Bipolar Density Violation alarm is raised on the TCC2P card if there is a frequency variation in the 8K BITS clock.

The TCC2P card contains an 8K clock and a 64K clock. Each has some bipolar variation, which is normal. This alarm is raised on the 8K clock if that variation discontinues. The BPV alarm is demoted by an LOF or LOS against the BITS clock.

**Note** This alarm is not raised on the TCC2 card.

## Clear the BPV Alarm

**Step 1** Reestablish a normal BITS input signal to clear the alarm. Clear any alarms on the incoming signal or against the BITS timing sources.

**Step 2** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

# 2.7.18 CARLOSS (EQPT)

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: EQPT

A Carrier Loss on the LAN Equipment alarm generally occurs on MXP or TXP cards when the ONS system and the workstation hosting CTC do not have a TCP/IP connection. The problem involves the LAN or data circuit used by the RJ-45 (LAN) connector on the TCC2/TCC2P or the LAN backplane pin connection. This CARLOSS alarm does not involve an Ethernet circuit connected to an Ethernet port. The problem is in the connection and not CTC or the node.

On TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, and MXP_2.5G_10G cards, CARLOSS is also raised against trunk ports when ITU-T G.709 encapsulation is turned off.

A TXP_MR_2.5G card can raise a CARLOSS alarm when the payload is incorrectly configured for the 10 Gigabit Ethernet or 1 Gigabit Ethernet payload data types.

**Warning** **Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard.** Statement 1056

**Warning** **Use of controls, adjustments, or performing procedures other than those specified could result in hazardous radiation exposure.** Statement 1057

**Note** For more information about provisioning MXP or TXP PPMs (also called SFPs), refer to the "Turn Up a Node" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For PPM (SFP) specifications, refer to the "Hardware Specifications" appendix. For more information about MRC-12 and OC192-XFP/STM64-XFP cards, refer to the "Optical Cards" chapter in the *Cisco ONS 15454 DWDM Reference Manual*.

**Note** For more information about Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.

## Clear the CARLOSS (EQPT) Alarm

**Step 1** If the reporting card is an MXP or TXP card in an ONS 15454 node, verify the data rate configured on the PPM (also called SFP):

a. Double-click the reporting MXP or TXP card.

b. Click the **Provisioning > Pluggable Port Modules** tabs.

c. View the Pluggable Port Modules area port listing in the **Actual Equipment Type** column and compare this with the contents of the Selected PPM area Rate column for the MXP or TXP multirate port.

d. If the rate does not match the actual equipment, you must delete and recreate the selected PPM. Select the PPM (SFP), click **Delete**, then click **Create** and choose the correct rate for the port rate.

**Note** For more information about provisioning PPMs (SFPs), refer to the "Turn Up a Node" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For PPM (SFP) specifications, refer to the "Hardware Specifications" appendix.

**Step 2** If the reporting card is an OC-N/STM-N card, verify connectivity by pinging the ONS system that is reporting the alarm by completing the "Verify PC Connection to the ONS 15454 (ping)" procedure on page 1-37.

**Step 3** If the ping is successful, it demonstrates that an active TCP/IP connection exists. Restart CTC:

a. Exit from CTC.

b. Reopen the browser.

c. Log into CTC.

**Step 4** Using optical test equipment, verify that proper receive levels are achieved. (For instructions about using optical test equipment, refer to the manufacturer documentation.)

**Caution** Always use the supplied electrostatic discharge wristband when working with a powered ONS system. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

**Step 5** Verify that the optical LAN cable is properly connected and attached to the correct port. For more information about fiber connections and terminations, refer to the "Turn Up a Node" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Step 6** If the fiber cable is properly connected and attached to the port, verify that the cable connects the card to another Ethernet device and is not misconnected to an OC-N/STM-N card.

**Step 7** If you are unable to establish connectivity, replace the fiber cable with a new known-good cable. To do this, refer to the "Turn Up a Node" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Step 8** If you are unable to establish connectivity, perform standard network or LAN diagnostics. For example, trace the IP route, verify cable continuity, and troubleshoot any routers between the node and CTC. To verify cable continuity, follow site practices.

**Step 9** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

## 2.7.19 CARLOSS (FC)

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: FC

The Carrier Loss for Fibre Channel (FC) alarm occurs on the client port of a TXP_MR_10G, TXP_MR_10E, TXP_MR_2.5G, TXPP_MR_2.5G, MXP_MR_2.5G, and MXPP_MR_2.5G supporting 1-Gb Fibre Channel (FC1G), 2-Gb FC (FC2G), or 10Gb Fiber Channel (10G Fiber Channel) traffic. The loss can be due to a misconfiguration, fiber cut, or client equipment problem.

**Note** For general information about MXP and TXP cards, refer to the "Card Reference" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For information about provisioning them, refer to the "Provision Transponder and Muxponder Cards" chapter.

### Clear the CARLOSS (FC) Alarm

**Step 1** Complete the "Clear the CARLOSS (GE) Alarm" procedure on page 2-28.

**Step 2** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

## 2.7.20 CARLOSS (GE)

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: GE

The Carrier Loss for Gigabit Ethernet (GE) alarm occurs on the client port of a TXP_MR_10G, TXP_MR_10E, TXP_MR_2.5G, TXPP_MR_2.5G, MXP_MR_2.5G, and MXPP_MR_2.5G supporting 1-Gbps or 10-Gbps traffic. The loss can be due to a misconfiguration, fiber cut, or client equipment problem.

**Note** For general information about MXP and TXP cards, refer to the "Card Reference" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For information about provisioning them, refer to the "Provision Transponder and Muxponder Cards" chapter.

### Clear the CARLOSS (GE) Alarm

**Step 1** Ensure that the GE client is correctly configured:

a. Double-click the card to open the card view.

b. Click the **Provisioning > Pluggable Port Modules** tabs.

c. View the Pluggable Port Modules area port listing in the **Actual Equipment Type** column and compare this with the client equipment. If no PPM (SFP) is provisioned, refer to the "Turn Up a Node" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*. PPM (SFP) specifications are listed in the "Hardware Specifications" appendix.

d. If a PPM (SFP) has been created, view the contents of the Selected PPM area Rate column for the MXP or TXP MR card and compare this rate with the client equipment data rate. In this case, the rate should be ONE_GE or 10G Ethernet. If the PPM (SFP) rate is differently provisioned, select the PPM (SFP), click **Delete**, then click **Create** and choose the correct rate for the equipment type.

**Note** For information about installing provisioning PPMs (SFPs), refer to the "Turn Up a Node" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Step 2** If there is no PPM (SFP) misprovisioning, check for a fiber cut. An LOS alarm would also be present. If there is an alarm, complete the "Clear the LOS (OCN/STMN) Alarm" procedure located in Chapter 2, "Alarm Troubleshooting," of the *Cisco ONS 15454 Troubleshooting Guide* or *Cisco ONS 15454SDH Troubleshooting Guide*.

**Step 3** If there is no fiber cut or provisioning error, check the client-side equipment for any transmission errors on the line.

**Step 4** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

## 2.7.21 CARLOSS (ISC)

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: ISC

The Carrier Loss for Inter-Service Channel (ISC) alarm occurs on the client port of a TXP_MR_10G, TXP_MR_10E, TXP_MR_2.5G, TXPP_MR_2.5G, MXP_MR_2.5G, and MXPP_MR_2.5G supporting ISC traffic. The loss can be due to a misconfiguration, fiber cut, or client equipment problem.

**Note** For general information about MXP and TXP cards, refer to the "Card Reference" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For information about provisioning them, refer to the "Provision Transponder and Muxponder Cards" chapter.

### Clear the CARLOSS (ISC) Alarm

**Step 1** Complete the "Clear the CARLOSS (GE) Alarm" procedure on page 2-28.

**Step 2** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

## 2.7.22 CARLOSS (TRUNK)

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: TRUNK

A Carrier Loss alarm is raised on the optical Trunk-RX port of a TXP_MR_10G, TXP_MR_10E, TXP_MR_2.5G, TXPP_MR_2.5G, MXP_MR_2.5G, and MXPP_MR_2.5G when the Ethernet payload is lost. This alarm only occurs when ITU-T G.709 encapsulation is disabled.

**Note** For general information about TXP cards and their monitoring capabilities, refer to the "Card Reference" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For information about provisioning them, refer to the "Provision Transponder and Muxponder Cards" chapter.

### Clear the CARLOSS (TRUNK) Alarm

**Step 1** Check for any upstream equipment failures:

- Verify that the far-end TXP or MXP is generating the signal to be received by the alarmed card.
- Verify that the Trunk-Tx port is not reporting any performance monitoring (PM) problems.
- Verify that the Client-Rx port is not reporting any PM problems that could cause the CARLOSS in this card.

**Note** For more information about performance monitoring, refer to the "Performance Monitoring" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Step 2** If there is no cause upstream, verify cabling continuity from the transmitting port of the DWDM card (AD-xC-xx.x-xx.x, 32DMX-O, or 32DMX) connected to the TXP receiving port reporting this alarm.

**Step 3** If a patch panel is used, ensure that the LC-LC adapter managing the connection is in good working order.

**Step 4** If the continuity is good, clean the fiber according to site practice. If none exists, complete the fiber cleaning procedure in the "Maintain the Node" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Step 5** If the signal is valid, ensure that the transmit and receive outputs from the patch panel to your equipment are properly connected (that is, the correct wavelength is coming from the patch panel). For more information about fiber connections and terminations, refer to the "Turn Up a Node" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Step 6** If the correct port is in service but the alarm has not cleared, use an optical test set to confirm that a valid signal exists on the input port of the alarmed TXP. For specific procedures to use the test set equipment, consult the manufacturer. Test the line as close to the receiving card as possible.

**Step 7** If the alarm does not clear, complete the "Physically Replace a Card" procedure on page 2-154 for the reporting card.

**Step 8** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

## 2.7.23 CASETEMP-DEG

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: AOTS

The Case Temperature Degrade alarm is raised when a DWDM card temperature sensor detects an out-of-range external temperature at the shelf level. The working range for DWDM cards is from 23 degrees F (–5 degrees C) to 149 degrees F (65 degrees C).

**Note** For specific temperature and environmental information about each DWDM card, refer to the "Hardware Specifications" appendix in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

### Clear the CASETEMP-DEG Alarm

**Step 1** Determine whether the air filter needs replacement. Complete the "Inspect, Clean, and Replace the Reusable Air Filter" procedure on page 2-156.

**Step 2** If the filter is clean, complete the "Remove and Reinsert a Fan-Tray Assembly" procedure on page 2-158.

**Step 3** If the fan does not run or the alarm persists, complete the "Replace the Fan-Tray Assembly" procedure on page 2-158. The fan should run immediately when correctly inserted.

**Step 4** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.24 DISCONNECTED

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: SYSTEM

The Disconnected alarm is raised when CTC has been disconnected from the node. The alarm is cleared when CTC is reconnected to the node.

### Clear the DISCONNECTED Alarm

**Step 1** Restart the CTC application.

**Step 2** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call TAC (1-800-553-2447).

## 2.7.25 DSP-COMM-FAIL

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: TRUNK

The Digital Signal Processor (DSP) Communication Failure alarm indicates that there is a communication failure between an MXP or TXP card microprocessor and the on-board DSP chip that controls the trunk (or DWDM) port. This alarm typically occurs after a DSP code upgrade.

The alarm is temporary and does not require user action. The MXP or TXP card microprocessor attempts to restore communication with the DSP chip until the alarm is cleared. (For general information about MXP and TXP cards, refer to the "Card Reference" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.)

If the alarm is raised for an extended period, the MXP or TXP card raises the "DUP-IPADDR" alarm on page 2-32 and could affect traffic.

**Note** DSP-COMM-FAIL is an informational alarm and does not require troubleshooting.

## 2.7.26 DSP-FAIL

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: TRUNK

The DSP Failure alarm indicates that a "DSP-COMM-FAIL" alarm, page 2-31, has persisted for an extended period on an MXP or TXP card. It indicates that the card is faulty.

### Clear the DSP-FAIL Alarm

**Step 1** Complete the "Physically Replace a Card" procedure on page 2-154 for the reporting MXP or TXP card.

**Step 2** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

## 2.7.27 DUP-IPADDR

Default Severity: Minor (MN), Non-Service Affecting (NSA)

Logical Object: NE

The Duplicate IP Address alarm indicates that the alarmed node IP address is already in use within the same data communications channel (DCC) area. When this happens, CTC no longer reliably connects to either node. Depending on how the packets are routed, CTC could connect to either node (having the same IP address). If CTC has connected to both nodes before they shared the same address, it has two distinct NodeModel instances (keyed by the node ID portion of the MAC address).

### Clear the DUP-IPADDR Alarm

**Step 1** Isolate the alarmed node from the other node having the same address:

**a.** Connect to the alarmed node using the Craft port on the TCC2/TCC2P card.

**b.** Begin a CTC session.

**c.** In the login dialog box, uncheck the **Network Discovery** check box.

**Step 2** In node view, click the **Provisioning > Network > General** tabs.

**Step 3** In the IP Address field, change the IP address to a unique number.

**Step 4** Click **Apply**.

**Step 5** Restart any CTC sessions that are logged into either of the duplicate IP addresses. (For procedures to log in or log out, refer to the "Connect the PC and Log Into the GUI" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Step 6** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.28 DUP-NODENAME

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: NE

The Duplicate Node Name alarm indicates that the alarmed node alphanumeric name is already being used within the same DCC area.

### Clear the DUP-NODENAME Alarm

**Step 1** In node view, click the **Provisioning > General > General** tabs.

**Step 2** In the Node Name field, enter a unique name for the node.

**Step 3** Click **Apply**.

**Step 4** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.29 EHIBATVG

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: PWR

The Extreme High Voltage Battery alarm occurs in a –48 VDC environment when a battery lead input voltage exceeds the extreme high power threshold. This threshold, with a default value of –56.5 VDC, is user-provisionable. The alarm remains raised until the voltage remains under the threshold for 120 seconds. (For information about changing this threshold, refer to the "Turn Up Node" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.)

### Clear the EHIBATVG Alarm

**Step 1** The problem is external to the ONS system. Troubleshoot the power source supplying the battery leads.

**Step 2** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

## 2.7.30 ELWBATVG

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: PWR

The Extreme Low Voltage Battery alarm occurs in a –48 VDC environment when a battery lead input voltage falls below the extreme low power threshold. This threshold, with a default value of –40.5 VDC, is user-provisionable. The alarm remains raised until the voltage remains over the threshold for 120 seconds. (For information about changing this threshold, refer to the "Turn Up Node" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

### Clear the ELWBATVG Alarm

**Step 1** The problem is external to the ONS system. Troubleshoot the power source supplying the battery leads.

**Step 2** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

## 2.7.31 EOC

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Objects: OCN, TRUNK

The SONET DCC Termination Failure alarm occurs when the ONS system loses its DCC. Although this alarm is primarily SONET, it can apply to DWDM. For example, the OSCM card can raise this alarm on its OC-3 section overhead.

The SDCC consists of three bytes, D1 through D3, in the SONET overhead. The bytes convey information about operation, administration, maintenance, and provisioning (OAM&P). The ONS system uses the DCC on the SONET section layer to communicate network management information.

**Warning** **Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard.** Statement 1056

**Warning** **Use of controls, adjustments, or performing procedures other than those specified could result in hazardous radiation exposure.** Statement 1057

**Note** If a circuit shows a partial state when this alarm is raised, the logical circuit is in place. The circuit is able to carry traffic when the connection issue is resolved. You do not need to delete the circuit when troubleshooting this alarm.

**Note** For general information about OSCM or other DWDM cards, refer to the “Card Reference” chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For information about changing their settings, refer to the “Change DWDM Card Settings” chapter. For more information about the SONET or SDH (ETSI) overhead, refer to the “SONET Topologies and Upgrades” chapter of the *Cisco ONS 15454 Procedure Guide* or the “SDH Topologies and Upgrades” chapter of the *Cisco ONS 15454 SDH Procedure Guide*.

**Note** The EOC alarm is raised on the DWDM trunk in MSTP systems. Its SDH (ETSI) counterpart, MS-EOC, is not raised against the trunk port.

## Clear the EOC Alarm

**Step 1** If the LOS (DS1) alarm or SF-L alarm is reported, complete the appropriate troubleshooting procedure in the "Alarm Troubleshooting" chapter of the *Cisco ONS 15454 Troubleshooting Guide*.

**Caution** Always use the supplied electrostatic discharge wristband when working with a powered ONS system. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

**Step 2** If the alarm does not clear on the reporting node, verify the physical connections between the cards and that the fiber-optic cables are configured to carry SDCC traffic. For more information about fiber connections and terminations, refer to the "Turn Up a Node" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Step 3** If the physical connections are correct and configured to carry DCC traffic, ensure that both ends of the fiber span have in-service (IS) ports. Verify that the ACT/SBY LED on each card is green.

**Step 4** When the LEDs on the cards are correctly illuminated, complete the "Verify or Create Node Section DCC Terminations" procedure on page 2-155 to verify that the DCC is provisioned for the ports at both ends of the fiber span.

**Step 5** Repeat Step 4 at the adjacent nodes.

**Step 6** If DCC is provisioned for the ends of the span, verify that the port is active and in service by completing the following steps:

a. Confirm that the card shows a green LED in CTC or on the physical card. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

b. To determine whether the port is in service, double-click the card in CTC to open the card view.

c. Click the **Provisioning > Line** tabs.

d. Verify that the Admin State column lists the port as IS (or Unlocked).

e. If the Admin State column lists the port as OOS,MT (or Locked,maintenance) or OOS,DSBLD, click the column and choose **IS** , or **Unlocked**. Click **Apply**.

**Step 7** For all nodes, if the card is in service, use an optical test set to determine whether signal failures are present on fiber terminations. For specific procedures to use the test set equipment, consult the manufacturer.

**Caution** Using an optical test set disrupts service on a card. It could be necessary to manually switch traffic carrying circuits over to a protection path. Refer to the "2.9.1 Protection Switching, Lock Initiation, and Clearing" section on page 2-149 for commonly used switching procedures.

**Step 8** If no signal failures exist on terminations, measure power levels to verify that the budget loss is within the parameters of the receiver. Refer to the "Hardware Specifications" appendix in the *Cisco ONS 15454 DWDM Installation and Operations Guide* for card power levels.

**Step 9** If budget loss is within parameters, ensure that fiber connectors are securely fastened and properly terminated. For more information about cabling, refer to the "Turn Up a Node" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Step 10** If fiber connectors are properly fastened and terminated, complete the "Reset an Active TCC2/TCC2P Card and Activate the Standby Card" procedure on page 2-152.

Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card.

Resetting the active TCC2/TCC2P switches control to the standby TCC2/TCC2P. If the alarm clears when the ONS system node switches to the standby TCC2/TCC2P, the user can assume that the previously active card is the cause of the alarm.

**Step 11** If the TCC2/TCC2P reset does not clear the alarm, delete the problematic SDCC termination:

a. From the View menu in card view, choose **Go to Previous View** if you have not already done so.

b. Click the **Provisioning > Comm Channels > SDCC** tabs.

c. Highlight the problematic DCC termination.

d. Click **Delete**.

e. Click **Yes** in the Confirmation Dialog box.

**Step 12** Recreate the SDCC termination. Refer to the "Turn Up a Node" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide* for procedures.

**Step 13** Verify that both ends of the DCC have been recreated at the optical ports.

**Step 14** If the alarm has not cleared, call Cisco TAC (1 800 553-2447). If the Cisco TAC technician tells you to reseat the card, complete the "Remove and Reinsert (Reseat) the Standby TCC2/TCC2P Card" procedure on page 2-153. If the Cisco TAC technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Card" procedure on page 2-154.

## 2.7.32 EOC-L

Default Severity: Minor (MN), Non-Service-Affecting (NSA) for OCN/STMN

Logical Object: TRUNK

The Line DCC (LDCC) Termination Failure alarm occurs when the ONS system loses its line data communications channel (LDCC) termination. For example, the OSCM card can raise this alarm on its OC-3 line overhead.

The LDCC consists of nine bytes, D4 through D12, in the SONET overhead. The bytes convey information about OAM&P. The ONS system uses the LDCCs on the SONET line layer to communicate network management information.

**Warning** **On the OC-192 card, the laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. The laser is off when the safety key is off (labeled 0).** Statement 293

**Warning** **Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard.** Statement 1056

**Warning** **Use of controls, adjustments, or performing procedures other than those specified could result in hazardous radiation exposure.** Statement 1057

> **Note** If a circuit shows a partial status when the EOC or EOC-L alarm is raised, it occurs when the logical circuit is in place. The circuit is able to carry traffic when the DCC termination issue is resolved. You do not need to delete the circuit when troubleshooting this alarm.

> **Note** For general information about OSCM or other DWDM cards, refer to the “Card Reference” chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For information about changing their settings, refer to the “Change DWDM Card Settings” chapter. For more information about the SONET or SDH (ETSI) overhead, refer to the “SONET Topologies and Upgrades” chapter of the *Cisco ONS 15454 Procedure Guide* or the “SDH Topologies and Upgrades” chapter of the *Cisco ONS 15454 SDH Procedure Guide*.

### Clear the EOC-L Alarm

**Step 1** Complete the “Clear the EOC Alarm” procedure on page 2-35.

**Step 2** If the alarm has not cleared, call Cisco TAC (1 800 553-2447). If the Cisco TAC technician tells you to reseat the card, complete the “Remove and Reinsert (Reseat) the Standby TCC2/TCC2P Card” procedure on page 2-153. If the Cisco TAC technician tells you to remove the card and reinstall a new one, follow the “Physically Replace a Card” procedure on page 2-154.

## 2.7.33 EQPT

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Objects: AICI-AEP, AICI-AIE, EQPT, PPM

An Equipment Failure alarm indicates that a hardware failure has occurred on the reporting card. If the EQPT alarm occurs with a “BKUPMEMP” alarm, page 2-24, refer to the procedure to clear the alarm. (Clearing a BKUPMEMP alarm also clears an EQPT alarm.)

This alarm is also invoked if a diagnostic circuit detects a card application-specific integrated circuit (ASIC) failure. In this case, if the card is part of a protection group, an APS switch occurs. If the card is the protect card, switching is inhibited and a “PROTNA” alarm, page 2-119, is raised. The standby path generates a path-type alarm. For more information about provisioning PPMs (SFPs), refer to the “Turn Up a Node” chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

### Clear the EQPT Alarm

**Step 1** If traffic is active on the alarmed port, you could need to switch traffic away from it. See the “2.9.1 Protection Switching, Lock Initiation, and Clearing” section on page 2-149 for commonly used traffic-switching procedures.

**Step 2** Complete the “Reset a Card in CTC” procedure on page 2-152 for the reporting card.

**Step 3** Verify that the reset is complete and error-free and that no new related alarms appear in CTC. Verify the LED status. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

**Step 4** If the CTC reset does not clear the alarm, complete the "Remove and Reinsert (Reseat) Any Card" procedure on page 2-154 for the reporting card.

**Step 5** If the physical reseat of the card fails to clear the alarm, complete the "Physically Replace a Card" procedure on page 2-154 for the reporting card.

**Step 6** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

## 2.7.34 EQPT-MISS

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: FAN

The Replaceable Equipment or Unit Missing alarm is reported against the fan-tray assembly unit. It indicates that the replaceable fan-tray assembly is missing or is not fully inserted. It could also indicate that the ribbon cable connecting the AIP to the system board is bad.

**Caution** Always use the supplied electrostatic discharge wristband when working with a powered ONS system. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

### Clear the EQPT-MISS Alarm

**Step 1** If the alarm is reported against the fan, verify that the fan-tray assembly is present.

**Step 2** If the fan-tray assembly is present, complete the "Replace the Fan-Tray Assembly" procedure on page 2-158.

**Step 3** If no fan-tray assembly is present, obtain a fan-tray assembly and refer to the "Install the Fan-Tray Assembly," procedure in the "Install the Shelf and Common Control Cards" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Step 4** If the alarm does not clear, replace the ribbon cable from the AIP to the system board with a known-good ribbon cable.

**Step 5** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

## 2.7.35 EXCCOL

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: EQPT

The Excess Collisions on the LAN alarm indicates that too many collisions are occurring between data packets on the network management LAN, and communications between the ONS system and CTC could be affected. The network management LAN is the data network connecting the workstation running the CTC software to the TCC2/TCC2P. The problem causing the alarm is external to the ONS system.

Troubleshoot the network management LAN connected to the TCC2/TCC2P for excess collisions. You might need to contact the system administrator of the network management LAN to accomplish the following steps.

### Clear the EXCCOL Alarm

**Step 1** Verify that the network device port connected to the TCC2/TCC2P has a flow rate set to 10 Mb, half-duplex.

**Step 2** If the port has the correct flow rate and duplex setting, troubleshoot the network device connected to the TCC2/TCC2P and the network management LAN.

**Step 3** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.36 EXT

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: ENVALRM

A Failure Detected External to the NE alarm occurs because an environmental alarm is present. For example, a door could be open or flooding could have occurred.

### Clear the EXT Alarm

**Step 1** In node view, double-click the AIC-I card to open the card view.

**Step 2** Double-click the **Maintenance > External Alarms** tabs.

**Step 3** Follow your standard operating procedure to remedy environmental conditions that cause alarms. The alarm clears when the situation is remedied.

**Step 4** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.37 FAILTOSW (2R, EQPT, ESCON, FC, GE, ISC, OCN/STMN)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Objects: 2R, EQPT, ESCON, FC, GE, ISC, OCN/STMN, TRUNK

The Failure to Switch to Protection Facility condition for MXP and TXP client ports occurs in a Y-cable protection group when a working or protect facility switches to its companion port by using a MANUAL command. For example, if you attempt to manually switch traffic from an unused protect port to an in-service working port, the switch will fail (because traffic is already present on the working port) and you will see the FAILTOSW condition.

**Note** For more information about protection schemes, refer to the "Manage the Node" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

### Clear the FAILTOSW (2R, EQPT, ESCON, FC, GE, ISC, OCN/STMN) Condition

**Step 1** Look up and troubleshoot the higher-priority alarm. Clearing the higher-priority condition frees the card and clears the FAILTOSW.

**Step 2** If the condition does not clear, replace the working card that is reporting the higher-priority alarm by following the "Physically Replace a Card" procedure on page 2-154. This card is the working facility using the protect facility and not reporting FAILTOSW.

Replacing the working card that is reporting the higher-priority alarm allows traffic to revert to the working slot and the card reporting the FAILTOSW to switch to the protect card.

**Step 3** If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.38 FAILTOSW (TRUNK)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: TRUNK

The Failure to Switch to Protection Facility condition applies to MXP and TXP trunk ports in splitter protection groups and occurs when a working or protect trunk port switches to its companion port by using a MANUAL command.

**Note** For more information about protection schemes, refer to the "Manage the Node" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

### Clear the FAILTOSW (TRUNK) Condition

**Step 1** Look up and troubleshoot the higher-priority alarm. Clearing the higher-priority condition frees the card and clears the FAILTOSW.

**Step 2** If the condition does not clear, replace the working card that is reporting the higher-priority alarm by following the "Physically Replace a Card" procedure on page 2-154. This card is the working facility using the protect facility and not reporting FAILTOSW.

Replacing the working card that is reporting the higher-priority alarm allows traffic to revert to the working slot and the card reporting the FAILTOSW to switch to the protect card.

**Step 3** If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.39 FEC-MISM

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: TRUNK

The Forward Error Correction (FEC) Mismatch alarm applies to all cards featuring FEC/E-FEC capability: TXP_MR_10G, TXP_MR_10E, TXP_MR_2.5G, TXPP_MR_2.5G, MXP_10G, and MXP_MR_10E. FEC-MISMATCH is reported only on the card configured in Standard FEC mode or with FEC disabled. A card configured in enhanced FEC mode will report an "OTUK-LOF" alarm on page 2-110.

The alarm is related to ITU-T G.709 encapsulation and is only raised against a trunk port.

**Note** For general information about MXP and TXP cards and their monitoring capabilities, refer to the "Card Reference" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For information about provisioning them, refer to the "Provision Transponder and Muxponder Cards" chapter.

### Clear the FEC-MISM Alarm

**Step 1** Double-click the TXP_MR_10G, TXP_MR_10E, TXP_MR_2.5G, TXPP_MR_2.5G, MXP_MR_10G, and MXP_MR_10E card.

**Step 2** Click the **Provisioning > OTN > OTN Lines** tabs.

**Step 3** In the FEC column, click **Enable** to activate the FEC feature. This causes a different OTN frame to be transmitted. Alternately, in the E-FEC column (TXP_MR_10E and MXP_MR_10E), click **Enable** to activate the Enhanced FEC feature.

**Step 4** Verify that the far-end card is configured the same way by repeating Step 1 through Step 3.

**Step 5** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

## 2.7.40 FIBERTEMP-DEG

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: AOTS

The Fiber Temperature Degrade alarm occurs when a DWDM card internal heater-control circuit fails. Degraded temperature can cause some signal drift. The card should be replaced at the next opportunity.

**Note** For general information about DWDM cards, refer to the "Card Reference" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For information about changing their settings, refer to the "Change DWDM Card Settings" chapter.

### Clear the FIBERTEMP-DEG Alarm

**Step 1** For the alarmed card, complete the "Physically Replace a Card" procedure on page 2-154 at the next opportunity.

**Step 2** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.41 FORCED-REQ-SPAN (2R, ESCON, FC, GE, ISC, OCN/STMN)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Objects: 2R, ESCON, FC, GE, ISC, OCN/STMN

The Force Switch Request Span condition applies to Y-cable-protected TXP configurable clients (OC-3, OC-12/STM-4,OC-48/STM-16, OC-192/STM-64, FC, ESCON, or FICON). If traffic is present on a working port and you use the FORCE command to prevent it from switching to the protect port (indicated by "FORCED TO WORKING"), FORCED-REQ-SPAN indicates this force switch. In this case, the force is affecting not only the facility, but the span.

**Note** For more information about protection schemes, refer to the "Manage the Node" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

## 2.7.42 FORCED-REQ-SPAN (TRUNK)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: TRUNK

The Force Switch Request Span condition applies to MXP and TXP trunk ports in splitter protection groups. If traffic is present on a working port and you use the FORCE command to prevent it from switching to the protect port (indicated by "FORCED TO WORKING"), FORCED-REQ-SPAN indicates this force switch. In this case, the force is affecting not only the facility, but the span.

**Note** For more information about protection schemes, refer to the "Manage the Node" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

## 2.7.43 FRCDSWTOINT

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: NE-SREF

The Force Switch to Internal Timing condition occurs when the user issues a Force command to switch to an internal timing source.

**Note** FRCDSWTOINT is an informational condition and does not require troubleshooting.

## 2.7.44 FRCDSWTOPRI

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Objects: EXT-SREF, NE-SREF

The Force Switch to Primary Timing Source condition occurs when the user issues a Force command to switch to the primary timing source.

**Note** FRCDSWTOPRI is an informational condition and does not require troubleshooting.

## 2.7.45 FRCDSWTOSEC

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Objects: EXT-SREF, NE-SREF

The Force Switch to Second Timing Source condition occurs when the user issues a Force command to switch to the second timing source.

**Note** FRCDSWTOSEC is an informational condition and does not require troubleshooting.

## 2.7.46 FRCDSWTOTHIRD

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Objects: EXT-SREF, NE-SREF

The Force Switch to Third Timing Source condition occurs when the user issues a Force command to switch to a third timing source.

**Note** FRCDSWTOTHIRD is an informational condition and does not require troubleshooting.

## 2.7.47 FRNGSYNC

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: NE-SREF

The Free Running Synchronization Mode condition occurs when the reporting ONS system is in free-run synchronization mode. External timing sources have been disabled and the node is using its internal clock, or the node has lost its designated building integrated timing supply (BITS) timing source. After the 24-hour holdover period expires, timing slips could begin to occur on an ONS system node relying on an internal clock.

**Note** If the ONS system is configured to operate from its internal clock, disregard the FRNGSYNC condition.

### Clear the FRNGSYNC Condition

**Step 1** If the ONS system is configured to operate from an external timing source, verify that the BITS timing source is valid. Common problems with a BITS timing source include reversed wiring and bad timing cards. Refer to the "Timing" chapter in the *Cisco ONS 15454 DWDM Reference Manual* for more information.

**Step 2** If the BITS source is valid, clear alarms related to the failures of the primary and secondary reference sources, such as the "SYNCPRI" alarm on page 2-138 and the "SYNCSEC" alarm on page 2-138.

**Step 3** If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.48 FSTSYNC

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: NE-SREF

A Fast Start Synchronization Mode condition occurs when the node is choosing a new timing reference. The previous timing reference has failed.

The FSTSYNC alarm disappears after approximately 30 seconds. If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

**Note** FSTSYNC is an informational condition. It does not require troubleshooting.

## 2.7.49 GAIN-HDEG

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: AOTS

The Gain High Degrade alarm is raised on an amplifier card (OPT-BST or OPT-PRE) when the amplifier reaches the Gain High Degrade Threshold. (This value is automatically provisioned with the gain setpoint, but the alarm threshold is 2 dBm higher than the setpoint. The card should be replaced at the first opportunity.

**Note** This alarm is applicable only when the amplifier working mode is set to Control Gain.

**Note** For general information about DWDM amplifier cards, refer to the "Card Reference" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For information about changing their settings, refer to the "Change DWDM Card Settings" chapter. For information about control gain, refer to the "Node Reference" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

## Clear the GAIN-HDEG Alarm

**Step 1** Verify that the LED is correctly illuminated on the physical card. A green ACT/SBY LED indicates an active card. A red ACT/SBY LED indicates a failed card.

**Step 2** Complete "Reset a Card in CTC" procedure on page 2-152 on the failing amplifier.

**Step 3** If the alarm does not clear, identify all the OCHNC circuits applying to the failing card. Force all the protected circuits on the optical path that the faulty amplifier does not belong to. Switch the OCHNC administrative state of all these circuits to **OOS,DSBLD** (or **Locked,disabled)**.

**Caution** All remaining unprotected circuits will suffer for a traffic hit when you disable the circuits.

**Step 4** Switch the administrative state of only one of the OCHNC circuits to **IS,AINS** (or **Unlocked,automaticInService**. This forces the amplifier to recalculate its gain setpoint and value.

**Step 5** If the alarm does not clear and no other alarms exist that could be the source of the "GAIN-HDEG" alarm on page 2-44, or if clearing an alarm did not clear the GAIN-HDEG, place all of the card ports in **OOS,DSBLD** (or **Locked,disabled)** administrative state.

**Step 6** Complete the "Physically Replace a Card" procedure on page 2-154 for the reporting card.

**Step 7** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

# 2.7.50 GAIN-HFAIL

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: AOTS

The Gain High Degrade alarm is raised on an amplifier card (OPT-BST or OPT-PRE) when the amplifier reaches the Gain High Degrade Threshold. (This value is automatically provisioned with the gain setpoint, but the alarm threshold is 5 dBm higher than the setpoint.) If the alarm cannot be cleared, the card must be replaced.

**Note** This alarm is applicable only when the amplifier working mode is set to Control Gain.

**Note** For general information about DWDM amplifier cards, refer to the "Card Reference" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For information about changing their settings, refer to the "Change DWDM Card Settings" chapter. For information about control gain, refer to the "Node Reference" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

### Clear the GAIN-HFAIL Alarm

**Step 1** For the alarmed card, complete the "Clear the GAIN-HDEG Alarm" procedure on page 2-45.

**Step 2** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) to report a Service-Affecting (SA) problem.

## 2.7.51 GAIN-LDEG

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: AOTS

The Gain High Degrade alarm is raised on an amplifier card (OPT-BST or OPT-PRE) when the amplifier does not reach Gain High Degrade Threshold. (This value is automatically provisioned with the gain setpoint, but the alarm threshold is 2 dBm lower than the setpoint.) The card should be replaced at the first opportunity.

**Note** This alarm is applicable only when the amplifier working mode is set to Control Gain.

**Note** For general information about DWDM amplifier cards, refer to the "Card Reference" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For information about changing their settings, refer to the "Change DWDM Card Settings" chapter. For information about control gain, refer to the "Node Reference" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

### Clear the GAIN-LDEG Alarm

**Step 1** For the alarmed card, complete the "Clear the GAIN-HDEG Alarm" procedure on page 2-45.

**Step 2** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.52 GAIN-LFAIL

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: AOTS

The Gain High Degrade alarm is raised on an amplifier card (OPT-BST or OPT-PRE) when the amplifier does not reach Gain High Degrade Threshold. (This value is automatically provisioned with the gain setpoint, but the alarm threshold is 5 dBm lower than the setpoint. If the alarm cannot be cleared, the card must be replaced.

**Note** This alarm is applicable only when the amplifier working mode is set to Control Gain.

**Note** For general information about DWDM amplifier cards, refer to the "Card Reference" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For information about changing their settings, refer to the "Change DWDM Card Settings" chapter. For information about control gain, refer to the "Node Reference" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

### Clear the GAIN-LFAIL Alarm

**Step 1** For the alarmed card, complete the "Clear the GAIN-HDEG Alarm" procedure on page 2-45.

**Step 2** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.53 GCC-EOC

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: TRUNK

The GCC Embedded Operation Channel Failure alarm applies to the optical transport network (OTN) communication channel for TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, MXP_2.5G_10G, and MXP_2.5G_10E cards. The GCC-EOC alarm is raised when the channel cannot operate.

This alarm applies to trunk ports only when ITU-T G.709 encapsulation is enabled and a general communication channel (GCC) has been provisioned between the two TXP/MXP cards.

**Note** For more information about GCC circuits, please refer to the "Create Channels and Circuits" chapter located in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

### Clear the GCC-EOC Alarm

**Step 1** Complete the "Clear the EOC Alarm" procedure on page 2-35.

**Step 2** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.54 GE-OOSYNC (FC, GE, ISC)

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Objects: FC, GE, ISC

The Gigabit Ethernet Out of Synchronization alarm applies to TXP_MR_10G,TXP_MR_10E, TXP_MR_2.5G,TXPP_MR_2.5G,MXP_MR_2.5G and MXPP_MR_2.5G cards when the Ethernet signal incoming on the Client-Rx port is out of synchronization.

**Note** For general information about MXP and TXP cards, refer to the "Card Reference" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For information about provisioning them, refer to the "Provision Transponder and Muxponder Cards" chapter.

### Clear the GE-OOSYNC (FC, GE, ISC) Alarm

**Step 1** Ensure that the incoming signal from the Client-Rx port is provisioned with the correct physical-layer protocol (Ethernet).

**Step 2** Ensure that the line is provisioned with the correct line speed (10G or 1G Ethernet).

**Step 3** Verify that the optical power and the optical signal-to-noise range (OSNR) of the incoming Client-Rx port optical signal are within the accepted ranges. You can find XFP/SFP ranges in the "Hardware Specifications" appendix of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Step 4** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

## 2.7.55 GE-OOSYNC (TRUNK)

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Objects: TRUNK

The Gigabit Ethernet Out of Synchronization alarm applies to TXP_MR_10G,TXP_MR_10E, TXP_MR_2.5G,TXPP_MR_2.5G,MXP_MR_2.5G and MXPP_MR_2.5G cards only when the ITU-T G.709 encapsulation framer is disabled.

**Note** For general information about MXP and TXP cards, refer to the "Card Reference" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For information about provisioning them, refer to the "Provision Transponder and Muxponder Cards" chapter.

### Clear the GE-OOSYNC (TRUNK) Alarm

**Step 1** Verify that ITU-T G.709 encapsulation is disabled:

a. Double-click the card to display the card view.

b. Click the **Provisioning > OTN > OTN Lines** tabs.

c. If the G.709 OTN column says Enable, choose **Disable** from the drop-down list.

d. Click **Apply**.

**Step 2** For the TRUNK-RX port, double-click the card and click the **Performance > OTN PM > FEC PM** tabs. If post-FEC errors are present, troubleshoot this problem first. If not, move to next step.

**Step 3** Verify the status of far-end TXP/MXP connected to the faulty near-end card. Look for any alarms reported by the Client-Rx port of far-end card. If these alarms exist, troubleshoot them.

**Step 4** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

## 2.7.56 HIBATVG

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: PWR

The High Voltage Battery alarm occurs in a –48 VDC environment when a battery lead input voltage exceeds the high power threshold. This threshold, with a default value of –52 VDC, is user-provisionable. The alarm remains raised until the voltage remains under the threshold for 120 seconds. (For information about changing this threshold, refer to the “Turn Up Node” chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

### Clear the HIBATVG Alarm

**Step 1** The problem is external to the ONS system. Troubleshoot the power source supplying the battery leads.

**Step 2** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

## 2.7.57 HI-CCVOLT

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: BITS

The 64K Composite Clock High NE Voltage alarm occurs when the 64K signal peak voltage exceeds 1.1 VDC.

### Clear the HI-CCVOLT Condition

**Step 1** Lower the source voltage to the clock.

**Step 2** If the condition does not clear, add more cable length or add a 5 dBm attenuator to the cable.

**Step 3** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

## 2.7.58 HI-LASERBIAS

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Objects: 2R, EQPT, ESCON, FC, GE, ISC, OCN/STMN, PPM, TRUNK

The Equipment High Transmit Laser Bias Current alarm is raised against TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, MXP_2.5G_10G, and OC192-XFP card laser performance. The alarm indicates that the card laser has reached the maximum laser bias tolerance.

Laser bias typically starts at about 30 percent of the manufacturer maximum laser bias specification and increases as the laser ages. If the HI-LASERBIAS alarm threshold is set at 100 percent of the maximum, the laser usability has ended. If the threshold is set at 90 percent of the maximum, the card is still usable for several weeks or months before it needs to be replaced.

**Note** For general information about MXP and TXP cards, refer to the "Card Reference" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*. Specific hardware values are listed in the "Hardware Specifications" appendix of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

### Clear the HI-LASERBIAS Alarm

**Step 1** Complete the "Clear the LASEREOL Alarm" procedure on page 2-62, which can include replacing the card. Replacement is not urgent and can be scheduled during a maintenance window.

**Caution** Removing an active card can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "2.9.1 Protection Switching, Lock Initiation, and Clearing" section on page 2-149 for commonly used traffic-switching procedures.

**Step 2** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.59 HI-LASERTEMP

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Objects: EQPT, OCN/STMN, PPM

The Equipment High Laser Optical Transceiver Temperature alarm applies to the TXP and MXP cards. HI-LASERTEMP occurs when the internally measured transceiver temperature exceeds the card setting by 35.6 degrees F (2 degrees C). A laser temperature change affects the transmitted wavelength.

When the TXP or MXP card raises this alarm, the laser is automatically shut off. The LOS (OCN/STMN) alarm is raised at the far-end node and the "DUP-IPADDR" alarm, page 2-32, is raised at the near end. (For instructions to clear either of these alarms, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 Troubleshooting Guide* or *Cisco ONS 15454SDH Troubleshooting Guide*.)

**Note** For information about MXP and TXP cards and PPMs (SFPs), refer to the "Card Reference" and "Turn Up a Node" chapters, respectively, in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

### Clear the HI-LASERTEMP Alarm

**Step 1** In node view, double-click the TXP or MXP card to open the card view.

**Step 2** Click the **Performance > Optics PM > Current Values** tabs.

**Step 3** Verify the card laser temperature levels. Maximum, minimum, and average laser temperatures are shown in the Current column entries in the Laser Temp rows.

**Step 4** Complete the "Reset a Card in CTC" procedure on page 2-152 for the MXP or TXP card.

**Step 5** If the alarm does not clear, complete the "Physically Replace a Card" procedure on page 2-154 for the reporting MXP or TXP card.

**Step 6** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.60 HI-RXPOWER

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Objects: 2R, ESCON, FC, GE, ISC, OCN/STMN, TRUNK

The Equipment High Receive Power alarm is an indicator of the optical signal power that is transmitted to the TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, MXP_2.5G_10G, or OC192-XFP card. HI-RXPOWER occurs when the measured optical power of the received signal exceeds the threshold. The threshold value is user-provisionable.

**Note** For general information about MXP and TXP cards and their power levels, refer to the "Card Reference" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For information about provisioning them, refer to the "Provision Transponder and Muxponder Cards" chapter.

### Clear the HI-RXPOWER Alarm

**Step 1** Check the PM of the TRUNK-RX port. Verify that received power is above the optics threshold:

a. Double-click the card to display the card view.

b. For the TRUNK-RX port, double-click the card and click the **Performance > Optics PM > Historical PM** tabs, choose the port in the **Port** drop-down list, and click **Refresh**.

c. Compare the refreshed PM values with the threshold (ensuring that it is above the threshold value) by clicking the **Performance > Optics PM > Current Values** tabs.

d. Ensure that a proper threshold has been provisioned for the receive value. (Refer to the "Provision Transponder and Muxponder Cards" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.) If an incorrect threshold has been set, adjust it to a value within the allowed limits. If instead the alarm condition does not clear, move to next step.

**Step 2** Verify that the Trunk-Rx port is cabled correctly, and clean the fiber connecting the faulty TXP/MXP to the Drop port of the DWDM card (32DMX, 32DMX-O or AD-xC-xx.x). If no site cleaning practices are available, refer to the fiber cleaning procedure in the "Maintain the Node" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Step 3** Determine whether a bulk attenuator is specified by the Cisco MetroPlanner (MP) design. If so, verify that the proper fixed attenuation value has been used.

**Step 4** Using a test set, check the optical power value of the Drop port of the DWDM card (32DMX, 32DMX-O or AD-xC-xx.x) connected to the faulty TXP/MXP. If the read value is different (+1 dBm or –1 dBm) from the ANS setpoint for "Padd&drop-Drop power," move to next step.

**Step 5** Look for and troubleshoot any alarm reported by the DWDM cards belonging to the OCHNC circuit destinating at the faulty TXP/MXP. Possible alarms include amplifier Gain alarms (the "GAIN-HDEG" alarm on page 2-44, the "GAIN-HFAIL" alarm on page 2-45, the "GAIN-LDEG" alarm on page 2-46, or "GAIN-LFAIL" alarm on page 2-47); APC alarms ("APC-CORRECTION-SKIPPED" alarm on page 2-17 or "APC-OUT-OF-RANGE" alarm on page 2-19), or LOS-P alarms on the Add or Drop ports involved in the OCHNC circuit.

**Step 6** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.61 HITEMP

Default Severity: Critical (CR), Service-Affecting (SA) for NE; Default Severity: Minor (MN), Non-Service-Affecting (NSA) for EQPT

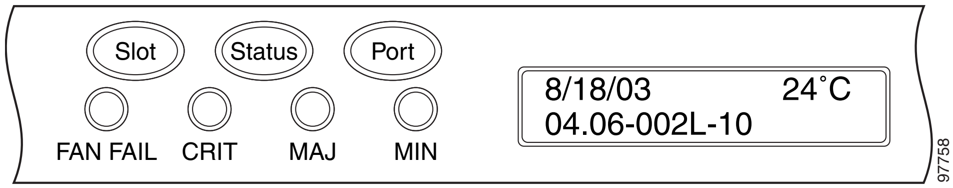
Logical Objects: EQPT, NE

The High Temperature alarm occurs when the temperature of the ONS system is above 122 degrees F (50 degrees C).

### Clear the HITEMP Alarm

**Step 1** View the temperature displayed on the ONS system LCD front panel. For example, the ONS 15454 front panel is illustrated in Figure 2-1.

*Figure 2-1 Shelf LCD Panel*




**Step 2** Verify that the environmental temperature of the room is not abnormally high.

**Step 3** If the room temperature is not abnormal, physically ensure that nothing prevents the fan-tray assembly from passing air through the ONS system shelf.

**Step 4** If airflow is not blocked, physically ensure that blank faceplates fill the ONS system shelf empty slots. Blank faceplates help airflow.

**Step 5** If faceplates fill the empty slots, determine whether the air filter needs replacement. Refer to the "Inspect, Clean, and Replace the Reusable Air Filter" procedure on page 2-156.

**Step 6** If the fan does not run or the alarm persists, complete the "Replace the Fan-Tray Assembly" procedure on page 2-158.

**Note** The fan should run immediately when correctly inserted.

**Step 7** If the replacement fan-tray assembly does not operate correctly, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC to report a Service-Affecting (SA) problem (1 800 553-2447) if it applies to the NE, or a Non-Service-Affecting (NSA) problem if it applies to equipment.

## 2.7.62 HI-TXPOWER

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Objects: 2R, EQPT, ESCON, FC, GE, ISC, OCN/STMN, PPM, TRUNK

The Equipment High Transmit Power alarm is an indicator on the TXP_MR_E, TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, MXP_2.5G_10G, or OC192-XFP card transmitted optical signal power. HI-TXPOWER occurs when the measured optical power of the transmitted signal exceeds the threshold.

**Note** For general information about MXP and TXP cards and power levels, refer to the "Card Reference" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For information about provisioning them, refer to the "Provision Transponder and Muxponder Cards" chapter.

### Clear the HI-TXPOWER Alarm

**Step 1** Check the PM of the Trunk-Tx port. Verify that received power is above the optics threshold:

**a.** Double-click the card to display the card view.

b. For the Trunk-Tx port, double-click the card and click the **Performance > Optics PM > Historical PM** tabs, choose the port in the **Port** drop-down list, and click **Refresh**.

c. Compare the refreshed PM values with the threshold (ensuring that it is above the threshold value) by clicking the **Performance > Optics PM > Current Values** tabs.

d. Ensure that a proper threshold has been provisioned for the receive value. (Refer to the "Provision Transponder and Muxponder Cards" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.) If an incorrect threshold has been set, adjust it to a value within the allowed limits. If instead the alarm condition does not clear, move to next step.

**Step 2** Physically verify, by using a standard power meter that the optical output power is overcoming the expected power threshold. If so, the card should be replaced at first opportunity

**Note** The higher power level is not a major issue for the DWDM card (32MUX-O, 32WSS-O, or AD-xC-xx.x) connected to the faulty TXP/MXP, because an internal VOA can automatically decrease the optical power to the expected level.

**Step 3** Complete the "Physically Replace a Card" procedure on page 2-154.

**Step 4** If the alarm does not clear after the replacement, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem. If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.63 HLDOVRSYNC

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: NE-SREF

The Holdover Synchronization Mode condition is caused by loss of the primary and second timing references in the node. Timing reference loss occurs when line coding on the timing input is different from the configuration on the node, and it often occurs during the selection of a new node reference clock. The condition clears when primary or second timing is reestablished. After the 24-hour holdover period expires, timing slips could begin to occur on an ONS system relying on an internal clock.

### Clear the HLDOVRSYNC Condition

**Step 1** Clear additional alarms that relate to timing, such as:


- 2.7.47 FRNGSYNC, page 2-44
- 2.7.48 FSTSYNC, page 2-44
- 2.7.77 LOF (BITS), page 2-64
- 2.7.86 LOS (BITS), page 2-70
- 2.7.109 MANSWTOINT, page 2-89
- 2.7.110 MANSWTOPRI, page 2-89
- 2.7.111 MANSWTOSEC, page 2-89
- 2.7.112 MANSWTOTHIRD, page 2-89

- 2.7.188 SWTOPRI, page 2-135
- 2.7.189 SWTOSEC, page 2-136
- 2.7.190 SWTOTHIRD, page 2-136
- 2.7.191 SYNC-FREQ, page 2-136
- 2.7.193 SYNCPRI, page 2-138
- 2.7.194 SYNCSEC, page 2-138
- 2.7.195 SYNCTHIRD, page 2-139


**Step 2** Reestablish a primary and secondary timing source according to local site practice. If none exists, refer to the "Turn Up Network" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Step 3** If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

## 2.7.64 I-HITEMP

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: NE

The Industrial High Temperature alarm occurs when the temperature of the ONS system is above 149 degrees F (65 degrees C) or below –40 degrees F (–40 degrees C). This alarm is similar to the HITEMP alarm but is used for the industrial environment. If this alarm is used, you can customize your alarm profile to ignore the lower-temperature HITEMP alarm.

### Clear the I-HITEMP Alarm

**Step 1** Complete the "Clear the HITEMP Alarm" procedure on page 2-52.

**Step 2** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call TAC (1-800-553-2447) in order to report a Service-Affecting (SA) problem.

## 2.7.65 IMPROPRMVL

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Objects: EQPT, PPM

The Improper Removal (IMPROPRMVL) alarm occurs under the following conditions:

- A card is removed when the card was rebooting. It is recommended that after the card completely reboots, delete the card in CTC and only then remove the card physically. When you delete the card, CTC loses connection with the node view (single-shelf mode) or shelf view (multishelf mode), and goes to network view.
- When a card is physically removed from its slot before it is deleted from CTC. It is recommended that any card be deleted in CTC before physically removing the card from the chassis.

**Note** CTC provides the user approximately 15 seconds to physically remove the card before it begins rebooting the card.
It can take up to 30 minutes for software to be updated on a standby TCC2/TCC2P card.

- A card is inserted into a slot but is not fully plugged into the backplane.
- A PPM (SFP) is provisioned but the physical module is not inserted into the port.
- Removal of an SFP from the client ports of a Y-cable protection group card causes an IMPROPRMVL (PPM) alarm.

  For more information about protection schemes, refer to the "Manage the Node" chapter of the *Cisco ONS 15454 DWDM Procedure Guide*.

  For more information about provisioning PPMs (SFPs), refer to the "Turn Up a Node" chapter of the *Cisco ONS 15454 DWDM Procedure Guide*. For specific PPM (SFP) values, refer to the "Hardware Specifications" appendix of the *Cisco ONS 15454 DWDM Reference Manual*.
- Electrical issues such as short circuit or failure of DC-DC conversion.

## Clear the IMPROPRMVL Alarm

**Step 1** In node view, right-click the card reporting the IMPROPRMVL.

**Step 2** Choose **Delete** from the shortcut menu.

**Note** CTC does not allow you to delete the reporting card if the card is in service, does have circuits mapped to it, is paired in a working protection scheme, has DCC enabled, or is used as a timing reference.

**Step 3** If any ports on the card are in service, place them out of service (OOS,MT):

**Caution** Before placing a port out of service (OOS,MT) or OOS,DSBLD, ensure that no live traffic is present.

a. In node view, double-click the reporting card to open the card view.

b. Click the **Provisioning > Line** tabs.

c. Click the Admin State column of any in-service (IS) ports.

d. Choose **OOS,MT** (or **Locked,maintenance**) to take the ports out of service.

**Step 4** If a circuit has been mapped to the card, complete the "Delete a Circuit" procedure on page 2-155.

**Caution** Before deleting the circuit, ensure that the circuit does not carry live traffic.

**Step 5** If the card is paired in a protection scheme, delete the protection group by completing the following steps:

a. Click **View > Go to Previous View** to return to node view.

b. If you are already in node view, click the **Provisioning > Protection** tab.

c. Click the protection group of the reporting card.

d. Click **Delete**.

**Step 6** If the card is provisioned for DCC, delete the DCC provisioning by completing the following steps:

a. Click the ONS system **Provisioning > Comm Channels > SDCC** (or **Provisioning > Comm Channels > MS DCC**) tabs.

b. Click the slots and ports listed in DCC terminations.

c. Click **Delete** and click **Yes** in the dialog box that appears.

**Step 7** If the card is used as a timing reference, change the timing reference by completing the following steps:

a. Click the **Provisioning > Timing > General** tabs.

b. Under NE Reference, click the drop-down arrow for **Ref-1**.

c. Change Ref-1 from the listed OC-N/STM-N card to **Internal Clock**.

d. Click **Apply**.

**Step 8** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

## 2.7.66 INCOMPATIBLE-SEND-PDIP

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: SYSTEM

The Incompatible Software alarm is raised when CTC'S send PDI-P provisioning differs from the host node's provisioning.

### Clear the INCOMPATIBLE-SEND-PDIP Alarm

**Step 1** Reconfigure CTC's send PDI-P alarm capability to align with the host node settings.

**Step 2** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call TAC (1-800-553-2447).

## 2.7.67 INCOMPATIBLE-SW

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: SYSTEM

The Incompatible Software alarm is raised when CTC cannot connect to the NE due to differing, incompatible versions of software between CTC and the NE. The alarm is cleared by restarting CTC in order to redownload the CTC JAR files from the NE.

### Clear the INCOMPATIBLE-SW Alarm

**Step 1** Restart the CTC application.

**Step 2** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call TAC (1-800-553-2447).

## 2.7.68 INTRUSION-PSWD

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: NE

The Security Intrusion Incorrect Password condition occurs after a user attempts a provisionable (by Superuser) number of unsuccessful logins, a login with an expired password, or an invalid password. The alarmed user is locked out of the system, and INTRUSION-PSWD condition is raised. This condition is only shown in Superuser login sessions, not in login sessions for lower-level users. The INTRUSION-PSWD condition is automatically cleared when a provisionable lockout timeout expires, or it can be manually cleared in CTC by the Superuser if the lockout is permanent.

### Clear the INTRUSION-PSWD Condition

**Step 1** Log in as a user ID with superuser rights. (For more information about this, refer to the "Connect the PC and Log Into the GUI" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.)

**Step 2** Click the **Provisioning > Security > Users** tabs.

**Step 3** Click **Clear Security Intrusion Alarm**.

**Step 4** If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.69 INVMACADR

Default Severity: Major (MJ), Non-Service Affecting (NSA)

Logical Object: AIP

The Equipment Failure Invalid MAC Address alarm occurs when the ONS system MAC address is invalid. Each ONS system has a unique, permanently assigned MAC address. The address resides on an AIP EEPROM. The TCC2/TCC2P reads the address value from the AIP chip during boot-up and keeps this value in its synchronous dynamic RAM (SDRAM).

Under normal circumstances, the read-only MAC address can be viewed in the Provisioning > Network tab in CTC.

The ONS system uses both IP and MAC addresses for circuit routing. When an INVMACADR alarm exists on a node, you see a PARTIAL circuit in the CTC circuit status column. The circuit works and is able to carry traffic, but CTC cannot logically display the circuit end-to-end information.

An invalid MAC address can be caused when:

- There is a read error from the AIP during boot-up; in this case, the reading TCC2/TCC2P uses the default MAC address (00-10-cf-ff-ff-ff).
- There is a read error occurring on one of the redundant TCC2/TCC2Ps that read the address from the AIP; these cards read the address independently and could therefore each read different address values.
- An AIP component failure causes a read error.
- The ribbon cable connecting the AIP card to the backplane is bad.

## Clear the INVMACADR Alarm

**Step 1** Check for any outstanding alarms that were raised against the active and standby TCC2/TCC2P and resolve them.

**Step 2** If the alarm does not clear, determine whether the LCD display on the fan tray (Figure 2-1 on page 2-53) is blank or if the text is garbled. If so, proceed to Step 8. If not, continue with Step 3.

**Step 3** At the earliest maintenance window, reset the standby TCC2/TCC2P:

**Note** The reset requires approximately five minutes. Do not perform any other step until the reset is complete.

**a.** Log into a node on the network. If you are already logged in, continue with Step b.

**b.** Identify the active TCC2/TCC2P.

A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

**c.** Right-click the standby TCC2/TCC2P in CTC.

**d.** Choose **Reset Card** from the shortcut menu.

**e.** Click **Yes** in the Are You Sure dialog box.

The card resets, the FAIL LED blinks on the physical card, and connection to the node is lost. CTC switches to network view.

**f.** Verify that the reset is complete and error-free, and that no new related alarms appear in CTC. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

**g.** Double-click the node and ensure that the reset TCC2/TCC2P is still in standby mode and that the other TCC2/TCC2P is active.

A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

**h.** Ensure that no new alarms associated with this reset appear in the CTC Alarms window.

If the standby TCC2/TCC2P fails to boot into standby mode and reloads continuously, the AIP is probably defective. In this case, the standby TCC2/TCC2P is unsuccessfully attempting to read the EEPROM located on the AIP. The TCC2/TCC2P reloads until it reads the EEPROM. Proceed to Step 8.

**Step 4** If the standby TCC2/TCC2P rebooted successfully into standby mode, complete the "Remove and Reinsert (Reseat) the Standby TCC2/TCC2P Card" procedure on page 2-153.

Resetting the active TCC2/TCC2P causes the standby TCC2/TCC2P to become active. The standby TCC2/TCC2P keeps a copy of the chassis MAC address. If its stored MAC address is valid, the alarm should clear.

**Step 5** After the reset, note whether or not the INVMACADR alarm has cleared or is still present.

**Step 6** Complete the "Reset an Active TCC2/TCC2P Card and Activate the Standby Card" procedure on page 2-152 again to place the standby TCC2/TCC2P back into active mode.

After the reset, note whether or not the INVMACADR alarm has cleared or is still present. If the INVMACADR alarm remains standing through both TCC2/TCC2P resets, this indicates that the AIP is probably defective. Proceed to Step 8.

If the INVMACADR was raised during one TCC2/TCC2P reset and cleared during the other, the TCC2/TCC2P that was active while the alarm was raised needs to be replaced. Continue with Step 7.

**Step 7** If the faulty TCC2/TCC2P is currently in standby mode, complete the "Physically Replace a Card" procedure on page 2-154 for this card. If the faulty TCC2/TCC2P is currently active, during the next available maintenance window complete the "Reset an Active TCC2/TCC2P Card and Activate the Standby Card" procedure on page 2-152 and then complete the "Physically Replace a Card" procedure on page 2-154.

**Note** If the replacement TCC2/TCC2P is loaded with a different software version from the current TCC2/TCC2P, the card boot-up could take up to 30 minutes. During this time, the card LEDs flicker between Fail and Act/Sby as the active TCC2/TCC2P version software is copied to the new standby card.

**Step 8** Open a case with Cisco TAC (1 800 553-2447) for assistance with determining the node's previous MAC address.

**Step 9** Replace the ribbon cable between the system board and the AIP with a known-good cable.

**Step 10** If the alarm persists, complete the "Replace an Alarm Interface Panel" procedure located in the "Alarm Troubleshooting" chapter of the *Cisco ONS 15454 Troubleshooting Guide*.

**Step 11** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.70 LASER-APR

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: AOTS

The Laser Automatic Power Reduction (APR) alarm condition is raised by OSC-CSM, OSCM, OPT-BST, and OPT-PRE cards when the laser is working in power reduction mode. The condition clears as soon as safety conditions are released and the power value reaches the normal setpoint.

**Note** LASER-APR is an informational condition and does not require troubleshooting. For more information about optical amplifier APR, refer to the "Card Reference" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

## 2.7.71 LASERBIAS-DEG

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Objects: AOTS, OTS

The Laser Bias Current Degrade alarm occurs on an amplifier card (OPT-BST or OPT-PRE) when laser aging causes a degrade, but not failure, of laser transmission. The card should be replaced at the next opportunity.

**Note** For general information about optical amplifier cards, refer to the "Card Reference" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For information about changing their settings, refer to the "Change DWDM Card Settings" chapter.

### Clear the LASERBIAS-DEG Alarm

**Step 1** For the alarmed card, complete the "Physically Replace a Card" procedure on page 2-154 at the next opportunity.

**Step 2** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.72 LASERBIAS-FAIL

Default Severity: Major (MJ), Non-Service-Affecting (NSA)

Logical Object: AOTS

The Laser Bias Current Failure alarm occurs on an amplifier card (OPT-BST or OPT-PRE) when the laser control circuit fails or if the laser itself fails service. The card must be replaced to restore traffic.

**Note** For general information about optical amplifier cards, refer to the "Card Reference" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For information about changing their settings, refer to the "Change DWDM Card Settings" chapter.

### Clear the LASERBIAS-FAIL Alarm

**Step 1** For the alarmed card, complete the "Physically Replace a Card" procedure on page 2-154.

**Step 2** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.73 LASEREOL

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: OCN/STMN

The Laser Approaching End of Life alarm applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G cards. It is typically accompanied by the "HI-LASERBIAS" alarm, page 2-50. It is an indicator that the laser in the card must be replaced. How soon the replacement must happen depends upon the HI-LASERBIAS threshold. If the threshold is set under 100 percent, the laser replacement can usually be done during a maintenance window. But if the HI-LASERBIAS threshold is set at 100 percent and is accompanied by data errors, the card must be replaced sooner.

**Note** For general information about MXP and TXP cards, refer to the "Card Reference" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For information about provisioning them, refer to the "Provision Transponder and Muxponder Cards" chapter.

### Clear the LASEREOL Alarm

**Step 1** Complete the "Physically Replace a Card" procedure on page 2-154.

**Step 2** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.74 LASERTEMP-DEG

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: AOTS

The Laser Temperature Degrade alarm occurs when the Peltier control circuit fails on an amplifier card (OPT-BST or OPT-PRE). The Peltier control provides cooling for the amplifier. The card should be replaced at the next opportunity.

**Note** For general information about DWDM cards, refer to the "Card Reference" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For information about changing their settings, refer to the "Change DWDM Card Settings" chapter.

### Clear the LASERTEMP-DEG Alarm

**Step 1** For the alarmed DWDM card, complete the "Physically Replace a Card" procedure on page 2-154 at the next opportunity.

**Step 2** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.75 LOCKOUT-REQ (2R, EQPT, ESCON, FC, GE, ISC)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Objects: 2R, EQPT, ESCON, FC, GE, ISC

The Lockout Switch Request on Facility or Equipment condition occurs in a Y-cable MXP or TXP client protection group for the above-listed clients when a user initiates a lockout switch request. The condition is raised when you lock traffic onto the working port with the Lock On command (thus locking it off the protect port), or you lock it off the protect port with the Lock Out command. In either case, the protect port will show "Lockout of Protection," and the Conditions window will show the LOCKOUT-REQ condition.

A lockout prevents protection switching. Clearing the lockout again allows protection switching and clears the LOCKOUT-REQ condition.

### Clear the LOCKOUT-REQ (2R, EQPT, ESCON, FC, GE, ISC) Condition

**Step 1** Complete the "Clear a Lock-On or Lockout Command" procedure on page 2-151.

**Step 2** If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.76 LOCKOUT-REQ (TRUNK)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: TRUNK

The Lockout Switch Request on Facility or Equipment condition occurs in an MXP or TXP trunk port splitter protection group when you lock traffic onto the working port with the Lock On command (thus locking it off the protect port), or lock it off the protect port with the Lock Out command. In either case, the protect port will show "Lockout of Protection," and the Conditions window will show the LOCKOUT-REQ condition.

A lockout prevents protection switching. Clearing the lockout again allows protection switching and clears the LOCKOUT-REQ condition.

### Clear the LOCKOUT-REQ (TRUNK) Condition

**Step 1** Complete the "Clear a Lock-On or Lockout Command" procedure on page 2-151.

**Step 2** If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.77 LOF (BITS)

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: BITS

The Loss of Frame (LOF) BITS alarm occurs when a port on theTCC2/TCC2P BITS input detects an LOF on the incoming BITS timing reference signal. LOF indicates that the receiving ONS system has lost frame delineation in the incoming data.

**Note** The procedure assumes that the BITS timing reference signal is functioning properly. It also assumes the alarm is not appearing during node turn-up.

### Clear the LOF (BITS) Alarm

**Step 1** Verify that the line framing and line coding match between the BITS input and the TCC2/TCC2P:

a. In node or card view, note the slot and port reporting the alarm.

b. Find the coding and framing formats of the external BITS timing source. The formats should be in the user documentation for the external BITS timing source or on the timing source itself.

c. Click the **Provisioning > Timing > BITS Facilities** tabs.

d. Verify that the Coding setting matches the coding of the BITS timing source, either B8ZS or AMI.

e. If the coding does not match, click **Coding** and choose the appropriate coding from the drop-down list.

f. Verify that Framing matches the framing of the BITS timing source, either ESF or SF (D4).

g. If the framing does not match, click **Framing** and choose the appropriate framing from the drop-down list.

**Note** On the timing subtab, the B8ZS coding field is normally paired with ESF in the Framing field and the AMI coding field is normally paired with SF (D4) in the Framing field.

**Step 2** If the alarm does not clear when the line framing and line coding match between the BITS input and the TCC2/TCC2P, complete the "Physically Replace a Card" procedure on page 2-154 for the TCC2/TCC2P.

**Step 3** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

## 2.7.78 LOF (TRUNK)

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: TRUNK

The Loss of Frame for the DWDM trunk applies to the trunk optical or electrical signal that is carried to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G cards. It indicates that the receiving ONS system has lost frame delineation in the incoming data from trunk that serves the cards. LOF occurs when the SONET overhead loses a valid framing pattern for 3 milliseconds. Receiving two consecutive valid A1/A2 framing patterns clears the alarm.

### Clear the LOF (TRUNK) Alarm

**Step 1** Using site practices, verify fiber continuity to the port. Refer to the "Network Reference" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide* for a procedure to detect a fiber cut.

**Step 2** If the cabling is good, verify that the correct port is in service by completing the following steps:

a. Confirm that the LED is correctly illuminated on the physical card. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

b. To determine whether the port is in service, double-click the card in CTC to open the card view.

c. Click the **Provisioning > Line** tabs.

d. Verify that the Admin State column lists the port as IS (or Unlocked).

e. If the Admin State column lists the port as OOS,MT (or Locked,maintenance) or OOS,DSBLD, click the column and choose **IS** , or **Unlocked**.

f. Click **Apply**.

**Step 3** If the correct port is in service, clean the fiber according to site practice. If no site practice exists, complete the fiber cleaning procedure in the "Maintain the Node" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Step 4** If the alarm does not clear, verify that the power level of the optical signal is within the TXP or MXP card receiver specifications. (These specifications are listed in the "Hardware Specifications" appendix of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.)

**Step 5** If the optical power level is within specifications, use an optical test set to verify that a valid signal exists on the line. For specific procedures to use the test set equipment, consult the manufacturer. Test the line as close to the receiving card as possible.

**Step 6** If a valid signal exists, replace the connector on the backplane.

**Step 7** Repeat Steps 1 to 6 for any other port on the card reporting the LOF.

**Step 8** If the alarm does not clear, look for and troubleshoot any other alarm that could identify the source of the problem.

**Step 9** If no other alarms exist that could be the source of the LOF, or if clearing an alarm did not clear the LOF, complete the "Physically Replace a Card" procedure on page 2-154 for the reporting card.

**Step 10** If the alarm does not clear, or if you need assistance conducting network troubleshooting tests, call Cisco TAC (1 800 553-2447) to report a Service-Affecting (SA) problem.

## 2.7.79 LOGBUFR90

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: SYSTEM

The Log Buffer Over 90 alarm indicates that the per-NE queue of incoming alarm, event, or update capacity of 5000 entries is over 90 percent full. LOGBUFR90 will clear if CTC recovers. If it does not clear, LOGBUFROVFL occurs.

**Note** LOGBUFR90 is an informational alarm and does not require troubleshooting.

## 2.7.80 LOGBUFROVFL

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: SYSTEM

The Log Buffer Overflow alarm indicates that the CTC per-NE queue of incoming alarm, event, or updates, which has a capacity of 5,000 entries, has overflowed. This happens only very rarely. However if it does, you must restart the CTC session. It is likely that some updates will have been missed if this alarm occurs.

### Clear the LOGBUFROVFL Alarm

**Step 1** Restart the CTC session.

**Step 2** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call TAC (1-800-553-2447).

## 2.7.81 LO-LASERBIAS

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Objects: EQPT, OCN/STMN, PPM

The Equipment Low Transmit Laser Bias Current alarm is raised against the TXP and MXP card laser performance. The alarm indicates that the card laser has reached the minimum laser bias tolerance.

If the LO-LASERBIAS alarm threshold is set at 0 percent (the default), the laser's usability has ended. If the threshold is set at 5 percent to 10 percent, the card is still usable for several weeks or months before you need to replace it.

**Note** For general information about MXP and TXP cards, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For information about provisioning them, refer to the "Provision Transponder and Muxponder Cards" chapter.

### Clear the LO-LASERBIAS Alarm

**Step 1** Complete the "Physically Replace a Card" procedure on page 2-154.

**Step 2** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.82 LO-LASERTEMP

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Objects: EQPT, OCN/STMN, PPM

The Equipment Low Laser Optical Transceiver Temperature alarm applies to the TXP and MXP cards. LO-LASERTEMP occurs when the internally measured transceiver temperature falls below the card setting by35.6 degrees F or 2 degrees C. A laser temperature change affects the transmitted wavelength. (This temperature is equivalent to about 200 picometers of wavelength.)

When the TXP or MXP card raises this alarm, the laser is automatically shut off. The An LOS for OCN/STMN is raised at the far-end node and the "DUP-IPADDR" alarm on page 2-32 is raised at the near end. (Both of these alarms are described in the "Alarm Troubleshooting" chapter of the *Cisco ONS 15454 Troubleshooting Guide* or the *Cisco ONS 15454SDH Troubleshooting Guide*). To verify the card laser temperature level, double-click the card in node view and click the **Performance > Optics PM > Current Values** tabs. Maximum, minimum, and average laser temperatures are shown in the Current column entries in the Laser Temp rows.

**Note** For general information about MXP and TXP cards, refer to the "Card Reference" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For information about provisioning them, refer to the "Provision Transponder and Muxponder Cards" chapter.

### Clear the LO-LASERTEMP Alarm

**Step 1** Complete the "Reset a Card in CTC" procedure on page 2-152 for the reporting MXP or TXP card.

**Step 2** If the alarm does not clear, complete the "Physically Replace a Card" procedure on page 2-154 for the reporting MXP or TXP card.

**Step 3** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.83 LOM

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: TRUNK

The Optical Transport Unit (OTU) Loss of Multiframe alarm is an OTN alarm for the trunk port and occurs when the Multi Frame Alignment Signal (MFAS) is corrupted. The alarm applies to MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, TXP_MR_10E, and TXPP_MR_2.5G cards when the MFAS) overhead field is errored for more than five frames and persists for more than 3 milliseconds.

**Note** For general information about MXP and TXP cards, refer to the "Card Reference" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For information about provisioning them, refer to the "Provision Transponder and Muxponder Cards" chapter.

### Clear the LOM Alarm

**Step 1** Ensure that the fiber connector for the card is completely plugged in. For more information about fiber connections and card insertion, refer to the "Turn Up a Node" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Step 2** If the bit error rate (BER) threshold is correct and at the expected level, use an optical test set to measure the power level of the line to ensure it is within guidelines. For specific procedures to use the test set equipment, consult the manufacturer.

**Step 3** If the optical power level is good, verify that optical receive levels are within the acceptable range. Ranges for ONS 15454 DWDM cards are located in the "Hardware Specifications" appendix of the *Cisco ONS 15454 DWDM Installation and Operations Guide.*

**Step 4** If receive levels are good, clean the fibers at both ends according to site practice. If no site practice exists, complete the fiber cleaning procedure in the "Maintain the Node" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Step 5** If the condition does not clear, verify that single-mode fiber is used.

**Step 6** If the fiber is of the correct type, verify that a single-mode laser is used at the far-end node.

**Step 7** Clean the fiber connectors at both ends for a signal degrade according to site practice.

**Step 8** Verify that a single-mode laser is used at the far end.

**Step 9** If the problem does not clear, the transmitter at the other end of the optical line could be failing and require replacement. Refer to the "2.9.3 Physical Card Reseating, Resetting, and Replacement" section on page 2-153.

**Step 10** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

## 2.7.84 LO-RXPOWER

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Objects: 2R, ESCON, FC, GE, ISC, OCN/STMN, TRUNK

The Equipment Low Receive Power alarm is an indicator for TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, MXP_2.5G_10G and OC192-XFP card received optical signal power. LO-RXPOWER occurs when the measured optical power of the received signal falls below the threshold value, which is user-provisionable.

**Note** For general information about MXP and TXP cards and their necessary levels, refer to the "Card Reference" chapter and the "Hardware Specifications" appendix in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

### Clear the LO-RXPOWER Alarm

**Step 1** Check the PM of the TRUNK-RX port. Verify that received power is above the optics threshold:

**a.** Double-click the card to display the card view.

b. For the TRUNK-RX port, double-click the card and click the **Performance > Optics PM > Historical PM** tabs, choose the port in the **Port** drop-down list, and click **Refresh**.

c. Compare the refreshed PM values with the threshold (ensuring that they are above the threshold value) by clicking the **Performance > Optics PM > Current Values** tabs.

d. Ensure that a proper threshold has been provisioned for the receive value. (Refer to the "Provision Transponder and Muxponder Cards" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.) If an incorrect threshold has been set, adjust it to a value within the allowed limits. If instead the alarm condition does not clear, move to next step.

**Step 2** Verify that the Trunk-Rx port is cabled correctly, and clean the fiber connecting the faulty TXP/MXP to the Drop port of the DWDM card (32DMX, 32DMX-O or AD-xC-xx.x). If no site cleaning practices are available, refer to the "Maintain the Node" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Step 3** Determine whether a bulk attenuator is specified by the Cisco MetroPlanner design. If so, verify that the proper fixed attenuation value has been used.

**Step 4** Using a test set, check the optical power value of the Drop port of the DWDM card (32DMX, 32DMX-O or AD-xC-xx.x) connected to the faulty TXP/MXP. If the read value is different (+1 dBm or –1 dBm) from the ANS setpoint for "Padd&drop-Drop power," move to next step. If not, complete the "Physically Replace a Card" section on page 2-154.

**Step 5** Look for any alarm reported by the DWDM cards belonging to the OCHNC circuit whose destination is the faulty TXP/MXP and first troubleshoot that alarm. Possible alarm related include: amplifier Gain alarms (the "GAIN-HDEG" alarm on page 2-44, the "GAIN-HFAIL" alarm on page 2-45, the "GAIN-LDEG" alarm on page 2-46, or "GAIN-LFAIL" alarm on page 2-47); APC alarms (the "APC-CORRECTION-SKIPPED" alarm on page 2-17 or "APC-OUT-OF-RANGE" alarm on page 2-19), and LOS-P alarms on the Add or Drop ports belonging to the OCHNC circuit.

**Step 6** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.85 LOS (2R)

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: 2R

The Loss of Signal for a 2R client applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G cards. The alarm is raised when the card port is not receiving input. An AIS is sent upstream.

**Caution** Always use the supplied electrostatic discharge wristband when working with a powered ONS system. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly. To verify cable continuity, follow site practices.

**Note** For general information about MXP and TXP cards, refer to the "Card Reference" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

### Clear the LOS (2R) Alarm

**Step 1** Ensure that the signal entering the Client-Rx port is provisioned with the correct physical-layer protocol.

**Step 2** Ensure that the signal feeding the Client-Rx port is provisioned with the correct line speed.

**Step 3** Check the PM of the Client-Rx port.

**Step 4** Verify that received power is above the optics threshold.

**Step 5** Ensure that a proper threshold has been provisioned. (Refer to the "Provision Transponder and Muxponder Cards" chapter, and/or the SFP/XFP plug-in specifications located in the "Hardware Specifications" appendix of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.) If an incorrect threshold has been set, adjust it to a value within the allowed limits.

**Step 6** Verify the proper cabling and clean the fibers according with the site practice. Cabling procedures are located in the "Turn Up a Node" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*, and a fiber-cleaning procedure is located in the "Maintain the Node" chapter.

**Step 7** Verify using an optical test set that a valid signal exists on the line and feeds the Client-Rx port. (For specific procedures to use the test set equipment, consult the manufacturer.) Test the line as close to the receiving card as possible. If the alarm condition does not clear, move to next step.

**Step 8** Complete the XFP/SFP installation procedure in the "Turn Up a Node" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide* or the "Physically Replace a Card" procedure on page 2-154 as appropriate for your purposes.

**Step 9** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) to report a Service-Affecting (SA) problem.

## 2.7.86 LOS (BITS)

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: BITS

The LOS (BITS) alarm indicates that the TCC2/TCC2P has an LOS from the BITS timing source. LOS for BITS means the BITS clock or the connection to it failed.

### Clear the LOS (BITS) Alarm

**Caution** Always use the supplied electrostatic discharge wristband when working with a powered ONS system. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

**Step 1** Verify the wiring connection from the BITS clock pin fields on the ONS system backplane to the timing source.

**Step 2** If wiring is good, verify that the BITS clock is operating properly.

**Step 3** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

## 2.7.87 LOS (ESCON)

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: ESCON

The ESCON LOS alarm occurs on the TXP_MR_2.5G or TXPP_MR_2.5G card when there is a loss of signal for this payload, usually due to a physical error such as incorrect cabling connections, faulty cabling, or a break. It can also be caused by an incorrectly configured SFP.

### Clear the LOS (ESCON) Alarm

**Step 1** Check for any upstream equipment failures that could cause the ESCON LOS alarm in this node.

**Step 2** If there is no cause upstream, verify cabling continuity from the transmitting port to the receiving port reporting this LOS. To verify cable continuity, follow site practices.

**Caution** Always use the supplied electrostatic discharge wristband when working with a powered ONS system. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

**Step 3** If the continuity is good, clean the fiber according to site practice. If none exists, complete the fiber-cleaning procedure in the "Maintain the Node" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Step 4** Ensure that the PPM (SFP) is correctly configured for this payload:

a. Double-click the card to open the card view.

b. Click the **Provisioning > Pluggable Port Modules** tabs.

c. Check the **Pluggable Port Modules** area for the PPM (SFP) associated with the port.

d. In the Pluggable Ports area, ensure that the rate for the errored PPM (SFP) is ESCON.

**Note** For information about provisioning PPMs (SFPs), refer to the "Turn Up a Node" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*. PPM (SFP) specifications are listed in the "Hardware Specifications" appendix.

**Step 5** If the physical cabling and PPM (SFP) are good but the alarm does not clear, verify that the correct port is actually in service:

a. Confirm that the LED is correctly lit on the physical TXP card.

A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

b. To determine whether the port is in service, double-click the card in CTC to open the card view.

c. Click the **Provisioning > Line** tabs.

d. Verify that the Admin State column lists the port as IS (or Unlocked).

e. If the Admin State column lists the port as OOS,MT (or Locked,maintenance) or OOS,DSBLD, click the column and choose **IS** , or **Unlocked**. Click **Apply**.

**Step 6** If the correct port is in service but the alarm has not cleared, use an optical test set to confirm that a valid signal exists on the line. For specific procedures to use the test set equipment, consult the manufacturer. Test the line as close to the receiving card as possible.

**Step 7** If the signal is valid, ensure that the transmit and receive outputs from the patch panel to your equipment are properly connected. For more information about fiber connections and terminations, refer to the "Turn Up a Node" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Step 8** If a valid signal exists but the alarm does not clear, replace the cable connector on the ONS system.

**Step 9** Repeat Steps 2 through 6 for any other port on the card that reports the LOS (ESCON).

**Step 10** If the alarm does not clear, the cabling could still be faulty despite correct attachments. Use the test set to locate the bad cable and replace it using the procedures in the "Manage the Node" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Step 11** If the alarm does not clear, look for any card-level alarm that could cause this port alarm.

**Step 12** If the alarm does not clear, complete the "Physically Replace a Card" procedure on page 2-154 for the reporting card.

**Step 13** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

## 2.7.88 LOS (ISC)

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: ISC

The LOS alarm for the ISC port applies to TXPP_MR_2.5G or TXP_MR_2.5G client PPMs (SFPs) provisioned at the ISC port rate. Troubleshooting is similar to the LOS (2R) alarm.

**Note** For general information about MXP and TXP cards, refer to the "Card Reference" chapter *Cisco ONS 15454 DWDM Installation and Operations Guide*. For information about provisioning them, refer to the "Provision Transponder and Muxponder Cards" chapter.

### Clear the LOS (ISC) Alarm

**Caution** Always use the supplied electrostatic discharge wristband when working with a powered ONS system. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

**Step 1** Complete the "Clear the LOS (2R) Alarm" procedure on page 2-70.

**Step 2** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

## 2.7.89 LOS (OTS)

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: OTS

The Loss of Signal for the OTS applies to the LINE-3-RX port of the OPT-BST amplifier and the LINE-2-RX port of the OSCM or OSC-CSM card. It indicates that a fiber cut has occurred and no power is being received from the span. The alarm is raised when both LOS-P and LOS-O alarms occur, and demotes them.

### Clear the LOS (OTS) Alarm

**Step 1** To troubleshoot this alarm, refer to the "1.12.1 Fiber Cut Detection" section on page 1-57.

**Step 2** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

## 2.7.90 LOS (TRUNK)

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: TRUNK

The Loss of Signal for a TRUNK applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G cards. The alarm is raised when the card port is not receiving input. An AIS is sent upstream.

**Note** For general information about MXP and TXP cards, refer to the "Card Reference" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For information about provisioning them, refer to the "Provision Transponder and Muxponder Cards" chapter.

### Clear the LOS (TRUNK) Alarm

**Step 1** Check the PMs of the TRUNK-RX port and verify that the received power is above the optics threshold.

**Step 2** Check that a proper threshold has been provisioned. (For procedures, refer to the "Provision Transponder and Muxponder Cards" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.) If an incorrect threshold has been set, adjust it to a value within the allowed limits. If the alarm condition does not clear, move to next step.

**Step 3** Verify the cabling of the Trunk-Rx port and clean the fiber connecting the faulty TXP/MXP to the Drop port of the DWDM card (32DMX, 32DMX-O or AD-xC-xx.x). For fiber cleaning procedures, refer to the "Maintain the Node" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Step 4** Using an optical test set, verify that a valid signal exists on the line and feeds the TRUNK-RX port.(For specific procedures to use the test set equipment, consult the manufacturer.) Test the line as close to the receiving card as possible. If the alarm condition does not clear, move to next step.

**Step 5** Verify whether a bulk attenuator is specified in the Cisco MetroPlanner design. If so, verify that the proper fixed attenuation value has been used.

**Step 6** Check the Drop port optical power value of the DWDM card (32DMX, 32DMX-O or AD-xC-xx.x) connected to the faulty TXP/MXP. If the read value is different (+1 dBm or –1 dBm) compared to the ANS setpoint "Padd&drop-Drop power," move to next step. If not, complete the "Physically Replace a Card" procedure on page 2-154.

**Step 7** If the alarm does not clear after the replacement, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

**Step 8** Look for and troubleshoot any alarms reported by the DWDM cards belonging to the OCHNC circuit whose destination is the faulty TXP/MXP. Possible alarms include: amplifier gain alarms (the "GAIN-HDEG" alarm on page 2-44, the "GAIN-HFAIL" alarm on page 2-45, the "GAIN-LDEG" alarm on page 2-46 or "GAIN-LFAIL" alarm on page 2-47); APC alarms (the "APC-CORRECTION-SKIPPED" alarm on page 2-17 and "APC-OUT-OF-RANGE" alarm on page 2-19), OR LOS-P alarms on the Add or Drop ports belonging to the OCHNC circuit.

**Step 9** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

## 2.7.91 LOS-O

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Objects: OCH, OMS, OTS

The Incoming Overhead Loss of Signal alarm applies to the OSC-TX port of OPT-BST (LINE-1-RX), the OSC-RX internal optical port of OSC-CSM card (LINE-3-RX Port 3). It is raised when the monitored input power crosses the FAIL-LOW threshold associated to the OSC Power received. The is alarm is demoted if another LOS alarm is also present.

### Clear the LOS-O Alarm

**Step 1** Verify fiber continuity to the port by following site practices. Refer to the "Network Reference" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide* for a procedure to detect a fiber cut.

**Step 2** If the cabling is good, confirm that the LED is correctly illuminated on the physical card. A green ACT/SBY LED indicates an active card. A red ACT/SBY LED indicates a failed card.

**Step 3** Display the optical thresholds by clicking one of the following tabs:

- For the OPT-BST card, click the **Provisioning > Opt. Ampli. Line > Optics Thresholds** tabs and click the Alarm checkbox in the Type panel.
- For the OSC-CSM cards, click the **Provisioning > Optical Line > Optics Thresholds** tabs.

**Step 4** Verify that OSC Fail Low thresholds are correct according with Cisco MetroPlanner configuration file. To identify the MP value:

a. In node view, click the **Provisioning > WDM-ANS > Provisioning** tabs.

b. Identify the following parameter: east or west side Rx channel OSC LOS threshold.

**Step 5** If the port power is below the threshold, verify that OSC connections have been created on the other side of the span. If the connections are not present, refer to the "Provision Channels and Circuits" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide* for procedures.

**Step 6** If OSC connections are present, check the OSC transmitted power using CTC on the far-end node. Refer to the "TurnUp Node" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide* for the proper procedure.

**Step 7** If the transmitted OSC value is out of range, troubleshoot that problem first.

**Step 8** If the OSC value is within range, come back to the port reporting the LOS-O alarm and clean the fiber according to site practice. If no site practice exists, complete the fiber-cleaning procedure in the "Maintain the Node" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Step 9** If the alarm does not clear, look for and troubleshoot any other alarm that could identify the source of the problem.

**Step 10** If no other alarms exist that could be the source of the LOS-O, place all of the card ports in **OOS,DSBLD** (or **Locked,disabled**) administrative state.

**Step 11** Complete the "Physically Replace a Card" procedure on page 2-154 for the reporting card.

**Step 12** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.92 LOS-P (AOTS, OMS, OTS)

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Objects: AOTS, OMS, OTS

The Loss of Signal for Optical Channel alarm (OMS and OTS layer) applies to all input ports of the following DWDM cards: AD-1B-xx.x, AD-4B-xx.x, 32DMX, 32DMX-O, OPT-PRE, OPT-BST, and OSC-CSM.

For AD-1C-xx.x, AD-2C-xx.x, AD-4C-xx.x, 32MUX-O and 32WSS cards, this alarm applies only to the input ports where an aggregate signal is managed, such as the COM-RX, EXP-RX, or xxBAND-RX ports). These ports are solely used for the AOTS, OMS, and OTS layers.

LOS-P (AOTS, OMS, or OTS) indicates a loss of receive signal, which means that the monitored input power value has crossed the Power Failure Low Threshold associated to the port.

**Note** When the LOS-P alarm is raised on the LINE-RX port of the OPT-BST or OSC-CSM card, it can indicate a fiber cut. Refer to the "Network Reference" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide* for a fiber cut detection procedure.

### Clear the LOS-P (AOTS, OMS, OTS) Alarm

**Step 1** Verify that the card has the correct physical behavior by checking the LED on the physical card. A green ACT/SBY LED indicates an active card, and a red ACT/SBY LED indicates a failed card. If the LED is red, complete the "Physically Replace a Card" procedure on page 2-154 and continue to Step 7.

**Note** When you replace a card with an identical type of card, you do not need to make any changes to the database other than restoring the card's port to the IS,AINS administrative state.

**Step 2** Verify that there truly is a loss of input signal by completing the following steps:

**a.** Double-click the card to open the card view.

**b.** Verify the proper input power values by clicking one of the following tabs as appropriate:

- For the OPT-BST card, click the **Provisioning > Optical Line > Parameters** tabs.
- For the OPT-PRE card, click the **Provisioning > Optical Line > Parameters** tabs.
- For the AD-xC-xx.x card, click the **Provisioning > Optical Line > Parameters** tabs.
- For the AD-xB-xx.x card, click the **Provisioning > Optical Band > Parameters** tabs.
- For the 32MUX-O card, click the **Provisioning > Optical Line > Parameter**s tabs.
- For the 32WSS card, click the **Provisioning > Optical Line > Parameters** tabs.
- For the 32DMX-O card, click the **Provisioning > Optical Line > Parameters** tabs.
- For the 32DMX card, click the **Provisioning > Optical Line > Parameters** tabs.
- For the OSC-CSM card, click the **Provisioning > Optical Line > Parameters** tabs.

**c.** Display the proper Power Failure Low threshold by clicking one of the following tabs as appropriate:

- For the OPT-BST card, click the **Provisioning > Optical Line > Optics Thresholds** tabs.
- For the OPT-PRE card, click the **Provisioning > Optical Line > Optics Thresholds** tabs.
- For the AD-xC-xx.x card, click the **Provisioning > Optical Line > Optics Thresholds** tabs.
- For the AD-xB-xx.x card, click the **Provisioning > Optical Band > Optics Thresholds** tabs.
- For the AD-xB-xx.x card, click the **Provisioning > Optical Line > Optics Thresholds** tabs.
- For the 32MUX-O card, click the **Provisioning > Optical Line > Optics Thresholds** tabs.
- For the 32WSS card, click the **Provisioning > Optical Line > Optics Thresholds** tabs.
- For the 32DMX-O card, click the **Provisioning > Optical Line > Optics Thresholds** tabs.
- For the 32DMX card, click the **Provisioning > Optical Line > Optics Thresholds** tabs.
- For the OSC-CSM card, click the **Provisioning > Optical Line > Optics Thresholds** tabs.

**Tip** To view the alarm thresholds (as opposed to the warning thresholds), check the **Alarm** check box on the bottom-left of the Optics Thresholds tab and click **Reset**.

**d.** Compare the actual Power value with the Alarm Threshold value and complete one of the following actions:

- If the Power value is less than the Fail Low threshold, go to Step 3.
- If the Power value is greater than the Fail Low threshold plus the alarm hysteresis (allowance value) default of 1 dBm, complete the "Reset a Card in CTC" procedure on page 2-152 for the card.

If the alarm does not clear, complete the "Physically Replace a Card" procedure on page 2-154 and continue to Step 7.

**Note** When you replace a card with an identical type of card, you do not need to make any changes to the database other than restoring the card's port to the IS,AINS administrative state.

**Step 3** Verify the fiber continuity to the port by following site practices. Refer to the "Network Reference" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide* for a procedure to detect a fiber cut.

**Step 4** Check the "Internal Connections" file generated by Cisco MetroPlanner for the node where the errored card is located. If necessary, recable the node cabling in accordance with the MP file connections list. To cable a DWDM node, refer to the "Turn Up a Node" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Step 5** If the cabling is good, use an optical test set to measure the power value on the output port connected to the alarmed card. For specific procedures to use the test set equipment, consult the manufacturer. If the power difference reported is greater than 1 dBm (standard fiber jumper insertion loss is 0.3 dBm), clean the fiber according to site practice. If no site practice exists, complete the fiber-cleaning procedure in the "Maintain the Node" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Note** Unplugging the fiber can cause a traffic hit. To avoid this, perform a traffic switch if possible. Refer to the "Manage the Node" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide* for detailed information.

**Step 6** If the alarm does not clear, follow the general troubleshooting rules in the "Network Level (Intranode) Troubleshooting" chapter for identifying any other upstream alarm in the logical signal flow that could be the root cause of the outstanding alarm.

**Step 7** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

## 2.7.93 LOS-P (OCH)

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: OCH

The Loss of Signal for Optical Channel alarm on the OCH layer applies to the channel Add or pass-through ports on the AD-1C-xx.x, AD-2C-xx.x, AD-4C-xx.x, 32MUX-O and 32WSS-O DWDM cards.

For the 32WSS-O, the LOS-P alarm can be associated with Add ports as well as pass-through internal ports. If the LOS-P (OCH) alarm is raised against this kind of port a different troubleshooting procedure is needed because the port does not have an optical power source directly connected to it. In this case, follow the general troubleshooting rules for network-level (inter-node) troubleshooting in Chapter 1, "General Troubleshooting," to identify upstream alarms in the logical signal flow that could cause an LOS-P.

LOS-P (OCH) indicates a loss of received signal, which means the monitored input power value has crossed the Power Failure Low threshold associated with the port in accordance with the specific VOA power reference setpoint provisioned on VOA along the path.

**Note** For more information about provisioning VOA setpoints, refer to the "Network Reference" chapters of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

## Clear the LOS-P (OCH) Alarm

**Step 1** Verify that the card is exhibiting correct behavior by checking the LED behavior on the physical card. A green ACT/SBY LED indicates an active card, and a red ACT/SBY LED indicates a failed card. If the LED is red, complete the "Physically Replace a Card" procedure on page 2-154 and continue to Step 9.

**Note** When you replace a card with an identical type of card, you do not need to make any changes to the database other than restoring the card's port to the IS,AINS administrative state.

**Step 2** Verify that there truly is a loss of received signal by completing the following steps:

**a.** Double-click the card to open the card view.

**b.** View the proper input power values by clicking one of the following tabs as appropriate:

- For the AD-xC-xx.x card, click the **Provisioning > Optical Chn > Parameters** tabs.
- For the 32MUX-O card, click the **Provisioning > Optical Chn > Parameters** tabs.
- For the 32WSS-O card, click the **Provisioning > Optical Chn: Optical Connector** x **> Parameters** tabs.

**c.** Display the proper Power Failure Low threshold by clicking one of the following tabs as appropriate:

- For the AD-xC-xx.x card, click the **Provisioning > Optical Chn > Optics Thresholds** tabs.
- For the 32MUX-O card, click the **Provisioning > Optical Chn > Optics Thresholds** tabs.
- For the 32WSS-O card, click the **Provisioning > Optical Chn: Optical Connector** x **> Optics Thresholds** tabs.

**Tip** To view the alarm thresholds (as opposed to the warning thresholds), check the **Alarm** check box on the bottom-left of the Optics Thresholds tab and click **Reset**.

**d.** Compare the actual assigned Power value with the Alarm Threshold value and complete one of the following actions:

- If the Power value is less than the Fail Low threshold, go to Step 3.
- If the Power value is greater than the Fail Low threshold plus the alarm hysteresis (or allowance value) default of 1 dBm, complete the "Reset a Card in CTC" procedure on page 2-152 for the card.

If the alarm does not clear, complete the "Physically Replace a Card" procedure on page 2-154 and continue to Step 9.

**Note** When you replace a card with an identical type of card, you do not need to make any changes to the database other than restoring the card's port to the IS,AINS administrative state.

**Step 3** Verify the fiber continuity to the port using site practices. Refer to the "Network Reference" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide* for a procedure to detect a fiber cut.

**Step 4** Check the “Internal Connections” file generated by Cisco MetroPlanner for the node where the card is located. If necessary, recable the node in accordance with the MP file connections list. For procedures to cable a DWDM node, refer to the “Turn Up a Node” chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Step 5** If the cabling is good, verify that each involved optical signal source, including TXP, MXP or ITU-T line card trunk transmit ports, is in the IS (or Unlocked) administrative state. To do this, click the following tabs as appropriate:

- For the TXP_MR_10G card, click the **Provisioning > Line > SONET** (or **Provisioning > Line > SDH**) tabs.
- For the TXP_MR_10E card, click the **Provisioning > Line > SONET** (or **Provisioning > Line > SDH**) tabs.
- For the TXP_MR_2.5G card, click the **Provisioning > Line > SONET** (or **Provisioning > Line > SDH**) tabs.
- For the TXPP_MR_2.5G card, click the **Provisioning > Line > SONET** (or **Provisioning > Line > SDH**) tabs.
- For the MXP_MR_2.5G card, click the **Provisioning > Line > SONET** (or **Provisioning > Line > SDH**) tabs.
- For the MXPP_MR_2.5G card, click the **Provisioning > Line > SONET** (or **Provisioning > Line > SDH**) tabs.
- For the MXP_2.5G_10E card, click the **Provisioning > Line > Trunk** tabs.
- For the MXP_2.5G_10G card, click the **Provisioning > Line > SONET** (or **Provisioning > Line > SDH**) tabs.

If the port administrative state is not IS (or Unlocked), choose **IS** , or **Unlocked**, from the **Admin state** drop-down list. If the alarm does not clear, continue with Step 9.

**Note** If the LOS-P (OCH) alarm applies to a 32WSS-O passthrough port, it means that a single optical source is not directly connected to the port. In this case, follow the general troubleshooting rules given in “Network Level (Internode) Troubleshooting” to identify any other alarm upstream to the logical signal flow that could be the root cause for the outstanding alarm.

**Step 6** If the signal source is in IS (or Unlocked) administrative state, use an optical test set to verify that the transmit laser is active. For specific procedures to use the test set equipment, consult the manufacturer.

**Step 7** If the laser is active, compare the card’s provisioned transmit optical power value with the expected range in the “Provision Transponder and Muxponder Cards” chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*. To display the provisioned transmit optical power values, click the following tabs as appropriate:

- For the TXP_MR_10G card, click the **Performance > Optics PM > Current Values > Trunk Port** tabs.
- For the TXP_MR_10E card, click the **Performance > Optics PM > Current Values > Trunk Port** tabs.
- For the MXP_2.5G_10E card, click the **Performance > Optics PM > Current Values > Trunk Port** tabs.
- For the MXP_2.5G_10G card, click the **Performance > Optics PM > Current Values > Trunk Port** tabs.

**Step 8** Use a standard power meter to measure actual transmit optical power for the following cards as applicable:

- TXP_MR_2.5G
- TXPP_MR_2.5G
- MXP_MR_2.5G
- MXPP_MR_2.5G
- Every ITU-T line card

If the tested optical transmit optical power is within the expected range, go to Step 9. If the actual power value is outside the specification range, complete the "Physically Replace a Card" procedure on page 2-154. (These are listed in the "Hardware Specifications" appendix of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.) When the newly installed card becomes active, verify that the LOS-P (OCH) alarm clears. If it does not, continue with Step 9.

**Tip** If a spare card is unavailable and the transmit power still functions, you can temporarily clear the LOS-P alarm by following the general procedure to add path VOAs during startup failure as noted in the "Perform Node Acceptance Tests" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For more information about provisioning VOA setpoints, refer to the "Network Reference" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Step 9** If the power is within the expected range, return to the port that reported LOS-P and clean the alarmed port's fiber according to site practice. If no site practice exists, complete the procedure in the "Maintain the Node" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Note** Unplugging the fiber can cause a traffic hit. To avoid this, perform a traffic switch if possible. Refer to the "2.9.1 Protection Switching, Lock Initiation, and Clearing" section on page 2-149 for basic instructions, or refer to the "Manage the Node" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide* for more detailed information.

**Step 10** If the alarm does not clear, add path VOAs during startup failure as noted in the "Perform Node Acceptance Tests" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide* to remedy the problem.

**Step 11** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

## 2.7.94 LOS-P (TRUNK)

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: TRUNK

The Incoming Payload Signal Absent alarm for the trunk layer indicates that no optical power is detected at the input trunk port for the following cards:

- TXP_MR_10G
- TXP_MR_10E
- MXP_2.5G_10E

- MXP_2.5G_10G
- TXP_MR_2.5G
- TXPP_MR_2.5G
- MXP_MR_2.5G
- MXPP_MR_2.5G
- Every ITU-T line card

## Clear the LOS-P (TRUNK) Alarm

**Step 1** Verify that the card behaves correctly by checking the LED behavior on the physical card. A green ACT/SBY LED indicates an active card, and a red ACT/SBY LED indicates a failed card. If the LED is red, complete the "Physically Replace a Card" procedure on page 2-154 and continue to Step 7.

**Note** When you replace a card with an identical type of card, you do not need to make any changes to the database other than restoring the card's port to the IS,AINS administrative state.

**Step 2** Verify that there truly is a loss of received optical power by completing the following steps:

**a.** Double-click the alarmed card to open the card view.

**b.** Click the **Performance > Optics PM > Current Values > Trunk Port** tabs and view the RX Optical Pwr value.

**c.** Compare the actual power levels with the expected power range given in the "Hardware Specifications" appendix of the *Cisco ONS 15454 DWDM Installation and Operations Guide*. Complete one of the following actions:

- If power is higher than –40 dBm (that is, –20 dBm, –1 dBm, 0 dBm or 10 dBm) and within the accepted range go to Step 4.
- or if the power is lower than –40 dBm (that is, –40 dBm, –45 dBm or –50 dBm) complete the "Reset a Card in CTC" procedure on page 2-152 for the card.

**Step 3** If the alarm does not clear, complete the "Physically Replace a Card" procedure on page 2-154 for the reporting card and then go to Step 9.

**Note** When you replace a card with an identical type of card, you do not need to make any changes to the database other than restoring the card's port to the IS,AINS administrative state.

**Step 4** Verify the fiber continuity to the port by following site practices. Refer to the "Network Reference" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide* for a procedure to detect a fiber cut.

**Step 5** Check the "Internal Connections" file generated by Cisco MetroPlanner for the node containing the alarmed card. If necessary, recable the node in accordance with the MP file connections list. For procedures to cable a DWDM node, refer to the "Turn Up a Node" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Step 6** If the cabling is good, use a test set to verify the power value on the DWDM CH_DROP-TX port on the AD-xC-xx.x, 32DMX-O, or 32DMX. For specific procedures to use the test set equipment, consult the manufacturer.

**Step 7** If the power difference reported is greater than 1 dBm (standard fiber jumper insertion loss is 0.3 dBm), clean the fiber according to site practice. If no site practice exists, complete the procedure in the "Maintain the Node" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Note** Unplugging the fiber can cause a traffic hit. To avoid this, perform a traffic switch if possible. Refer to the "2.9.1 Protection Switching, Lock Initiation, and Clearing" section on page 2-149 for basic instructions, or to the "Manage the Node" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide* for more detailed information.

**Step 8** If the alarm does not clear, follow the general troubleshooting rules stated in the "Network Reference" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide* to identify upstream alarms in the logical signal flow that could cause an LOS-P.

**Step 9** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

## 2.7.95 LO-TXPOWER

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Objects: 2R, EQPT, ESCON, FC, GE, ISC, OCN/STMN, PPM, TRUNK

The Equipment Low Transmit Power alarm is an indicator for the TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, MXP_2.5G_10G and OC192-XFP card transmitted optical signal power. LO-TXPOWER occurs when the measured optical power of the transmitted signal falls under the threshold. The threshold value is user-provisionable.

**Note** For more information about MXP and TXP cards and their power levels, refer to the "Card Reference" and "Provision Transponder and Muxponder Cards" chapters in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

### Clear the LO-TXPOWER Alarm

**Step 1** Display the TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, MXP_2.5G_10G, or OC192-XFP card view.

**Step 2** Click the **Provisioning > Optics Thresholds > Current Values** tabs.

**Step 3** Increase the TX Power Low column value by 0.5 dBm.

**Step 4** If the card transmit power setting cannot be increased without affecting the signal, complete the "Physically Replace a Card" procedure on page 2-154.

**Step 5** If no ports are shown bad and the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.96 LPBKFACILITY (ESCON)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: ESCON

The LPBKFACILITY (ESCON) condition occurs on a TXP_MR_2.5G or TXPP_MR_2.5G card PPM (SFP) provisioned for FICON1G or FICON 2G line speed when there is a facility loopback active on the card.

For information about troubleshooting these circuits with loopbacks, refer to the "1.2 Troubleshooting MXP or TXP Circuit Paths With Loopbacks" section on page 1-6.

### Clear the LPBKFACILITY (ESCON) Condition

**Step 1** Complete the "Clear an MXP or TXP Card Loopback Circuit" procedure on page 2-156.

**Step 2** If the alarm does not clear, or if you need assistance conducting network troubleshooting tests, call Cisco TAC to report a Service-Affecting (SA) problem (1 800 553-2447).

## 2.7.97 LPBKFACILITY (FC)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: FC

A Loopback Facility condition for the FC payload occurs on a fibre channel (FC) line when a software facility (line) loopback is active for an MXPP_MR_2.5G, MXP_MR_2.5G, TXPP_MR_2.5G, and TXP_MR_2.5G card client PPM (SFP) provisioned at the FC1G, FC2G, FICON1G, or FICON 2G line speed.

For information about troubleshooting these circuits with loopbacks, refer to the "1.2 Troubleshooting MXP or TXP Circuit Paths With Loopbacks" section on page 1-6.

**Note** For more information about MXP and TXP cards, refer to the "Card Reference" and "Provisioning Tranponder and Muxponder Cards" chapters in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

### Clear the LPBKFACILITY (FC) Condition

**Step 1** Complete the "Clear an MXP or TXP Card Loopback Circuit" procedure on page 2-156.

**Step 2** If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.98 LPBKFACILITY (GE)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: GE

A Loopback Facility condition for a Gigabit Ethernet (GE) port occurs when a software facility (line) loopback is active for an MXP_MR_2.5G, MXPP_MR_2.5G, TXP_MR_2.5G, and TXPP_MR_2.5G card client PPM (SFP) provisioned at the ONE_GE port rate. For the TXP_MR_10E and TXP_MR_10G cards, this condition occurs when there is a facility loopback on a client PPM (SFP) provisioned at the TEN_GE port rate.

For information about troubleshooting these circuits with loopbacks, refer to the "1.2 Troubleshooting MXP or TXP Circuit Paths With Loopbacks" section on page 1-6.

**Note** For more information about MXP and TXP cards, refer to the "Card Reference" and "Provision Transponder and Muponder Cards" chapters in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

### Clear the LPBKFACILITY (GE) Condition

**Step 1** Complete the "Clear an MXP or TXP Card Loopback Circuit" procedure on page 2-156.

**Step 2** If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.99 LPBKFACILITY (ISC)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: ISC

A Loopback Facility condition for an ISC port occurs when a software facility (line) loopback is active for a TXPP_MR_2.5G or TXP_MR_2.5G client PPM (SFP) provisioned at the ISC port rate.

For information about troubleshooting these circuits with loopbacks, refer to the "1.2 Troubleshooting MXP or TXP Circuit Paths With Loopbacks" section on page 1-6.

**Note** For more information about MXP and TXP cards, refer to the "Card Reference" and "Provision Transponder and Muxponder Cards" chapters in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

### Clear the LPBKFACILITY (ISC) Condition

**Step 1** Complete the "Clear an MXP or TXP Card Loopback Circuit" procedure on page 2-156.

**Step 2** If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.100 LPBKFACILITY (TRUNK)

Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)

Logical Object: TRUNK

A Loopback Facility condition on MXP and TXP card trunk ports indicates that there is an active facility (line) loopback on the port. For this condition to be present, the administrative state is OOS,MT (or Locked,maintenance).

For information about troubleshooting these circuits with loopbacks, refer to the "1.2 Troubleshooting MXP or TXP Circuit Paths With Loopbacks" section on page 1-6.

**Caution** CTC permits loopbacks on an in-service (IS) circuit. Loopbacks are service-affecting.

### Clear the LPBKFACILITY (TRUNK) Condition

**Step 1** Complete the "Clear an MXP or TXP Card Loopback Circuit" procedure on page 2-156.

**Step 2** If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.101 LPBKTERMINAL (ESCON)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: ESCON

The LPBKTERMINAL (ESCON) condition occurs on a TXP_MR_2.5G or TXPP_MR_2.5G card PPM (SFP) provisioned for FICON1G or FICON 2G line speed when there is a terminal loopback active on the card.

For information about troubleshooting these circuits with loopbacks, refer to the "1.2 Troubleshooting MXP or TXP Circuit Paths With Loopbacks" section on page 1-6.

### Clear the LPBKTERMINAL (ESCON) Condition

**Step 1** Complete the "Clear an MXP or TXP Card Loopback Circuit" procedure on page 2-156.

**Step 2** If the alarm does not clear, or if you need assistance conducting network troubleshooting tests, call Cisco TAC to report a Service-Affecting (SA) problem (1 800 553-2447).

## 2.7.102 LPBKTERMINAL (FC)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: FC

A Loopback Terminal condition for the FC payload occurs on an FC when a software terminal (inward) loopback is active for an MXPP_MR_2.5G, MXP_MR_2.5G, TXPP_MR_2.5G, and TXP_MR_2.5G card client PPM (SFP) provisioned at the FC1G, FC2G, FICON1G, or FICON2G line speed.

For information about troubleshooting these circuits with loopbacks, refer to the "1.2 Troubleshooting MXP or TXP Circuit Paths With Loopbacks" section on page 1-6.

**Note** For more information about MXP and TXP cards, refer to the "Card Reference" and "Provisioning Transponder and Muxponder Cards" chapters in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

### Clear the LPBKTERMINAL (FC) Condition

**Step 1** Complete the "Clear an MXP or TXP Card Loopback Circuit" procedure on page 2-156.

**Step 2** If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.103 LPBKTERMINAL (GE)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: GE

A Loopback Terminal condition for a GE port occurs when a software terminal (inward) loopback is active for an MXP_MR_2.5G, MXPP_MR_2.5G, TXP_MR_2.5G, and TXPP_MR_2.5G card client PPM (SFP) provisioned at the ONE_GE port rate. For the TXP_MR_10E and TXP_MR_10G cards, this condition occurs when there is a facility loopback on a client PPM (SFP) provisioned at the TEN_GE port rate.

For information about troubleshooting these circuits with loopbacks, refer to the "1.2 Troubleshooting MXP or TXP Circuit Paths With Loopbacks" section on page 1-6.

**Note** For more information about MXP and TXP cards, refer to the "Card Reference" and "Provision Transponder and Muxponder Cards" chapters in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

### Clear the LPBKTERMINAL (GE) Condition

**Step 1** Complete the "Clear an MXP or TXP Card Loopback Circuit" procedure on page 2-156.

**Step 2** If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.104 LPBKTERMINAL (ISC)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: ISC

A Loopback Terminal condition for an ISC port occurs when a software terminal (inward) loopback is active for a TXPP_MR_2.5G or TXP_MR_2.5G client PPM (SFP) provisioned at the ISC port rate.

For information about troubleshooting these circuits with loopbacks, refer to the "1.2 Troubleshooting MXP or TXP Circuit Paths With Loopbacks" section on page 1-6.

**Note** For more information about MXP and TXP cards, refer to the "Card Reference" and "Provisioning Transponder and Muxponder Cards" chatpers in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

### Clear the LPBKTERMINAL (ISC) Condition

**Step 1** Complete the "Clear an MXP or TXP Card Loopback Circuit" procedure on page 2-156.

**Step 2** If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.105 LPBKTERMINAL (TRUNK)

Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)

Logical Object: TRUNK

A Loopback Terminal condition on MXP or TXP trunk card indicates that there is an active terminal (inward) loopback on the port.

For information about troubleshooting, refer to the "1.2 Troubleshooting MXP or TXP Circuit Paths With Loopbacks" section on page 1-6.

### Clear the LPBKTERMINAL (TRUNK) Condition

**Step 1** Complete the "Clear an MXP or TXP Card Loopback Circuit" procedure on page 2-156.

**Step 2** If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.106 LWBATVG

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: PWR

The Low Voltage Battery alarm occurs in a –48 VDC environment when a battery lead input voltage falls below the low power threshold. This threshold, with a default value of –44 VDC, is user-provisionable. The alarm remains raised until the voltage remains above the threshold for 120 seconds. (For information about changing this threshold, refer to the "Turn Up Node" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

### Clear the LWBATVG Alarm

**Step 1** The problem is external to the ONS system. Troubleshoot the power source supplying the battery leads.

**Step 2** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

## 2.7.107 MAN-REQ

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: EQPT

The Manual Switch Request condition occurs when a user initiates a Manual switch request on an OC-N/STM-N port. Clearing the Manual switch clears the MAN-REQ condition. You do not need to clear the switch if you want the Manual switch to remain.

### Clear the MAN-REQ Condition

**Step 1** Complete the "Initiate a 1+1 Manual Switch Command" procedure on page 2-150.

**Step 2** If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.108 MANRESET

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: EQPT

A User-Initiated Manual Reset condition occurs when you right-click a card in CTC and choose Reset. Resets performed during a software upgrade also prompt the condition. The MANRESET condition clears automatically when the card finishes resetting.

**Note** MANRESET is an informational condition and does not require troubleshooting.

## 2.7.109 MANSWTOINT

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: NE-SREF

The Manual Switch To Internal Clock condition occurs when the NE timing source is manually switched to an internal timing source.

**Note** MANSWTOINT is an informational condition and does not require troubleshooting.

## 2.7.110 MANSWTOPRI

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Objects: EXT-SREF, NE-SREF

The Manual Switch To Primary Reference condition occurs when the NE timing source is manually switched to the primary timing source.

**Note** MANSWTOPRI is an informational condition and does not require troubleshooting.

## 2.7.111 MANSWTOSEC

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Objects: EXT-SREF, NE-SREF

The Manual Switch To Second Reference condition occurs when the NE timing source is manually switched to a second timing source.

**Note** MANSWTOSEC is an informational condition and does not require troubleshooting.

## 2.7.112 MANSWTOTHIRD

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Objects: EXT-SREF, NE-SREF

The Manual Switch To Third Reference condition occurs when the NE timing source is manually switched to a third timing source.

**Note** MANSWTOTHIRD is an informational condition and does not require troubleshooting.

## 2.7.113 MANUAL-REQ-SPAN (2R, ESCON, FC, GE, ISC, OCN/STMN)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Objects: 2R, ESCON, FC, GE, ISC, OCN/STMN

The Manual Switch Request on Ring condition for clients occurs when a user initiates a Manual Span command on an MXP or TXP client for the above-listed client types to move traffic from a working span to a protect span. This condition appears on the network view Alarms, Conditions, and History tabs. The port where the MANUAL SPAN command was applied is marked with an "M" on the network view detailed circuit map.

**Note** For more information about protection schemes, refer to the "Network Reference" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

## 2.7.114 MANUAL-REQ-SPAN (TRUNK)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: TRUNK

The Manual Switch Request on Ring condition for the trunk occurs when a user initiates a Manual Span command on an MXP or TXP trunk port in a splitter protection group to move traffic from a working span to a protect span. This condition appears on the network view Alarms, Conditions, and History tabs. The port where the MANUAL SPAN command was applied is marked with an "M" on the network view detailed circuit map.

**Note** For more information about protection schemes, refer to the "Network Reference" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

## 2.7.115 MEA (EQPT)

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: EQPT

The MEA alarm for equipment is reported against a card slot when the physical card inserted into a slot does not match the card type that is provisioned for that slot in CTC. Removing the incompatible cards clears the alarm. For more information about card compatibility, refer to the "Card Reference" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Note** For more information about protection schemes, refer to the "Network Reference" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

### Clear the MEA (EQPT) Alarm

**Step 1** Physically verify the type of card that is installed in the slot reporting the MEA alarm. In node view, click the **Inventory** tab and compare it to the actual installed card.

**Step 2** Determine whether the ONS system shelf assembly is a newer 10-Gbps-compatible shelf assembly (15454-SA-ANSI or 15454-SA-HD) or an earlier shelf assembly. Under the HW Part # column, if the part number is 800-19857-XX or 800-19856-XX, then you have a 15454-SA-ANSI shelf. If the part number is 800-24848-XX, then you have a 15454-SA-HD shelf. If the number is not one of those listed here, then you are using an earlier shelf assembly.

**Note** On the 15454-SA-HD (P/N: 800-24848), 15454-SA-NEBS3E, 15454-SA-NEBS3, and 15454-SA-R1 (P/N: 800-07149) shelves, the AIP cover is clear plastic. On the 15454-SA-ANSI shelf (P/N: 800-19857), the AIP cover is metal.

**Step 3** If you prefer the card type depicted by CTC, complete the "Physically Replace a Card" procedure on page 2-154 for the reporting card.

**Step 4** If you prefer the card that physically occupies the slot but the card is not in service, does not have circuits mapped to it, and is not part of a protection group, place the cursor over the provisioned card in CTC and right-click to choose **Delete Card**.

The card that physically occupies the slot reboots, and CTC automatically provisions the card type into that slot.

**Note** If the card is in service, does have circuits mapped to it, is paired in a working protection scheme, has DCC communications turned on, or is used as a timing reference, CTC does not allow you to delete the card.

**Step 5** If any ports on the card are in service, place them out of service (OOS,MT):

**Caution** Before placing ports out of service, ensure that live traffic is not present.

a. Double-click the reporting card to open the card view.

b. Click the **Provisioning** tab.

c. Click the administrative state of any in-service ports.

d. Choose **OOS,MT** (or **Locked,maintenance**) to take the ports out of service.

**Step 6** If a circuit has been mapped to the card, complete the "Delete a Circuit" procedure on page 2-155.

**Caution** Before deleting the circuit, ensure that live traffic is not present.

**Step 7** If the card is paired in a protection scheme, delete the protection group:

a. Click the **Provisioning > Protection** tabs.

b. Choose the protection group of the reporting card.

c. Click **Delete**.

**Step 8** Right-click the card reporting the alarm.

**Step 9** Choose **Delete**.

The card that physically occupies the slot reboots, and CTC automatically provisions the card type into that slot.

**Step 10** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

## 2.7.116 MEA (FAN)

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: FAN

The MEA alarm is reported against the fan-tray assembly when a newer fan-tray assembly (15454-FTA3) with a 5-A fuse is used with an older shelf assembly or when an older fan-tray assembly with a 2-A fuse is used with a newer 10-Gbps-compatible shelf assembly (15454-SA-ANSI or 15454-SA-HD) that contains cards introduced in Release 3.1 or later. If a 10-Gbps-compatible shelf assembly contains only cards introduced before Release 3.1, then an older fan-tray assembly (15454-FTA-2) can be used and does not report an MEA alarm.

### Clear the MEA (FAN) Alarm

**Step 1** Determine whether the shelf assembly is a newer 10-Gbps-compatible shelf assembly (15454-SA-ANSI or 15454-SA-HD) or an earlier shelf assembly. In node view, click the **Inventory** tab.

Under the HW Part # column, if the part number is 800-19857-XX or 800-19856-XX, then you have a 15454-SA-ANSI shelf. If the part number is 800-24848-XX, you have a 15454-SA-HD shelf.

Under the HW Part # column, if the number is not one of those listed here, then you are using an earlier shelf assembly.

**Step 2** If you have a 10-Gbps-compatible shelf assembly (15454-SA-ANSI or 15454-SA-HD), the alarm indicates that an older incompatible fan-tray assembly is installed in the shelf assembly. Obtain a newer fan-tray assembly (15454-FTA3) with a 5-A fuse and complete the "Replace the Fan-Tray Assembly" procedure on page 2-158.

**Step 3** If you are using an earlier shelf assembly, the alarm indicates that you are using a newer fan-tray assembly (15454-FTA3), which is incompatible with the earlier version of the shelf assembly. Obtain an earlier version of the fan-tray assembly (15454-FTA2) and complete the "Replace the Fan-Tray Assembly" procedure on page 2-158.

**Step 4** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

## 2.7.117 MEA (PPM)

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: PPM

The Missing Equipment Attributes alarm for the PPM (SFP) is raised on TXP, MXP, MRC-12 and OC192-XFP/STM-64-XP cards when the PPM (SFP) is misprovisioned or unsupported. It can occur when you provision the PPM (SFP) for a wavelength that is explicitly not the first tunable wavelength.

**Note** For general information about DWDM cards, refer to the "Card Reference" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For PPM (SFP) specifications, refer to the "Hardware Specifications" appendix. For information about MRC-12 cards, refer to the "Optical Cards" chapter in the *Cisco ONS 15454 DWDM Reference Manual*.

## Clear the MEA (PPM) Alarm

**Step 1** To provision the PPM (SFP), you must first create it in CTC. To do this, complete the following steps:

**a.** Double-click the reporting card to open the card view.

**b.** Click the **Provisioning > Pluggable Port Modules** tabs. (If you already see the PPM [SFP] listed in the Pluggable Port Modules Area, go to Step 2.)

**c.** Under the Pluggable Port Modules area, click **Create**.

**d.** In the Create PPM dialog box, choose the card PPM (SFP) number from the drop-down list (for example, PPM 1).

**e.** Choose the PPM (SFP) type from the second drop-down list, for example PPM (1 Port).

**f.** Click **OK**.

**Note** For more information about provisioning MXP or TXP PPMs (SFPs), refer to the "Turn Up a Node" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For information to provision PPMs (SFPs) for the MRC-12 and OC192/STM64-XFP, refer to the "Optical Cards" chapter in the *Cisco ONS 15454 DWDM Reference Manual*.

**Step 2** After you have created the PPM (SFP), or if you see it listed in the Pluggable Port Modules area but not in the Selected PPM area, choose the port rate:

**a.** Under the Selected PPM area, click **Create**.

**b.** In the Create Port dialog box, choose the port (for example, 1-1) from the drop-down list.

**c.** Choose the correct port type from the drop-down list. (For more information about selecting PPM (SFP) port types, refer to the "Provision Transponder and Muxponder Cards" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.)

**d.** Click **OK**.

**Step 3** If you see the port listed in the Pluggable Port Modules area and the Selected PPM area, the MEA indicates that the incorrect port rate was selected. Click the port in the Selected PPM area and click **Delete**.

**Step 4** Complete Step 2 to correctly provision the port rate.

**Step 5** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

## 2.7.118 MEM-GONE

Default Severity: Major (MJ), Non-Service-Affecting (NSA)

Logical Object: EQPT

The Memory Gone alarm occurs when data generated by software operations exceeds the memory capacity of the TCC2/TCC2P. The TCC2/TCC2P cards which exceed the memory capacity reboot to avoid failure of card operations.

**Note** The alarm does not require user intervention. The MEM-LOW alarm always preceeds the MEM-GONE alarm.

## 2.7.119 MEM-LOW

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: EQPT

The Free Memory of Card Almost Gone alarm occurs when data generated by software operations is close to exceeding the memory capacity of the TCC2/TCC2P. The alarm clears when additional memory becomes available. If additional memory is not made available and the memory capacity of the card is exceeded, CTC ceases to function.

The alarm does not require user intervention. If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.120 MFGMEM

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Objects: AICI-AEP, AICI-AIE, AIP, BPLANE, FAN, PPM

The Manufacturing Data Memory Failure alarm occurs when the EEPROM fails on a card or component, or when the TCC2/TCC2P cannot read this memory. EEPROM stores manufacturing data that a system TCC2/TCC2P uses to determine system compatibility and shelf inventory status. Unavailability of this information can cause less-significant problems. The AIP EEPROM also stores the system MAC address. If the MFGMEM alarm indicates EEPROM failure on these panels, IP connectivity could be disrupted and the system icon is grayed out in CTC network view.

**Tip** When you lose LAN connectivity with an ONS system due to an MFGMEM alarm on the AIP, you can reestablish node management by disconnecting the Ethernet cable from the panel and connecting it to the active TCC2/TCC2P LAN port.

### Clear the MFGMEM Alarm

**Step 1** Complete the "Reset an Active TCC2/TCC2P Card and Activate the Standby Card" procedure on page 2-152.

Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card.

**Step 2** If the reset card has not rebooted successfully, or the alarm has not cleared, call Cisco TAC (1 800 553-2447). If the Cisco TAC technician tells you to reseat the card, complete the "Remove and Reinsert (Reseat) the Standby TCC2/TCC2P Card" procedure on page 2-153. If the Cisco TAC technician tells you to remove the card and reinstall a new one, complete the "Physically Replace a Card" procedure on page 2-154.

**Step 3** If the MFGMEM alarm continues to report after replacing the TCC2/TCC2Ps, the problem lies with the EEPROM.

**Step 4** If the MFGMEM is reported from the fan-tray assembly, obtain a fan-tray assembly and complete the "Replace the Fan-Tray Assembly" procedure on page 2-158.

**Step 5** If the MFGMEM is reported from the AIP, the backplane, or the alarm persists after the fan-tray assembly is replaced, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) to report a Service-Affecting (SA) problem.

## 2.7.121 NOT-AUTHENTICATED

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: SYSTEM

The NOT-AUTHENTICATED alarm is raised by CTC (not by the NE) when CTC fails to log into a node. This alarm only appears in CTC where the login failure occurred. This alarm differs from the "INTRUSION-PSWD" alarm, page 2-58, because INTRUSION-PSWD occurs when a user exceeds the login failures threshold.

**Note** NOT-AUTHENTICATED is an informational alarm and is resolved when CTC successfully logs into the node.

## 2.7.122 OCHNC-INC

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: OCHNC-CONN

The Optical Channel (OCH) Incomplete Cross-Connection condition is raised when an OCH cross connection on a two-way circuit is deleted. For example, if you create an OCH circuit on a linear DWDM structure with Nodes A, B and C—originating at Node A, traversing through Node B, and terminating at Node C—then mistakenly delete a cross-connect (such as by TL1 command DLT-WLEN) on Nodes B or C, this condition is raised on the source node (A). The condition is corrected by regenerating the cross-connect. The alarm also follows these guidelines:

- Two-way circuit with Nodes A, B, and C (as described in the preceding example): Deleting a cross-connection on Nodes B or C will raise OCHNC-INC on the Node A cross connection.
- Two-way circuit with Nodes A, B, and C: Deleting a cross connection on Node A will raise an OCHNC-INC alarm on the Node C cross connection.
- One-way circuit with Nodes A, B and C: Deleting a cross connection on Nodes B or C will raise an OCHNC-INC alarm on Node A cross connection.
- One-way circuit with Nodes A, B, and C: Deleting a cross connection on Node A will not raise an OCHNC-INC alarm.

**Note** If you delete one of the cross-connects, you might not be able to recreate this same circuit with CTC because the wavelength is already being used on the other component nodes for add, drop, or express.

The OCHNC-INC alarm can also be raised if you restore one node's database that is inconsistent with other node databases, following the guidelines previously listed. (That is, an inconsistent database that does not contain up-to-date circuit cross-connection information will cause the same problem as if you had deleted the cross-connect.)

**Caution** It is important to create a backup version of the database for each node of a topology during a known-stable situation. You should give the saved files names that indicate their version and date or any other information needed to verify their consistency. For procedures to back up or restore database files, refer to the "Maintain the Node" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

### Clear the OCHNC-INC Alarm

**Step 1** To recreate the missing cross-connect itself, establish a Telnet connection with the node where it was deleted and use the ENT-WLEN command with the Add port, Drop port, or Express port on the node.

For information about establishing a TL1 session connection, refer to the *Cisco ONS SONET TL1 Reference Guide*. For more information about ENT-WLEN and other TL1 commands, as well as their syntax, refer to the *Cisco SONET TL1 Command Guide* .

**Step 2** If the alarm is not due to a deleted cross-connect but instead to an inconsistent database being restored on a node, correct the problem by restoring the correct backup version to that node. For the restore procedure, refer to the "Maintain the Node" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Note** When you restore a database on a node, it replaces the database being used on both (ACT and SBY) TCC2/TCC2Ps as the cards synchronize this version into their active flash memory. If the active (ACT) TCC2/TCC2P is reset, the standby (SBY) TCC2/TCC2P will therefore use the same database version from its active flash memory. In the case of a power-up, both TCC2/TCC2Ps boot and choose which database to use from two criteria: (1) the most recent version compatible with the node software, and (2) the most recently loaded version of that compatible database (with the highest sequence number).

**Step 3** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

## 2.7.123 ODUK-1-AIS-PM

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

Logical Object: TRUNK

The ODUK-1-AIS-PM is a secondary condition raised on MXP card trunk signals when they experience an LOS (2R). Although the ODUK-1-AIS-PM is raised against the TRUNK object, it actually refers to the client signals contained within the trunk.

A single ODUK-x-AIS-PM can occur when one far-end client signal is lost; multiple ODK-x-AIS-PMs can occur (ODUK-1-AIS-PM, ODUK-2-AIS-PM, ODUK-3-AIS-PM, ODUK-4-AIS-PM) if more than one far-end client is lost. If the entire trunk signal is lost, LOS (TRUNK) occurs and demotes any LOS (2R) alarms.

### Clear the ODUK-1-AIS-PM Condition

**Step 1** Look for and clear the LOS (2R) alarm on the far-end client. This should clear the ODUK-1-AIS-PM condition on the trunk.

**Step 2** If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.124 ODUK-2-AIS-PM

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

Logical Object: TRUNK

The ODUK-2-AIS-PM is a secondary condition raised on MXP card trunk signals when they experience an LOS (2R). Although the ODUK-2-AIS-PM is raised against the TRUNK object, it actually refers to the client signals contained within the trunk.

### Clear the ODUK-2-AIS-PM Condition

**Step 1** Complete the "Clear the ODUK-1-AIS-PM Condition" procedure on page 2-97.

**Step 2** If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.125 ODUK-3-AIS-PM

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

Logical Object: TRUNK

The ODUK-3-AIS-PM is a secondary condition raised on MXP card trunk signals when they experience an LOS (2R). Although the ODUK-3-AIS-PM is raised against the TRUNK object, it actually refers to the client signals contained within the trunk.

### Clear the ODUK-3-AIS-PM Condition

**Step 1** Complete the "Clear the "Clear the ODUK-1-AIS-PM Condition" procedure on page 2-97.

**Step 2** If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.126 ODUK-4-AIS-PM

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

Logical Object: TRUNK

The ODUK-4-AIS-PM is a secondary condition raised on MXP card trunk signals when they experience an LOS (2R). Although the ODUK-4-AIS-PM is raised against the TRUNK object, it actually refers to the client signals contained within the trunk.

### Clear the ODUK-4-AIS-PM Condition

**Step 1** Complete the "Clear the ODUK-1-AIS-PM Condition" procedure on page 2-97.

**Step 2** If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.127 ODUK-AIS-PM

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

Logical Object: TRUNK

The Optical Data Unit (ODUK) AIS Path Monitoring (PM) condition applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G cards when ITU-T G.709 encapsulation is enabled for the cards. ODUK-AIS-PM is a secondary condition that indicates a more serious condition such as the LOS (OCN/STMN) alarm occurring downstream. (This is described in the "Alarm Troubleshooting" chapter of the *Cisco ONS 15454 Troubleshooting Guide* or the *Cisco ONS 15454SDH Troubleshooting Guide*.) The ODUK-AIS-PM condition is reported in the path monitoring area of the optical data unit wrapper overhead. ODUK-AIS-PM is caused by the upstream 2.7.130 ODUK-OCI-PM, page 2-100.

ITU-T G.709 encapsulation refers to a digital data wrapper that is transparent across networking standards such as SONET and protocols (such as Ethernet or IP). For information about provisioning the TXP card or MXP card to enable ITU-T G.709 encapsulation, refer to the "Provision Transponder and Muxponder Cards" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Note** For general information about MXP and TXP cards, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For information about provisioning them, refer to the "Provision Transponder and Muxponder Cards" chapter.

### Clear the ODUK-AIS-PM Condition

**Step 1** Determine whether upstream nodes and equipment have alarms, especially the LOS (OCN/STMN) alarm, or OOS (or Locked) ports.

**Step 2** Clear the upstream alarms using the "Clear the LOS (OCN/STMN) Procedure" located in the *Cisco ONS 15454 Troubleshooting Guide* or *Cisco ONS 15454SDH Troubleshooting Guide*.

**Step 3** If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.128 ODUK-BDI-PM

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

Logical Object: TRUNK

The ODUK Backward Defect Indicator (BDI) PM condition applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G cards when ITU-T G.709 encapsulation is enabled for the cards. It indicates that there is a path termination error upstream in the data. The error is read as a BDI bit in the path monitoring area of the digital wrapper overhead.

**Note** For general information about MXP and TXP cards, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For information about provisioning them, refer to the "Provision Transponder and Muxponder Cards" chapter.

### Clear the ODUK-BDI-PM Condition

**Step 1** Complete the "Clear the OTUK-BDI Condition" procedure on page 2-109.

**Step 2** If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.129 ODUK-LCK-PM

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

Logical Object: TRUNK

The ODUK Locked Defect (LCK) PM condition applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G cards when ITU-T G.709 encapsulation is enabled for the cards. ODUK-LCK-PM indicates that a signal is being sent downstream to indicate that the upstream connection is locked, preventing the signal from being passed. The lock is indicated by the STAT bit in the path overhead monitoring fields of the optical transport unit overhead of the digital wrapper.

**Note** For general information about MXP and TXP cards, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For information about provisioning them, refer to the "Provision Transponder and Muxponder Cards" chapter.

### Clear the ODUK-LCK-PM Condition

**Step 1** Unlock the upstream node signal.

**Step 2** If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.130 ODUK-OCI-PM

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

Logical Object: TRUNK

The ODUK Open Connection Indication (OCI) PM condition applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G cards when ITU-T G.709 encapsulation is enabled for the cards. It indicates that the upstream signal is not connected to a trail termination source. The error is read as a STAT bit in the path monitoring area of the digital wrapper overhead. ODUK-OCI-PM causes a downstream "ODUK-LCK-PM" alarm on page 2-99.

**Note** For general information about MXP and TXP cards, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For information about provisioning them, refer to the "Provision Transponder and Muxponder Cards" chapter.

### Clear the ODUK-OCI-PM Condition

**Step 1** Verify the fiber connectivity at nodes upstream.

**Step 2** If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.131 ODUK-SD-PM

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: TRUNK

The ODUK Signal Degrade (SD) PM condition applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G cards when ITU-T G.709 encapsulation is enabled. ODUK-SD-PM indicates that incoming signal quality is poor, but the incoming line BER has not passed the fail threshold. The BER problem is indicated in the path monitoring area of the optical data unit frame overhead.

**Note** For general information about MXP and TXP cards, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For information about provisioning them, refer to the "Provision Transponder and Muxponder Cards" chapter.

### Clear the ODUK-SD-PM Condition

**Step 1** Complete the "Clear the OTUK-SD Condition" procedure on page 2-111.

**Step 2** If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.132 ODUK-SF-PM

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: TRUNK

The ODUK Signal Fail (SF) PM condition (ODUK-SD-PM) applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, and MXP_2.5G_10G cards when ITU-T G.709 encapsulation is enabled. ODUK-SF-PM indicates that incoming signal quality is poor and the incoming line BER has passed the fail threshold. The BER problem is indicated in the path monitoring area of the optical data unit frame overhead.

**Note** For general information about MXP and TXP cards, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For information about provisioning them, refer to the "Provision Transponder and Muxponder Cards" chapter.

### Clear the ODUK-SF-PM Condition

**Step 1** Complete the "Clear the SF (DS1, DS3) Condition" procedure located in the "Alarm Troubleshooting" chapter of the *Cisco ONS 15454 Troubleshooting Guide*.

**Step 2** If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.133 ODUK-TIM-PM

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: TRUNK

The ODUK-TIM- PM condition applies to the path monitoring area of the OTN overhead for TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G cards. The condition occurs when there is a trace identifier mismatch in the data stream. ODUK-TIM-PM causes an 2.7.128 ODUK-BDI-PM, page 2-99, downstream.

The ODUK-TIM-PM condition applies to TXP cards and MXP cards when ITU-T G.709 encapsulation is enabled for the cards. It indicates that there is an error upstream in the optical transport unit overhead of the digital wrapper.

ITU-T G.709 encapsulation refers to a digital data wrapper that is transparent across networking standards such as SONET and protocols (such as Ethernet or IP). For information about provisioning the TXP card or MXP card to enable ITU-T G.709 encapsulation, refer to the "Provision Transponder and Muxponder Cards" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Note** For general information about MXP and TXP cards, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For information about provisioning them, refer to the "Provision Transponder and Muxponder Cards" chapter.

### Clear the ODUK-TIM-PM Condition

**Step 1** Complete the "Clear the TIM-P Condition" procedure located in the "Alarm Troubleshooting" chapter of the *Cisco ONS 15454 Troubleshooting Guide*.

**Step 2** If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.134 OPEN-SLOT

Default Severity: Not Alarmed (NA)

Logical Object: EQPT

The Open Slot condition indicates that there is an open slot in the system shelf. Slot covers assist with airflow and cooling.

### Clear the OPEN-SLOT Condition

**Step 1** To install a slot cover and clear this condition, refer to the procedures located in the "Install Shelf and Common Control Cards" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Step 2** If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.135 OPTNTWMIS

Default Severity: Major (MJ), Non-Service-Affecting (NSA)

Logical Object: NE

The Optical Network Type Mismatch alarm is raised when DWDM nodes are not configured for the same type of network, either MetroCore or MetroAccess. All DWDM nodes on the same network must be configured for the same network type because APC and ANS behave differently on each of these network types. For more information about APC and ANS, refer to the "Network Reference" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

When the OPTNTWMIS alarm occurs, the "APC-DISABLED" alarm on page 2-18 could also be raised.

**Note** For general information about DWDM cards, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For information about provisioning them, refer to the "Change DWDM Card Settings" chapter.

### Clear the OPTNTWMIS Alarm

**Step 1** In node view of the alarmed node, click the **Provisioning > WDM-ANS > Provisioning** tabs.

**Step 2** Choose the correct option from the Network Type list box, and click **Apply**.

**Step 3** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.136 OPWR-HDEG

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Objects: AOTS, OCH, OMS, OTS

The Output Power High Degrade alarm occurs on all DWDM ports that use a power setpoint, including the OPT-BST and OPT-PRE card AOTS ports in control-power mode; the 32DMX, 32DMX-O, 32MUX-O, and 32WSS card OCH ports; and the OSC-CSM and OSCM OSC-TX ports.

The alarm generally indicates that an internal signal transmission problem prevents the signal output power from maintaining its setpoint and the signal has crossed the high-degrade threshold. For 32DMX, 32DMX-O, 32MUX-O, and 32WSS OCH ports and OSC-CSM and OSCM OSC-TX ports, OPWR-HDEG indicates that the card has a VOA control circuit failure affecting its attenuation capability. The alarmed card should be replaced at the next opportunity.

**Note** For more information about provisioning gain setpoints and VOA setpoints, refer to the "Node Reference" and "Network Reference" chapters, respectively, of the *Cisco ONS 15454 DWDM Installation and Operations Guide*. The "Hardware Specifications" appendix contains power level tables for each card.

### Clear the OPWR-HDEG Alarm

**Step 1** Verify fiber continuity to the port by following site practices. Refer to the "Network Reference" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide* for a procedure to detect a fiber cut.

**Step 2** If the cabling is good, confirm that the LED is correctly illuminated on the physical card. A green ACT/SBY LED indicates an active card. A red ACT/SBY LED indicates a failed card.

**Step 3** Verify that the power read by photodiode on the port is within the expected range as projected by Cisco MetroPlanner. The application generates a spreadsheet of values containing this information.

**Step 4** If the optical power level is within specifications, check the opwrMin threshold. (These are listed in the “Hardware Specifications” appendix of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.) Refer to the *Cisco MetroPlanner DWDM Operations Guide* and decide what value to use for modifying the power level:

a. Double-click the card to open the card view.

b. Display the optical thresholds by clicking the following tabs:

- For the OPT-BST card, click the **Provisioning > Opt. Ampli. Line > Optics Thresholds** tabs.
- For the OPT-PRE card, click the **Provisioning > Opt. Ampli. Line > Optics Thresholds** tabs.
- For the WXC card, click the **Provisioning** > **Optical Chn** > **Optics Thresholds** tabs.
- For the AD-xC-xx.x card, click the **Provisioning > Optical Chn > Optics Thresholds** tabs.
- For the AD-xB-xx.x card, click the **Provisioning > Optical Band > Optics Thresholds** tabs.
- For the 32DMX or 32DMX-O card, click the **Provisioning > Optical Chn > Optics Thresholds** tabs.
- For the 32MUX-O card, click the **Provisioning > Optical Chn > Optics Thresholds** tabs.
- For the 32WSS card, click the **Provisioning > Optical Chn: Optical Connector** x **> Optics Thresholds** tabs.
- For the OSCM or OSC-CSM cards, click the **Provisioning > Optical Line > Optics Thresholds** tabs.

**Step 5** If the received optical power level is within specifications, refer to the *Cisco MetroPlanner DWDM Operations Guide* to determine the correct levels and check the opwrMin threshold. (These are listed in the “Hardware Specifications” appendix of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.) If necessary, modify the value as required.

**Step 6** If the optical power is outside of the expected range, verify that all involved optical signal sources, namely the TXP or MXP trunk port or an ITU-T line card, are in IS administrative state by clicking the correct tab:

- For the MXPP_MR_2.5G card, click the **Provisioning > Line > SONET** (or **Provisioning > Line > SDH**) tabs.
- For the MXP_2.5G_10E card, click the **Provisioning > Line > Trunk** tabs.
- For the MXP_2.5G_10G card, click the **Provisioning > Line > SONET** (or **Provisioning > Line > SDH**) tabs.
- For the MXP_MR_2.5G card, click the **Provisioning > Line > SONET** (or **Provisioning > Line > SDH**) tabs.
- For the TXPP_MR_2.5G card, click the **Provisioning > Line > SONET** (or **Provisioning > Line > SDH**) tabs.
- For the TXP_MR_10E card, click the **Provisioning > Line > SONET** (or **Provisioning > Line > SDH**) tabs.
- For the TXP_MR_10G card, click the **Provisioning > Line > SONET** (or **Provisioning > Line > SDH**) tabs.
- For the TXP_MR_2.5G card, click the **Provisioning > Line > SONET** (or **Provisioning > Line > SDH**) tabs.

If it is not IS, choose **IS (or Unlocked)** from the administrative state drop-down list. This creates the IS-NR service state.

**Step 7** If the port is in IS (or Unlocked) state but its output power is outside of the specifications, complete the "Clear the LOS-P (OCH) Alarm" procedure on page 2-78. (These specifications are listed in the "Hardware Specifications" appendix of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.)

**Step 8** If the signal source is IS and within expected range, come back to the unit reporting OPWR-HDEG and clean all connected fiber in the same line direction as the reported alarm according to site practice. If no site practice exists, complete the procedure in the "Maintain the Node" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

> **Note** Unplugging fiber can cause a traffic hit. To avoid this, perform a traffic switch if possible. Refer to the procedures in the "2.9.1 Protection Switching, Lock Initiation, and Clearing" section on page 2-149. For more detailed protection switching information, refer to the "Manage the Node" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Step 9** Repeat Steps 1 to 8 for any other port on the card reporting the OPWR-HDEG alarm.

**Step 10** If the alarm does not clear, look for and troubleshoot any other alarm that could identify the source of the problem.

**Step 11** If no other alarms exist that could be the source of the OPWR-HDEG, or if clearing an alarm did not clear the alarm, place all of the card ports in **OOS,DSBLD** (or **Locked,disabled)** administrative state.

**Step 12** Complete the "Physically Replace a Card" procedure on page 2-154 for the reporting card.

**Step 13** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.137 OPWR-HFAIL

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Objects: AOTS, OCH, OMS, OTS

The Output Power Failure alarm occurs on an amplifier card (OPT-BST or OPT-PRE) AOTS port if the transmitted power exceeds the high fail threshold. This alarm is raised only in control power working mode. The alarmed card should be replaced at the next opportunity.

> **Note** For general information about DWDM cards, refer to the "Card Reference" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For information about changing their settings, refer to the "Change DWDM Card Settings" chapter.

### Clear the OPWR-HFAIL Alarm

**Step 1** Complete the "Clear the OPWR-HDEG Alarm" procedure on page 2-103.

**Step 2** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

## 2.7.138 OPWR-LDEG

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Objects: AOTS, OCH, OMS, OTS

The Output Power Low Degrade alarm occurs on all DWDM ports that use a setpoint, including the an amplifier card (OPT-BST or OPT-PRE) AOTS ports in control-power mode; the 32DMX, 32DMX-O, 32MUX-O, and 32WSS card OCH ports; and the OSC-CSM and OSCM card OSC-TX ports.

The alarm generally indicates that an internal signal transmission problem prevents the signal output power from maintaining its setpoint and the signal has crossed the low degrade threshold. For the 32DMX, 32DMX-O, 32MUX-O, and 32WSS card OCH ports and the OSC-CSM and OSCM card OSC-TX ports, the OPWR-HDEG alarm indicates that the card has a VOA control circuit failure affecting its attenuation capability. The alarmed card should be replaced at the next opportunity.

**Note** For general information about DWDM cards, refer to the "Card Reference" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For more information about provisioning VOA setpoints, refer to the "Network Reference" chapter.

### Clear the OPWR-LDEG Alarm

**Step 1** Complete the "Clear the OPWR-HDEG Alarm" procedure on page 2-103.

**Step 2** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.139 OPWR-LFAIL

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Objects: AOTS, OCH, OMS, OTS

The Output Power Failure alarm applies to an amplifier card (OPT-BST or OPT-PRE) AOTS ports. It also applies to AD-1B-xx.x, AD-4B-xx.x, AD-1C-xx.x, AD-2C-xx.x, AD-4C-xx.x, OPT-PRE, OPT-BST, 32MUX-O, 32DMX, 32DMX-O, 32DMX, 32WSS, WXC and OSC-CSM transmit ports. The alarm is raised when monitored input power crosses the low fail threshold.

For the AD-1B-xx.x, AD-4B-xx.x, AD-1C-xx.x, AD-2C-xx.x, and AD-4C-xx.x card OCH ports and the 32MUX-O, 32DMX, 32DMX-O; 32WSS, OSCM, and OSC-CSM cards, OPWR-LFAIL indicates that the card has a VOA control circuit failure that affects its attenuation capability.

**Note** For general information about DWDM cards, refer to the "Card Reference" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For more information about provisioning VOA setpoints, refer to the "Network Reference" chapter.

### Clear the OPWR-LFAIL Alarm

**Step 1** Complete the "Clear the OPWR-HDEG Alarm" procedure on page 2-103.

**Step 2** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

## 2.7.140 OSRION

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Objects: AOTS, OTS

The Optical Safety Remote Interlock On condition is raised an amplifier card (OPT-BST or OPT-PRE) when OSRI is set to ON. The condition does not correlate with the "OPWR-LFAIL" alarm on page 2-106, which is also reported on the same port.

### Clear the OSRION Condition

**Step 1** Turn the OSRI off:

a. Double-click the card to open the card view.

b. Click the **Maintenance > ALS** tabs.

c. In the OSRI column, choose **OFF** from the drop-down list.

**Step 2** If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.141 OTUK-AIS

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

Logical Object: TRUNK

The Optical Transport Unit (OTUK) AIS condition applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, MXP_2.5G_10G, and MXP_2.5G_10E cards when ITU-T G.709 encapsulation is enabled for the cards. OTUk-AIS is a generic AIS signal with a repeating AIS PN-11 sequence. This pattern is inserted by the card in the ITU-T G.709 frame (Trunk) when a faulty condition is present on the client side.

The detection of an OTUK-AIS on the RX-Trunk port of a near-end TXP or MXP is a secondary condition that indicates a more serious issue occurring on the far-end TXP/MXP card connected upstream, most likely on the client side. OTUK-AIS is reported in the optical transport unit overhead of the digital wrapper.

ITU-T G.709 encapsulation refers to a digital data wrapper that is transparent across networking standards such as SONET and protocols (such as Ethernet or IP).

**Note** For information about MXP and TXP cards and their monitoring capabilities, refer to the "Card Reference" and "Provision Transponder and Muxponder Cards" chapters in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

### Clear the OTUK-AIS Condition

**Step 1** Complete the "Clear the AIS Condition" procedure on page 2-16.

**Step 2** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.142 OTUK-BDI

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

Logical Object: TRUNK

The Section Monitoring Backward Defect Indication (OTUK BDI) condition applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, MXP_2.5G_10G, and MXP_2.5G_10E cards when ITU-T G.709 encapsulation feature is enabled for the cards. The presence of OTUK-BDI is detected by ITU-T G.709 frame section-monitoring overhead field. The BDI bit is a single bit defined to convey the signal fail status detected in a section termination sink in the upstream direction.

**Note** If the near-end TXP detects an OTUK-BDI condition on its Trunk-RX port, this means that the far-end TXP has inserted the BDI bit in the transmitted (Trunk-Tx) frame, because a failure such as LOS or SD was detected on the Trunk-RX port. Troubleshoot the failure on the far-end side to clear this condition. For information about various DWDM LOS alarms, refer to the appropriate sections in this chapter. For an OC-N/STM-N LOS failure or an SD, refer to the "Alarm Troubleshooting" chapter of the *Cisco ONS 15454 Troubleshooting Guide*.

ITU-T G.709 encapsulation refers to a digital data wrapper that is transparent across networking standards such as SONET and protocols (such as Ethernet or IP).

**Note** For general information about MXP and TXP cards, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For information about provisioning them, refer to the "Provision Transponder and Muxponder Cards" chapter.

### Clear the OTUK-BDI Condition

**Step 1** At the near-end node, use site practices to clean trunk transmitting fiber toward the far-end node and the client receiving fiber. If no site practice exists, complete the procedure in the "Maintain the Node" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Step 2** At the far-end node, determine whether an "OTUK-AIS" condition, page 2-107, is present on the Trunk-RX. If so, the root cause to be investigated is the Trunk-Tx side on the near-end card (the one alarmed for OTUK-BDI) because that is the section where the AIS bit is inserted.

**Step 3** If there is no OTUK-AIS at the far-end node, continue to investigate performances of the Trunk-Rx: Look for other OTU-related alarms, such as the "OTUK-LOF" condition on page 2-110 or "OTUK-SD" condition on page 2-111 at the far-end Trunk-RX. If either is present, resolve the condition using the appropriate procedure in this chapter.

**Step 4** If the OTUK-BDI alarm does not clear, use an OTN test set such as the Agilent OmniBerOTN tester to to check near-end transmitting signal quality. (For specific procedures to use the test set equipment, consult the manufacturer.)

**Step 5** If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.143 OTUK-IAE

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: TRUNK

The OTUK Section-Monitoring Incoming Alignment Error (IAE) alarm occurs on TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, MXP_2.5G_10G, and MXP_2.5G_10E cards when ITU-T G.709 encapsulation is enabled for the cards and the trunk connection is present. This alarm is raised on the near-end node to indicate that the far-end node it has detected errors in the received OTUK frames, but they are not bad enough to cause an "OTUK-LOF" alarm, page 2-110.

The IAE bit in the section overhead allows the ingress point (in this case, the far-end node) to inform its corresponding egress (near-end) point that the alignment error is detected on the incoming signal OTUK frame alignment errors from NE. The error is an out-of-frame (OOF) alignment, in which the optical transport unit overhead frame alignment (FAS) area is errored for more than five frames.

**Note** For general information about MXP and TXP cards, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For information about provisioning them, refer to the "Provision Transponder and Muxponder Cards" chapter.

### Clear the OTUK-IAE Alarm

**Step 1** At the near-end node and far-end node, use site practices to clean transmitting fiber on near-end node's reporting port and receiving fiber on correspondent far-end port. If no site practice exists, complete the procedure in the "Maintain the Node" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Step 2** If the OTUK-IAE alarm does not clear, look for other OTU-related alarm, such as the "OTUK-LOF" alarm, page 2-110, at the far-end node and resolve it using the appropriate procedure in this guide.

**Step 3** If the OTUK-IAE alarm does not clear, use an OTN test set such as the Agilent OmniBerOTN tester to to check near-end transmitting signal quality. For specific procedures to use the test set equipment, consult the manufacturer.

**Step 4** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.144 OTUK-LOF

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: TRUNK

The OTUK-LOF alarm applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, MXP_2.5G_10G, and MXP_2.5G_10E cards when ITU-T G.709 encapsulation is enabled for the cards. The alarm indicates that the card has lost frame delineation on the input data. Loss of frame occurs when the optical transport unit overhead frame alignment (FAS) area is errored for more than five frames and that the error persists more than three milliseconds.

ITU-T G.709 encapsulation refers to a digital data wrapper that is transparent across networking standards such as SONET and protocols (such as Ethernet or IP).

**Note** For general information about MXP and TXP cards, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For information about provisioning them, refer to the "Provision Transponder and Muxponder Cards" chapter.

### Clear the OTUK-LOF Alarm

**Step 1** Verify cabling continuity to the port reporting the alarm.

**Caution** Always use the supplied electrostatic discharge wristband when working with a powered ONS system. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly. To verify cable continuity, follow site practices.

**Step 2** At the far-end node, verify the cabling of the Trunk-TX port of the TXP or MXP connected to alarmed card in the near-end. Clean the fibers according with site practice.(If no site practice exists, refer to the "Maintain the Node" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide* for procedures.)

**Step 3** At the far-end node, verify the ITU-T G.709 encapsulation configuration of the Trunk-TX of the TXP/MXP connected to alarmed card in the near end.

**Step 4** Look for other OTU-related alarms at the far-end Trunk-TX and resolve them if necessary using the appropriate procedure in this guide.

**Step 5** If the OTUK-LOF alarm does not clear on the near end, use an OTN test set such as the Agilent OmniBer OTN tester to check far-end ITU-T G.709 transmitting signal quality. (For specific procedures to use the test set equipment, consult the manufacturer.)

**Step 6** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.145 OTUK-SD

Default Severity: Not Alarmed (NA) Non-Service-Affecting (NSA)

Logical Object: TRUNK

The OTUK-SD condition applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, MXP_2.5G_10G, and MXP_2.5G_10E cards when ITU-T G.709 encapsulation is enabled. The condition indicates that incoming signal quality is poor, but the incoming line BER has not passed the fail threshold. The BER value is calculated on the Trunk-Rx port's incoming ITU-T G.709 encapsulation frame. If FEC or E-FEC feature is enabled, the BER is a pre-FEC measurement.

ITU-T G.709 encapsulation refers to a digital data wrapper that is transparent across networking standards such as SONET and protocols (such as Ethernet or IP).

**Note** For general information about MXP and TXP cards, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For information about provisioning them, refer to the "Provision Transponder and Muxponder Cards" chapter.

### Clear the OTUK-SD Condition

**Step 1** Ensure that the fiber connector for the card is completely plugged in. For more information about fiber connections and card insertion, refer to the "Turn Up a Node" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Step 2** If the BER threshold is correct and at the expected level, use an optical test set to measure the power level of the line to ensure it is within guidelines. For specific procedures to use the test set equipment, consult the manufacturer.

**Step 3** If the optical power level is good, verify that optical receive levels are within the acceptable range.

**Step 4** If receive levels are good, clean the fibers at both ends according to site practice. If no site practice exists, complete the procedure in the "Maintain the Node" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Step 5** If the condition does not clear, verify that single-mode fiber is used.

**Step 6** If the fiber is of the correct type, verify that a single-mode laser is used at the far-end node.

**Step 7** Clean the fiber connectors at both ends for a signal degrade according to site practice.

**Step 8** Verify that a single-mode laser is used at the far end.

**Step 9** If the problem does not clear, the transmitter at the other end of the optical line could be failing and require replacement. Refer to the "2.9.3 Physical Card Reseating, Resetting, and Replacement" section on page 2-153.

**Step 10** If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.146 OTUK-SF

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: TRUNK

The OTUK-SF condition applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, MXP_2.5G_10G, and MXP_2.5G_10E cards when ITU-T G.709 encapsulation is enabled. The condition indicates that incoming signal quality is poor and that the BER for the incoming line has passed the fail threshold. The BER value is calculated on the Trunk-Rx port's incoming ITU-T G.709 encapsulation frame. If FEC or E-FEC feature is enabled, the BER is a pre-FEC measurement.

ITU-T G.709 encapsulation refers to a digital data wrapper that is transparent across networking standards such as SONET and protocols (such as Ethernet or IP).

**Note** For general information about MXP and TXP cards, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For information about provisioning them, refer to the "Provision Transponder and Muxponder Cards" chapter.

### Clear the OTUK-SF Condition

**Step 1** Complete the "Clear the OTUK-SD Condition" procedure on page 2-111.

**Step 2** If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.147 OTUK-TIM

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: TRUNK

The OTUK-TIM alarm applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, MXP_2.5G_10G, and MXP_2.5G_10E cards when ITU-T G.709 encapsulation is enabled and section trace mode is set to manual. The alarm indicates that the expected section-monitoring trail trace identifier (TT1) string does not match the received TTI string and raises a Trace Identifier Mismatch (TIM) alarm. The TIM alarm in turn, triggers an "OTUK-BDI" alarm, page 2-108.

ITU-T G.709 encapsulation refers to a digital data wrapper that is transparent across networking standards such as SONET and protocols (such as Ethernet or IP).

**Note** For general information about MXP and TXP cards, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For information about provisioning them, refer to the "Provision Transponder and Muxponder Cards" chapter.

### Clear the OTUK-TIM Condition

**Step 1** Complete the "Clear the TIM Alarm" procedure on page 2-141.

**Step 2** If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.148 OUT-OF-SYNC

Default Severity: Major (MJ), Service-Affecting (SA); Not Alarmed (NA), Non-Service-Affecting (NSA) for ISC

Logical Objects: FC, GE, ISC, TRUNK

The Ethernet Out of Synchronization condition occurs on TXP_MR_2.5 and TXPP_MR_2.5 cards when the PPM (SFP) port is not correctly configured for the Gigabit Ethernet payload rate.

**Note** For general information about MXP and TXP cards, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For information about provisioning them, refer to the "Provision Transponder and Muxponder Cards" chapter.

### Clear the OUT-OF-SYNC Condition

**Step 1** Double-click the alarmed card to open the card view.

**Step 2** Click the **Provisioning > Pluggable Port Modules** tabs.

**Step 3** Delete the provisioning for the PPM (SFP) by completing the following steps:

a. Click the PPM (SFP) in the Selected PPM area.

b. Click **Delete**.

**Step 4** Recreate the PPM (SFP):

a. In the Pluggable Port Modules area, click **Create**.

b. In the Create PPM dialog box, choose the PPM (SFP) number you want to create.

c. Click OK.

**Step 5** After the PPM (SFP) is created, provision the port's data rate:

a. In the Pluggable Ports area, click **Create**.

b. In Create Port dialog box, choose **ONE_GE** from the Port Type drop-down list.

c. Click **OK.**

**Step 6** If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.149 PARAM-MISM

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Objects: AOTS, OCH, OMS, OTS

The Plug-in Module Range Settings Mismatch condition is raised an amplifier card (OPT-BST and OPT-PRE), optical add-drop multiplexer (OADM) card (AD-1C-xx.x, AD-2C-xx.x, AD-4C-xx.x, AD-1B-xx.x, and AD-4B-xx.x), multiplexer card (32MUX-O and 32WSS), or demultiplexer cards (32DMX-O and 32DMX) when the parameter range values stored on the card are different from the parameters stored in TCC2/TCC2P database. The condition is not user-serviceable. Log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.150 PEER-NORESPONSE

Default Severity: Major (MJ), Non-Service-Affecting (NSA)

Logical Object: EQPT

The switch agent raises a Peer Card Not Responding alarm if either traffic card in a protection group does not receive a response to the peer status request message. PEER-NORESPONSE is a software failure and occurs at the task level, as opposed to a communication failure, which is a hardware failure between peer cards.

### Clear the PEER-NORESPONSE Alarm

**Step 1** Complete the "Reset a Card in CTC" procedure on page 2-152 for the reporting card.

**Step 2** Verify that the reset is complete and error-free and that no new related alarms appear in CTC. Verify the LED appearance: A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

**Step 3** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.151 PORT-ADD-PWR-DEG-HI

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: OCH

The Add Port Power High Degrade alarm occurs on 32-WSS Add port if an internal signal transmission problem prevents the signal output power from reaching its Degrade-High VOA power setpoint. This alarm indicates that the card has a VOA control circuit failure, which affects the card's automatic signal attenuation. The alarmed card should be replaced at the next opportunity.

**Note** For more information about provisioning VOA setpoints, refer to the "Network Reference" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

### Clear the PORT-ADD-PWR-DEG-HI Alarm

**Step 1** Complete the "Physically Replace a Card" procedure on page 2-154.

**Step 2** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.152 PORT-ADD-PWR-DEG-LOW

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: OCH

The Add Port Power Low Degrade alarm occurs on 32-WSS ADD port if an internal signal transmission problem prevents the signal output power from reaching its Degrade-Low VOA power setpoint. This alarm indicates that the card has a VOA control circuit failure, which affects the card's automatic signal attenuation. The alarmed card should be replaced at the next opportunity.

**Note** For more information about provisioning VOA setpoints, refer to the "Network Reference" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

### Clear the PORT-ADD-PWR-DEG-LOW Alarm

**Step 1** Complete the "Physically Replace a Card" procedure on page 2-154.

**Step 2** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.153 PORT-ADD-PWR-FAIL-HI

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: OCH

The Add Port Power High Fail alarm occurs on a 32WSS ADD port if an internal signal transmission crosses the High Fail threshold and the signal output power surpasses its VOA power setpoint.

**Note** For more information about provisioning VOA setpoints, refer to the "Network Reference" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

### Clear the PORT-ADD-PWR-FAIL-HI Alarm

**Step 1** Verify fiber continuity to the port by following site practices. Refer to the "Network Reference" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide* for a procedure to detect a fiber cut.

**Step 2** If the cabling is good, confirm that the LED is correctly illuminated on the physical card. A green ACT/SBY LED indicates an active card. A red ACT/SBY LED indicates a failed card.

**Step 3** Verify that the received power (opwrMin) is within the expected range shown in Cisco MetroPlanner. To check the level in CTC, complete the following steps:

a. Double-click the 32 WSS card to open the card view.

b. Display the optical thresholds by clicking the **Provisioning > Optical Chn: Optical Connector** x **> Optics Thresholds** tabs.

**Step 4** If the optical power level is within specifications, check the opwrMin threshold and refer to the *Cisco MetroPlanner DWDM Operations Guide* to determine the correct value. (These values are also listed in the "Hardware Specifications" appendix of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.) Modify the value as necessary.

**Step 5** If the power value is outside the expected range, verify that the trunk port of a TXP or MXP card connected to ADD-RX port is in IS-NR service state by clicking the correct tab:

- For the MXPP_MR_2.5G card, click the **Provisioning > Line > SONET** (or **Provisioning > Line > SDH**) tabs.
- For the MXP_2.5G_10E card, click the **Provisioning > Line > Trunk** tabs.
- For the MXP_2.5G_10G card, click the **Provisioning > Line > SONET** (or **Provisioning > Line > SDH**) tabs.
- For the MXP_MR_2.5G card, click the **Provisioning > Line > SONET** (or **Provisioning > Line > SDH**) tabs.
- For the TXPP_MR_2.5G card, click the **Provisioning > Line > SONET** (or **Provisioning > Line > SDH**) tabs.
- For the TXP_MR_10E card, click the **Provisioning > Line > SONET** (or **Provisioning > Line > SDH**) tabs.
- For the TXP_MR_10G card, click the **Provisioning > Line > SONET** (or **Provisioning > Line > SDH**) tabs.
- For the TXP_MR_2.5G card, click the **Provisioning > Line > SONET** (or **Provisioning > Line > SDH**) tabs.

If it is not IS-NR, choose **IS** , or **Unlocked** from the administrative state drop-down list. This creates the IS-NR service state.

**Step 6** If the port is in IS-NR service state but its output power is outside of the specifications, complete the "Clear the LOS-P (OCH) Alarm" procedure on page 2-78. (These specifications are listed in the "Hardware Specifications" appendix of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.)

**Step 7** If the signal source is IS-NR and within expected range, come back to the port reporting the PORT-ADD-PWR-FAIL-HIGH alarm and clean the fiber according to site practice. If no site practice exists, complete the procedure in the "Maintain the Node" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Step 8** Repeat Steps 1 through 7 for any other port on the card reporting the alarm.

**Step 9** If the alarm does not clear, look for and troubleshoot any other alarm that could identify the source of the problem.

**Step 10** If no other alarms exist that could be the source of the PORT-ADD-PWR-FAIL-HIGH, or if this procedure did not clear the alarm, place all of the card ports in **OOS,DSBLD** (or **Locked,disabled)** administrative state.

**Step 11** Complete the "Physically Replace a Card" procedure on page 2-154 for the reporting card.

**Step 12** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.154 PORT-ADD-PWR-FAIL-LOW

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: OCH

The Add Port Power Low Fail alarm occurs on a 32WSS ADD port if an internal signal transmission crosses the Low Fail threshold and prevents the signal output power from reaching its VOA power setpoint. This alarm indicates that the card has a VOA control circuit failure, which affects the card automatic signal attenuation.

**Note** For more information about provisioning VOA setpoints, refer to the "Netwkr Reference" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

### Clear the PORT-ADD-PWR-FAIL-LOW Alarm

**Step 1** Verify fiber continuity to the port by following site practices. Refer to the "Network Reference" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide* for a procedure to detect a fiber cut.

**Step 2** If the cabling is good, confirm that the LED is correctly illuminated on the physical card. A green ACT/SBY LED indicates an active card. A red ACT/SBY LED indicates a failed card.

**Step 3** Verify that the received power (opwrMin) is within the expected range shown in Cisco MetroPlanner. To check the level in CTC, complete the following steps:

a. Double-click the card to open the card view.

b. Display the optical thresholds by clicking the 32WSS **Provisioning > Optical Chn: Optical Connector** x **> Optics Thresholds** tabs.

**Step 4** If the optical power level is within specifications, check the opwrMin threshold and refer to the *Cisco MetroPlanner DWDM Operations Guide* to determine the correct value. (These specifications are also listed in the "Hardware Specifications" appendix of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.) Modify the value as necessary.

**Step 5** If the power value is outside the expected range verify that the trunk port of a TXP or MXP card connected to ADD-RX port is in IS-NR service state by clicking the correct tab:

- For the MXPP_MR_2.5G card, click the **Provisioning > Line > SONET** (or **Provisioning > Line > SDH**) tabs.
- For the MXP_2.5G_10E card, click the **Provisioning > Line > Trunk** tabs.
- For the MXP_2.5G_10G card, click the **Provisioning > Line > SONET** (or **Provisioning > Line > SDH**) tabs.
- For the MXP_MR_2.5G card, click the **Provisioning > Line > SONET** (or **Provisioning > Line > SDH**) tabs.
- For the TXPP_MR_2.5G card, click the **Provisioning > Line > SONET** (or **Provisioning > Line > SDH**) tabs.

- For the TXP_MR_10E card click the **Provisioning > Line > SONET** (or **Provisioning > Line > SDH**) tabs.
- For the TXP_MR_10G card, click the **Provisioning > Line > SONET** (or **Provisioning > Line > SDH**) tabs.
- For the TXP_MR_2.5G card, click the **Provisioning > Line > SONET** (or **Provisioning > Line > SDH**) tabs.

If it is not IS-NR, choose **IS** , or **Unlocked** from the administrative state drop-down list.

**Step 6** If the port is in IS-NR service state but its output power is outside of the specifications, complete the "Clear the LOS-P (OCH) Alarm" procedure on page 2-78. (These specifications are also listed in the "Hardware Specifications" appendix of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.)

**Step 7** If the signal source is IS-NR and within expected range, come back to the port reporting the PORT-ADD-PWR-FAIL-LOW alarm and clean the fiber according to site practice. If no site practice exists, complete the procedure in the "Maintain the Node" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Step 8** Repeat Steps 1 through 7 for any other port on the card reporting the alarm.

**Step 9** If the alarm does not clear, look for and troubleshoot any other alarm that could identify the source of the problem.

**Step 10** If no other alarms exist that could be the source of the PORT-ADD-PWR-FAIL-LOW, or if this procedure did not clear the alarm, place all of the card ports in **OOS,DSBLD** (or **Locked,disabled)** administrative state.

**Step 11** Complete the "Physically Replace a Card" procedure on page 2-154 for the reporting card.

**Step 12** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.155 PORT-FAIL

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: OCH

The APC Port Failure alarm occurs when amplifier margins and VOA are saturated for a port, so APC cannot apply any control. For example, it is raised if APC attempts to set an OPT-BST port's gain higher than 20 dBm (the maximum setpoint) or its attenuation on Express VOA lower than 0 dBm (the minimum setpoint).

**Note** For more information about provisioning VOA setpoints, refer to the "Network Reference" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

### Clear the PORT-FAIL Alarm

**Step 1** If a maintenance operation such as fiber repair, adding a card, or replacing a card has just been performed on the optical network (whether at the node raising the PORT-FAIL alarm or at any other node), determine whether this operation has added extra loss. This can happen if the repair is imperfect or if a patchcord is dirty. To test for signal loss, refer to procedures in the "Network Reference" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Step 2** If there is loss added and fiber has been repaired or removed, first try cleaning the fiber by completing the procedures in the "Maintain the Node" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Step 3** If the alarm does not clear and fiber has been repaired, perform the repair again with new fiber if necessary. For fibering procedures, refer to the "Turn Up a Node" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*. If the alarm does not clear, go to Step 4.

**Step 4** If a maintenance operation has not been recently executed on the network, the alarm indicates that the network has consumed all of its allocated aging margins. In this case, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

## 2.7.156 PROTNA

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: EQPT

The Protection Unit Not Available alarm is caused by an OOS (or Locked) protection card when a TCC2/TCC2P or XC10G card that has been provisioned as part of a protection group is not available. Unavailable protection can occur when a card is reset, but the alarm clears as soon as the card is back in service. The alarm clears if the device or facility is brought back in service.

### Clear the PROTNA Alarm

**Step 1** If the PROTNA alarm occurs and does not clear, and if it is raised against a controller card, ensure that there is a redundant TCC2/TCC2P installed and provisioned in the chassis.

**Step 2** If the alarm is raised against a line card, verify that the ports have been taken out of service (OOS,MT):

a. In CTC, double-click the reporting card to open the card view (if the card is not an XC10G card).

b. Click the **Provisioning** tab.

c. Click the administrative state of any in-service (IS) ports.

d. Choose **OOS,MT** (or **Locked,maintenance**) to take the ports out of service.

**Step 3** Complete the "Reset a Card in CTC" procedure on page 2-152 for the reporting card.

**Step 4** Verify that the reset is complete and error-free and that no new related alarms appear in CTC. Verify the LED appearance: A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

**Step 5** If the alarm does not clear, complete the "Remove and Reinsert (Reseat) Any Card" procedure on page 2-154 for the reporting card.

**Step 6** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.157 PROV-MISMATCH

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: PPM

The Provisioning Mismatch for an SFP alarm is raised against an SFP connector on MXP_2.5G_10E, MXP_2.5G_10G, MXP_MR_2.5G, MXPP_MR_2.5G, TXP_MR_2.5G, TXP_MR_10E, and TXPP_MR_2.5G under one of the following circumstances:

- The physical SFP's range or wavelength does not match the provisioned value. SFPs have static wavelength values which must match the wavelengths provisioned for the card.
- The SFP's reach (loss) value does not meet the reach value needed for the card.
- The reach of the inserted SFP does not match the physical SFP.

### Clear the PROV-MISMATCH Alarm

**Step 1** Determine what the SFP wavelength range should be by viewing the frequency provisioned for the card:

a. Double-click the card to open the card view.

b. Click the **Maintenance > Info** tabs.

c. Record the value shown in the **Value** column.

**Step 2** Remove the incorrect SFP connector:

a. Unplug the SFP connector and fiber from the reporting card.

b. if the SFP connector has a latch securing the fiber cable, pull the latch upward to release the cable.

c. Pull the fiber cable straight out of the connector.

**Step 3** Replace the unit with the correct SFP connector:

a. Plug the fiber into a Cisco-supported SFP connector. For more information about supported SFPs, refer to the "Hardware Specifications" appendix of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

b. If the new SFP connector has a latch, close the latch over the cable to secure it.

c. Plug the cabled SFP connector into the card port until it clicks.

**Step 4** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.158 PTIM

Default Severity: Major (MJ), Non-Service-Affecting (NSA)

Logical Object: TRUNK

The Payload Type Identifier Mismatch alarm occurs when there is a mismatch between the way the ITU-T G.709 encapsulation option is configured on MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, TXP_MR_10E, or TXPP_MR_2.5G card at each end of the optical span.

**Note** For general information about MXP and TXP cards, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For information about provisioning them, refer to the "Provision Transponder and Muxponder Cards" chapter.

### Clear the PTIM Alarm

**Step 1** Double-click the alarmed MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, TXP_MR_10E, or TXPP_MR_2.5G card to open the card view.

**Step 2** Click the **Provisioning > OTN > OTN Lines** tabs.

**Step 3** Ensure that the G.709 OTN check box is checked. If not, check it and click **Apply**.

**Step 4** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.159 PWR-FAIL-A

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: EQPT

The Equipment Power Failure at Connector A alarm occurs when there is no power supply from the main power connector to the equipment. This alarm occurs on the electrical interface assemblies (EIA), TCC2/TCC2P, or I/O cards.

**Warning** **The power supply circuitry for the equipment can constitute an energy hazard. Before you install or replace the equipment, remove all jewelry (including rings, necklaces, and watches). Metal objects can come into contact with exposed power supply wiring or circuitry inside the DSLAM equipment. This could cause the metal objects to heat up and cause serious burns or weld the metal object to the equipment.** Statement 207

### Clear the PWR-FAIL-A Alarm

**Step 1** If a single card has reported the alarm, take the following actions depending on the reporting card:

- If the reporting card is an active traffic line port in a 1+1 protection group or part of a path protection, ensure that an APS traffic switch has occurred to move traffic to the protect port.

  **Note** Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "2.9.1 Protection Switching, Lock Initiation, and Clearing" section on page 2-149 for commonly used traffic-switching procedures.

- If the alarm is reported against a TCC2/TCC2P, complete the "Reset an Active TCC2/TCC2P Card and Activate the Standby Card" procedure on page 2-152.
- If the alarm is reported against an OC-N/STM-N card, complete the "Reset a Card in CTC" procedure on page 2-152.

**Step 2** If the alarm does not clear, complete the "Remove and Reinsert (Reseat) Any Card" procedure on page 2-154.

**Step 3** If the alarm does not clear, complete the "Physically Replace a Card" procedure on page 2-154 for the reporting card.

**Step 4** If the single card replacement does not clear the alarm, or if multiple cards report the alarm, verify the office power. Refer to the "Install the Shelf and Common Control Cards" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide* for procedures. See the "1.10 Power Supply Problems" section on page 1-55 as necessary.

**Step 5** If the alarm does not clear, reseat the power cable connection to the connector.

**Step 6** If the alarm does not clear, physically replace the power cable connection to the connector.

**Step 7** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.160 PWR-FAIL-B

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: EQPT

The Equipment Power Failure at Connector B alarm occurs when there is no power supply from the main power connector to the equipment. This alarm occurs on the electrical interface assemblies (EIA), TCC2/TCC2P, or I/O cards.

**Warning** **The power supply circuitry for the equipment can constitute an energy hazard. Before you install or replace the equipment, remove all jewelry (including rings, necklaces, and watches). Metal objects can come into contact with exposed power supply wiring or circuitry inside the DSLAM equipment. This could cause the metal objects to heat up and cause serious burns or weld the metal object to the equipment.** Statement 207

### Clear the PWR-FAIL-B Alarm

**Step 1** Complete the "Clear the PWR-FAIL-A Alarm" procedure on page 2-121.

**Step 2** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.161 PWR-FAIL-RET-A

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: EQPT

The Equipment Power Failure at Connector A alarm occurs when there is no power supplied to the backup power connector on the shelf. This alarm occurs on the electrical interface assemblies (EIA), or TCC2/TCC2P.

### Clear the PWR-FAIL-RET-A Alarm

**Step 1** Complete the "Clear the PWR-FAIL-A Alarm" procedure on page 2-121.

**Step 2** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.162 PWR-FAIL-RET-B

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: EQPT

The Equipment Power Failure at Connector B alarm occurs when there is no power supplied to the backup power connector on the shelf. This alarm occurs on the electrical interface assemblies (EIA), or TCC2/TCC2P.

### Clear the PWR-FAIL-RET-A Alarm

**Step 1** Complete the "Clear the PWR-FAIL-A Alarm" procedure on page 2-121.

**Step 2** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.163 RFI

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

Logical Object: TRUNK

The Remote Failure Indication condition is raised against an MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, TXP_MR_10E, or TXPP_MR_2.5G card when the card has the "AIS" condition, page 2-16. The MXP or TXP cards only raise AIS (or remote failure indication [RFI]) when they are in line or section termination mode, that is, when the MXP or TXP cards in line termination mode or section termination mode have improperly terminated overhead bytes.

> **Note** For general information about MXP and TXP cards, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For information about provisioning them, refer to the "Provision Transponder and Muxponder Cards" chapter.

### Clear the RFI Condition

**Step 1** Complete the "Delete a Circuit" procedure on page 2-155 and then recreate the circuit.

**Step 2** If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.164 RING-ID-MIS

Default Severity: Major (MJ), Non-Service-Affecting (NSA)

Logical Object: OSC-RING

The Ring ID Mismatch condition refers to the ring ID in APC. It occurs when a ring name does not match other detectable node ring names, and can cause problems with applications that require data exchange with APC. This alarm is similar to the RING-MISMATCH alarm, but does not apply to ring protection; rather, RING-ID-MIS applies to DWDM node discovery within the same network.

> **Note** For more information about amplifier APC, refer to the "Card Reference" chapters of the *Cisco ONS 15454 DWDM Installation and Operations Guide.*

### Clear the RING-ID-MIS Alarm

**Step 1** In node view, click the **Provisioning > BLSR** (or **Provisioning > MS-SPRing**) tabs.

**Step 2** Note the name in the Ring Name field.

**Step 3** Log into the next ONS system node in the BLSR (or MS-SPRing).

**Step 4** Complete the "Identify a BLSR Ring Name or Node Number" procedure located in the "Alarm Troubleshooting" chapter of the *Cisco ONS 15454 Troubleshooting Guide* or the "Identify an MS-SPRing Name or Node Number" procedure located in the "Alarm Troubleshooting" chapter of the *Cisco ONS 15454 SDH Troubleshooting Guide*.

**Step 5** If the ring name matches the ring name in the reporting node, repeat Step 4 for the next ONS system in the BLSR (or MS-SPRing).

**Step 6** Complete the "Change a BLSR Ring Name" procedure located in the "Alarm Troubleshooting" chapter of the *Cisco ONS 15454 Troubleshooting Guide* or "Change an MS-SPRing Name or Node Number" procedure located in the "Alarm Troubleshooting" chapter of the *Cisco ONS 15454 SDH Troubleshooting Guide*.

**Step 7** Verify that the ring map is correct.

**Step 8** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.165 SD (TRUNK)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: TRUNK

A Signal Degrade (SD) condition on the trunk occurs when the quality of an optical signal to the MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, TXP_MR_10E, or TXPP_MR_2.5G card has BER on the incoming optical line that passes the signal degrade threshold. The alarm applies to the card ports and the trunk carrying optical or electrical signals to the card.

Signal degrade is defined by Telcordia as a soft failure condition. SD and SF both monitor the incoming BER and are similar, but SD is triggered at a lower BER than SF. The BER threshold on the ONS system is user-provisionable and has a range for SD from 1E–9 dBm to 1E–5 dBm.

**Note** For more information about MXP and TXP cards and their thresholds, refer to the "Card Reference" chapter and the "Hardware Specifications" appendix respectively in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

### Clear the SD (TRUNK) Condition

**Step 1** Ensure that the fiber connector for the card is completely plugged in. For more information about fiber connections and card insertion, refer to the "Turn Up a Node" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Step 2** If the BER threshold is correct and at the expected level, use an optical test set to measure the power level of the line to ensure it is within guidelines. For specific procedures to use the test set equipment, consult the manufacturer.

**Step 3** If the optical power level is good, verify that optical receive levels are within the acceptable range.

**Step 4** If receive levels are good, clean the fibers at both ends according to site practice. If no site practice exists, complete the procedure in the "Maintain the Node" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Step 5** If the condition does not clear, verify that single-mode fiber is used.

**Step 6** If the fiber is of the correct type, verify that a single-mode laser is used at the far-end node.

**Step 7** Clean the fiber connectors at both ends for a signal degrade according to site practice.

**Step 8** Verify that a single-mode laser is used at the far end.

**Step 9** If the problem does not clear, the transmitter at the other end of the optical line could be failing and require replacement. Refer to the "2.9.3 Physical Card Reseating, Resetting, and Replacement" section on page 2-153.

**Step 10** If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.166 SF (TRUNK)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: TRUNK

A Signal Fail (SF) condition for the trunk occurs when the quality of an optical signal to the MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, TXP_MR_10E, or TXPP_MR_2.5G card has BER on the incoming optical line that passes the signal fail threshold. The alarm applies to the card ports and the trunk carrying optical or electrical signals to the card.

Signal fail is defined by Telcordia as a hard failure condition. SF monitors the incoming BER and is triggered when the BER surpasses the default range.

**Warning** **Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard.** Statement 1056

**Warning** **Use of controls, adjustments, or performing procedures other than those specified could result in hazardous radiation exposure.** Statement 1057

**Note** For more information about MXP and TXP cards and their thresholds, refer to the “Card Reference” chapter and the “Hardware Specifications” appendix respectively in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

### Clear the SF (TRUNK) Condition

**Step 1** Complete the “Clear the SD (TRUNK) Condition” procedure on page 2-125.

**Caution** Always use the supplied electrostatic discharge wristband when working with a powered ONS system. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

**Step 2** If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.167 SFTWDOWN

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: EQPT

A Software Download in Progress alarm occurs when the TCC2/TCC2P is downloading or transferring software.

If the active and standby TCC2/TCC2Ps have the same versions of software, it takes approximately three minutes for software to be updated on a standby TCC2/TCC2P.

If the active and standby TCC2/TCC2Ps have different software versions, the transfer can take up to 30 minutes. Software transfers occur when different software versions exist on the two cards. After the transfer completes, the active TCC2/TCC2P reboots and goes into standby mode after approximately three minutes.

No action is necessary. Wait for the transfer or the software download to complete. If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

**Note** SFTWDOWN is an informational alarm.

## 2.7.168 SH-INS-LOSS-VAR-DEG-HIGH

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: OTS

The Switch Insertion Loss Variation Degrade High alarm occurs as the OSC-CSM card optical switch ages and slowly increases its insertion loss. This alarm indicates that the insertion loss has crossed the high degrade threshold. The card must eventually be replaced.

**Note** For more information about insertion loss, refer to the APC section of the "Network Reference" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

### Clear the SH-INS-LOSS-VAR-DEG-HIGH Alarm

**Step 1** For the alarmed card, complete the "Physically Replace a Card" procedure on page 2-154 as appropriate.

**Step 2** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.169 SH-INS-LOSS-VAR-DEG-LOW

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: OTS

The Switch Insertion Loss Variation Degrade Low alarm occurs as the OSC-CSM card optical switch ages and slowly decreases its insertion loss. This alarm indicates that the insertion loss has crossed the low degrade threshold. The card must eventually be replaced.

**Note** For more information about insertion loss, refer to the APC section in the "Network Reference" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

### Clear the SH-INS-LOSS-VAR-DEG-LOW Alarm

**Step 1** For the alarmed card, complete the "Physically Replace a Card" procedure on page 2-154 as appropriate.

**Step 2** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.170 SHUTTER-OPEN

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: OTS

The SHUTTER-OPEN condition occurs if an OSC-CSM card laser shutter remains open after the "LOS (OTS)" alarm on page 2-73 is detected. A laser shutter remains open if an optical safety issue is present and closes when the OSC-CSM card LINE-RX port receives OSC power for three consecutive seconds.

### Clear the SHUTTER-OPEN Condition

**Step 1** Complete the "Clear the LOS (OTS) Alarm" procedure on page 2-73.

**Step 2** If the SHUTTER-OPEN condition still does not clear, it indicates that the unit shutter is not working properly. Complete the "Physically Replace a Card" procedure on page 2-154.

**Step 3** If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.171 SIGLOSS

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Objects: FC, GE, ISC, TRUNK

The Signal Loss on Data Interface alarm is raised on MXP card FC and ISC client data ports when there is a loss of signal. (Loss of Gigabit Ethernet client signal results in a CARLOSS [GE], not SIGLOSS.) SIGLOSS can also be raised on the MXP trunk port.

If the SYNCLOSS alarm was previously raised on the port, the SIGLOSS alarm will demote it.

### Clear the SIGLOSS Alarm

**Step 1** Ensure that the port connection at the near end of the SONET or SDH (ETSI) link is operational.

**Step 2** Verify fiber continuity to the port. To verify fiber continuity, follow site practices.

**Step 3** Check the physical port LED on the card. The port LED looks clear (that is, not lit green) if the link is not connected.

**Step 4** If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

## 2.7.172 SNTP-HOST

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: NE

The Simple Network Timing Protocol (SNTP) Host Failure alarm indicates that an ONS system serving as an IP proxy for the other ONS system nodes in the ring is not forwarding SNTP information to the other nodes in the network. The forwarding failure can result from two causes: either the IP network attached to the ONS system proxy node is experiencing problems, or the ONS system proxy node itself is not functioning properly.

### Clear the SNTP-HOST Alarm

**Step 1** Ping the SNTP host from a workstation in the same subnet to ensure that communication is possible within the subnet by completing the "Verify PC Connection to the ONS 15454 (ping)" procedure on page 1-37.

**Step 2** If the ping fails, contact the network administrator who manages the IP network that supplies the SNTP information to the proxy and determine whether the network is experiencing problems, which could affect the SNTP server/router connecting to the proxy ONS system.

**Step 3** If no network problems exist, ensure that the ONS system proxy is provisioned correctly:

a. In node view for the ONS system serving as the proxy, click the **Provisioning > General** tabs.

b. Ensure that the Use NTP/SNTP Server check box is checked.

c. If the Use NTP/SNTP Server check box is not checked, click it.

d. Ensure that the Use NTP/SNTP Server field contains a valid IP address for the server.

**Step 4** If proxy is correctly provisioned, refer to the "Timing" chapter in the *Cisco ONS 15454 DWDM Reference Manual* for more information on SNTP Host.

**Step 5** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.173 SQUELCHED

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Objects: 2R, ESCON, FC, GE, ISC, OCN/STMN, TRUNK

The Client Signal Squelched condition is raised by a TXP_MR_10G, TXP_MR_10E, TXP_MR_2.5G, TXPP_MR_2.5G, MXP_2.5G_10G, MXP_2.5G_10E, MXP_MR_2.5G, and MXPP_MR_2.5G card.

The condition can be raised in the following situations:

- An MXP or TXP client facility detects that an upstream receive facility has experienced a loss of signal (such as an Ethernet CARLOSS, DWDM SIGLOSS, or optical LOS). In response, the facility's transmit is turned off (SQUELCHED). The upstream receive facilities are the trunk receive on the same card as the client, as well as the client receive on the card at the other end of the trunk span.
- The client will squelch if the upstream trunk receive (on the same card) experiences a SIGLOSS, Ethernet CARLOSS, LOS, or LOS (TRUNK) alarm. In some transparent modes, the client is squelched if the trunk detects an AIS condition or a TIM alarm.
- The client will squelch if the upstream client receive (on the card at the other end of the DWDM span) experiences CARLOSS, SIGLOSS, or LOS.

In an example situation, an upstream MXP_2.5G_10G client port receive experiences a "loss of light," and this port raises CARLOSS, SIGLOSS, or LOS (determined by the payload type) locally.

The local client raises SQUELCHED if it also raises one of the following alarms for the client, all of which are signalled by the upstream node:

- 2.7.123 ODUK-1-AIS-PM, page 2-96
- 2.7.124 ODUK-2-AIS-PM, page 2-97
- 2.7.125 ODUK-3-AIS-PM, page 2-97
- 2.7.126 ODUK-4-AIS-PM, page 2-98

On the MXP_MR_10G, the local client raises a SQUELCHED condition if the upstream client detects one of the following alarms. Note that no corresponding local alarm is raised to indicate which of these conditions is present upstream.

- LOS for the clients including the "LOS (2R)" alarm on page 2-69, the "LOS (ESCON)" alarm on page 2-71, and the "LOS (ISC)" alarm on page 2-72
- CARLOSS for the clients including the "CARLOSS (FC)" alarm on page 2-27, the "CARLOSS (GE)" alarm on page 2-28, and the "CARLOSS (ISC)" alarm on page 2-29

The local client raises a SQUELCHED condition if the local trunk raises one of the following alarms:

- 2.7.144 OTUK-LOF, page 2-110
- 2.7.141 OTUK-AIS, page 2-107
- 2.7.90 LOS (TRUNK), page 2-73
- 2.7.147 OTUK-TIM, page 2-112 (squelching enabled)
- 2.7.127 ODUK-AIS-PM, page 2-98
- 2.7.129 ODUK-LCK-PM, page 2-99
- 2.7.133 ODUK-TIM-PM, page 2-101 (squelching enabled)
- 2.7.198 TIM, page 2-140 (for the OCN/STMN, squelching enabled)
- LOF (OCN/STMN) alarm in the "Alarm Troubleshooting" chapter of the *Cisco ONS 15454 Troubleshooting Guide* or *Cisco ONS 15454SDH Troubleshooting Guide*
- LOS (OCN/STMN) alarm the "Alarm Troubleshooting" chapter of the *Cisco ONS 15454 Troubleshooting Guide* or *Cisco ONS 15454SDH Troubleshooting Guide*
- 2.7.22 CARLOSS (TRUNK), page 2-29
- 2.7.213 WVL-MISMATCH, page 2-147 (client or trunk)

When troubleshooting the SQUELCHED condition locally, look for failures progressing upstream in the following order. (If you are troubleshooting this alarm remotely, reverse the order of progress.)

- Local client alarms, as previously listed
- Local trunk alarms, as previously listed
- Remote (upstream) client receive alarms, as previously listed

**Note** If you see a SQUELCHED condition on the trunk, this can only be caused by a transponder (TXP) card.

### Clear the SQUELCHED Condition

**Step 1** If the object is reported against any object besides ESCON, determine whether the remote node and local node reports and LOF or the LOS alarm (for the client trunk, as listed here). If it does, turn to the relevant section in this chapter and complete the troubleshooting procedure.

**Step 2** If no LOF or LOS is reported, determine whether any other listed remote node or local node conditions as listed here have occurred. If so, turn to the relevant section of this chapter and complete the troubleshooting procedure.

**Step 3** If none of these alarms is reported, determine whether the local port reporting the SQUELCHED condition is in loopback. (You will see LPBKFACILITY OR LPBKTERMINAL in the condition window for this port.) If it is in loopback, complete the following steps:

a. Double-click the client card to open the card view.

b. Click the **Maintenance > Loopback > Port** tabs.

c. If the port Admin State column says OOS,MT (or Locked,maintenance) or OOS,DSBLD, click the cell to highlight it and choose **IS** , or **Unlocked** from the drop-down list. Changing the state to IS (or Unlocked) also clears any loopback provisioned on the port.

**Step 4** If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.174 SSM-DUS

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: TRUNK

The Synchronization Status (SSM) Message Quality Changed to Do Not Use (DUS) condition occurs on MXP trunk ports when the synchronization status message (SSM) quality level degrades to DUS or is manually changed to DUS.

The signal is often manually changed to DUS to prevent timing loops from occurring. Sending a DUS prevents the timing from being reused in a loop. The DUS signal can also be sent for line maintenance testing.

**Note** SSM-DUS is an informational condition and does not require troubleshooting.

## 2.7.175 SSM-FAIL

Single Failure Default Se verity: Minor (MN), Non-Service-Affecting (NSA); Double Failure Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: TRUNK

The SSM Failed alarm occurs on MXP trunk ports when the synchronization status messaging received by the system fails. The problem is external to the ONS system. This alarm indicates that although the ONS system is set up to receive SSM, the timing source is not delivering valid SSM messages.

### Clear the SSM-FAIL Alarm

**Step 1** Verify that SSM is enabled on the external timing source.

**Step 2** If timing is enabled, use an optical test set to determine that the external timing source is delivering SSM. For specific procedures to use the test set equipment, consult the manufacturer.

**Step 3** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.176 SSM-LNC

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: TRUNK

The SSM Local Node Clock (LNC) Traceable condition occurs on MXP trunk ports when the SSM (S1) byte of the SONET overhead multiplexing section has been changed to signify that the line or BITS timing source is the LNC.

**Note** SSM-LNC is an informational condition and does not require troubleshooting.

## 2.7.177 SSM-OFF

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: TRUNK

The SSM Off condition applies to references used for timing related to the MXP trunk port. It occurs when the SSM for the reference has been turned off. The node is set up to receive SSM, but the timing source is not delivering SSM messages.

### Clear the SSM-OFF Condition

**Step 1** Complete the "Clear the SSM-FAIL Alarm" procedure on page 2-132.

**Step 2** If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.178 SSM-PRC

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: TRUNK

The SSM Primary Reference Clock (PRC) Traceable condition occurs when the SONET transmission level for an MXP trunk port is PRC.

**Note** SSM-PRC is an informational condition and does not require troubleshooting.

## 2.7.179 SSM-PRS

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: TRUNK

The SSM Primary Reference Source (PRS) Traceable condition occurs when the SSM transmission level for an MXP trunk port is Stratum 1 Traceable.

**Note** SSM-PRS is an informational condition and does not require troubleshooting.

## 2.7.180 SSM-RES

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: TRUNK

The SSM Reserved (RES) For Network Synchronization Use condition occurs when the synchronization message quality level for an MXP trunk port is RES.

**Note** SSM-RES is an informational condition and does not require troubleshooting.

## 2.7.181 SSM-SMC

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: TRUNK

The SSM SONET Minimum Clock (SMC) Traceable condition occurs when the synchronization message quality level for an MXP trunk port is SMC. The login node does not use the clock because the node cannot use any reference beneath its internal level, which is ST3.

**Note** SSM-SMC is an informational condition and does not require troubleshooting.

## 2.7.182 SSM-ST2

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: TRUNK

The SSM Stratum 2 (ST2) Traceable condition occurs when the synchronization message quality level for an MXP trunk port is ST2.

**Note** SSM-ST2 is an informational condition and does not require troubleshooting.

## 2.7.183 SSM-ST3

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: TRUNK

The SSM Stratum 3 (ST3) Traceable condition occurs when the synchronization message quality level for an MXP trunk port is ST3.

**Note** SSM-ST3 is an informational condition and does not require troubleshooting.

## 2.7.184 SSM-ST3E

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: TRUNK

The SSM Stratum 3E (ST3E) Traceable condition indicates that the synchronization message quality level for an MXP trunk port is ST3E. SSM-ST3E is a Generation 2 SSM and is used for Generation 1.

**Note** SSM-ST3E is an informational condition and does not require troubleshooting.

## 2.7.185 SSM-ST4

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: TRUNK

The SSM Stratum 4 (ST4) Traceable condition occurs when the synchronization message quality level is ST4 for an MXP trunk port. The message quality is not used because it is below ST3.

**Note** SSM-ST4 is an informational condition and does not require troubleshooting.

## 2.7.186 SSM-STU

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: TRUNK

The SSM Synchronization Traceability Unknown (STU) condition occurs when the reporting node is timed to a reference that does not support SSM, but the ONS system has SSM support enabled (for the MXP trunk port). SSM-STU can also occur if the timing source is sending out SSM messages but SSM is not enabled on the ONS system.

### Clear the SSM-STU Condition

**Step 1** In node view, click the **Provisioning > Timing > BITS Facilities** tabs.

**Step 2** Complete one of the following depending upon the status of the Sync Messaging Enabled check box:

- If the **Sync. Messaging Enabled** check box for the BITS source is checked, uncheck the box.
- If the **Sync. Messaging Enabled** check box for the BITS source is not checked, check the box.

**Step 3** Click **Apply**.

**Step 4** If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.187 SSM-TNC

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: TRUNK

The SSM Transit Node Clock (TNC) Traceable condition occurs when the synchronization message quality level is TNC for an MXP trunk port.

**Note** SSM-TNC is an informational condition and does not require troubleshooting.

## 2.7.188 SWTOPRI

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Objects: EXT-SREF, NE-SREF

The Synchronization Switch to Primary Reference condition occurs when the ONS system switches to the primary timing source (reference 1). The ONS system uses three ranked timing references. The timing references are typically two BITS-level or line-level sources and an internal reference.

**Note** SWTOPRI is an informational condition and does not require troubleshooting.

## 2.7.189 SWTOSEC

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Objects: EXT-SREF, NE-SREF

The Synchronization Switch to Secondary Reference condition occurs when the ONS system has switched to a secondary timing source (reference 2).

### Clear the SWTOSEC Condition

**Step 1** To clear the condition, clear alarms related to failures of the primary source, such as the "SYNCPRI" alarm on page 2-138.

**Step 2** If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.190 SWTOTHIRD

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Objects: EXT-SREF, NE-SREF

The Synchronization Switch to Third Reference condition occurs when the ONS system has switched to a third timing source (reference 3).

### Clear the SWTOTHIRD Condition

**Step 1** To clear the condition, clear alarms related to failures of the primary source, such as the "SYNCPRI" alarm on page 2-138 or the "SYNCSEC" alarm on page 2-138.

**Step 2** If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.191 SYNC-FREQ

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: TRUNK

The Synchronization Reference Frequency Out of Bounds condition is reported against any reference that is out of the bounds for valid references. The login node fails the reference and chooses another internal or external reference to use.

### Clear the SYNC-FREQ Condition

**Step 1** Use an optical test set to verify the timing frequency of the line or BITS timing source and ensure that it falls within the proper frequency. For specific procedures to use the test set equipment, consult the manufacturer.

For BITS, the proper timing frequency range is approximately –15 PPM to 15 PPM. For optical line timing, the proper frequency range is approximately –16 PPM to 16 PPM.

**Step 2** If the reference source frequency is not outside of bounds, complete the "Physically Replace a Card" procedure on page 2-154 for the TCC2/TCC2P.

**Note** It takes up to 30 minutes for the TCC2/TCC2P to transfer the system software to the newly installed TCC2/TCC2P. Software transfer occurs in instances where different software versions exist on the two cards. When the transfer completes, the active TCC2/TCC2P reboots and goes into standby mode after approximately three minutes.

**Step 3** If the SYNC-FREQ condition continues to report after replacing the TCC2/TCC2P, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.192 SYNCLOSS

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Objects: FC, GE, ISC, TRUNK

The Loss of Synchronization on Data Interface alarm is raised on MXP card client and trunk ports when there is a loss of signal synchronization on the port. This alarm is demoted by the SIGLOSS alarm.

### Clear the SYNCLOSS Alarm

**Step 1** Ensure that the data port connection at the near end of the SONET or SDH (ETSI) link is operational.

**Step 2** Verify fiber continuity to the port. To do this, follow site practices.

**Step 3** View the physical port LED to determine whether the alarm has cleared.

- If the LED is green, the alarm has cleared.
- If the port LED is clear (that is, not lit green), the link is not connected and the alarm has not cleared.
- If the LED is red, this indicates that the fiber is pulled.

**Step 4** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) to report a service-affecting problem.

## 2.7.193 SYNCPRI

Default Severity: Minor (MN), Non-Service-Affecting (NSA) for EXT-SREF

Logical Objects: EXT-SREF, NE-SREF

A Loss of Timing on Primary Reference alarm occurs when the ONS system loses the primary timing source (reference 1). The ONS system uses three ranked timing references. The timing references are typically two BITS-level or line-level sources and an internal reference. If SYNCPRI occurs, the ONS system should switch to its secondary timing source (reference 2). Switching to the secondary timing source also triggers the "SWTOSEC" alarm, page 2-136.

### Clear the SYNCPRI Alarm

**Step 1** In node view, click the **Provisioning > Timing > General** tabs.

**Step 2** Verify the current configuration for REF-1 of the NE Reference.

**Step 3** If the primary timing reference is a BITS input, complete the "Clear the LOS (BITS) Alarm" procedure on page 2-70.

**Step 4** If the primary reference clock is an incoming port on the ONS system, complete the "Clear the LOS (OCN/STMN) Alarm" procedure located in the "Alarm Troubleshooting" chapter of the *Cisco ONS 15454 Troubleshooting Guide* or *Cisco ONS 15454SDH Troubleshooting Guide*.

**Step 5** If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.194 SYNCSEC

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Objects: EXT-SREF, NE-SREF

A Loss of Timing on Secondary Reference alarm occurs when the ONS system loses the secondary timing source (reference 2). If SYNCSEC occurs, the ONS system should switch to a third timing source (reference 3) to obtain valid timing for the ONS system. Switching to a third timing source also triggers the "SWTOTHIRD" alarm, page 2-136.

### Clear the SYNCSEC Alarm

**Step 1** In node view, click the **Provisioning > Timing > General** tabs.

**Step 2** Verify the current configuration of REF-2 for the NE Reference.

**Step 3** If the secondary reference is a BITS input, complete the "Clear the LOS (BITS) Alarm" procedure on page 2-70.

**Step 4** Verify that the BITS clock is operating properly.

**Step 5** If the secondary timing source is an incoming port on the ONS system, complete the "Clear the LOS (OCN/STMN) Alarm" procedure located in the "Alarm Troubleshooting" chapter of the *Cisco ONS 15454 Troubleshooting Guide* or the *Cisco ONS 15454SDH Troubleshooting Guide*.

**Step 6** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.195 SYNCTHIRD

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Objects: EXT-SREF, NE-SREF

A Loss of Timing on Third Reference alarm occurs when the ONS system loses the third timing source (reference 3). If SYNCTHIRD occurs and the ONS system uses an internal reference for source three, the TCC2/TCC2P could have failed. The ONS system often reports either the "FRNGSYNC" condition on page 2-44 or the "HLDOVRSYNC" condition on page 2-54 after a SYNCTHIRD alarm.

### Clear the SYNCTHIRD Alarm

**Step 1** In node view, click the **Provisioning > Timing > General** tabs.

**Step 2** Verify that the current configuration of REF-3 for the NE Reference. For more information about references, refer to the "Timing" chapter in the *Cisco ONS 15454 DWDM Reference Manual*.

**Step 3** If the third timing source is a BITS input, complete the "Clear the LOS (BITS) Alarm" procedure on page 2-70.

**Step 4** If the third timing source is an incoming port on the ONS system, complete the "Clear the LOS (OCN/STMN) Alarm" procedure located in the "Alarm Troubleshooting" chapter of the *Cisco ONS 15454 Troubleshooting Guide* or the *Cisco ONS 15454SDH Troubleshooting Guide*.

**Caution** Always use the supplied electrostatic discharge wristband when working with a powered ONS system. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

**Step 5** If the third timing source uses the internal ONS system timing, complete the "Reset an Active TCC2/TCC2P Card and Activate the Standby Card" procedure on page 2-152.

Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card.

**Step 6** If the reset card has not rebooted successfully, or the alarm has not cleared, call Cisco TAC (1 800 553-2447). If the Cisco TAC technician tells you to reseat the card, complete the "Remove and Reinsert (Reseat) the Standby TCC2/TCC2P Card" procedure on page 2-153. If the Cisco TAC technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Card" procedure on page 2-154.

## 2.7.196 SYSBOOT

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: NE

The System Reboot alarm indicates that new software is booting on the TCC2/TCC2P. No action is required. The alarm clears when all cards finish rebooting the new software. The reboot takes up to 30 minutes.

If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

**Note** SYSBOOT is an informational alarm. It only requires troubleshooting if it does not clear.

# 2.7.197 TEMP-MISM

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: NE

Temperature Reading Mismatch Between Control Cards is raised when the temperature readings on the two TCC2/TCC2Ps are out of range of each other by more than some predefined difference (such as 5 degrees C). A message containing power monitoring and temperature information is exchanged between the two TCC2/TCC2Ps, allowing the values to be compared. The temperature of each TCC2/TCC2P is read from a system variable.

This condition can be caused by a clogged fan filter or by fan tray stoppage.

## Clear the TEMP-MISM Condition

**Step 1** Complete the "Inspect, Clean, and Replace the Reusable Air Filter" procedure on page 2-156.

**Step 2** If the condition does not clear, complete the "Remove and Reinsert a Fan-Tray Assembly" procedure on page 2-158.

**Step 3** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

# 2.7.198 TIM

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: TRUNK

The Section TIM alarm occurs when the expected J0 section trace string does not match the received section trace string. This occurs because the data being received is not correct, and the receiving port could not be connected to the correct transmitter port.

If the alarm occurs on a port that has been operating with no alarms, the circuit path has changed due to a fibering misconnection, a TL1 routing change, or to someone entering an incorrect value in the Current Transmit String field.

TIM occurs on a port that has previously been operating without alarms if someone switches optical fibers that connect the ports. TIM is usually accompanied by other alarms, such as the LOS (OCN/STMN) or UNEQ-P (or HP-UNEQ) alarms. (For instructions to clear these alarms, refer to the "Alarm Troubleshooting" chapter of the *Cisco ONS 15454 Troubleshooting Guide* and the

*Cisco ONS 15454SDH Troubleshooting Guide*.) If these alarms accompany a TIM alarm, reattach or replace the original cables/fibers to clear the alarms. If a Transmit or Expected String was changed, restore the original string.

### Clear the TIM Alarm

**Step 1** Ensure that the physical fibers are correctly configured and attached. To do this, consult site documents. For more information about cabling an ONS system DWDM node, refer to the "Turn Up a Node" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Step 2** If the alarm does not clear, you can compare the J0 expected and transmitted strings and, if necessary, change them:

- **a.** Log into the circuit source node and click the **Circuits** tab.
- **b.** Select the circuit reporting the condition, then click **Edit**.
- **c.** In the Edit Circuit window, check the **Show Detailed Circuit Map** check box and click **Apply**.
- **d.** On the detailed circuit map, right-click the source circuit port and choose **Edit J0 Path Trace (port)** from the shortcut menu.
- **e.** Compare the Current Transmit String and the Current Expected String entries in the Edit J0 Path Trace dialog box.
- **f.** If the strings differ, correct the Transmit or Expected strings and click **Apply**.
- **g.** Click **Close**.

**Step 3** If the alarm does not clear, ensure that the signal has not been incorrectly routed. (Although the ONS system routes circuits automatically, the circuit route could have been changed using TL1.) If necessary, manually correct the routing using TL1. For instructions, refer to the *Cisco ONS SONET TL1 Reference Guide* and the *Cisco SONET TL1 Command Guide* .

**Step 4** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem if necessary.

## 2.7.199 TIM-MON

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: TRUNK

The TIM Section Monitor TIM alarm is similar to the "TIM" alarm on page 2-140, but it applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G cards when they are configured in transparent mode. (In transparent termination mode, all SONET overhead bytes are passed through from client ports to the trunk ports or from trunk ports to client ports.)

**Note** For general information about MXP and TXP cards, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For information about provisioning them, refer to the "Provision Transponder and Muxponder Cards" chapter.

### Clear the TIM-MON Alarm

**Step 1** Complete the "Clear the TIM Alarm" procedure on page 2-141.

**Step 2** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.200 UNC-WORD

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: TRUNK

The Uncorrected FEC Word condition indicates that the FEC capability could not sufficiently correct the frame.

**Note** For general information about MXP and TXP cards, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For information about provisioning them, refer to the "Provision Transponder and Muxponder Cards" chapter.

### Clear the UNC-WORD Condition

**Step 1** Ensure that the fiber connector for the card is completely plugged in. For more information about fiber connections and card insertion, refer to the "Turn Up a Node" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Step 2** Ensure that the ports on the far end and near end nodes have the same port rates and FEC settings. For more information about port rates and FEC settings, refer to the "Provision Transponder and Muxponder Cards" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Step 3** If the BER threshold is correct and at the expected level, use an optical test set to measure the power level of the line to ensure it is within guidelines. For specific procedures to use the test set equipment, consult the manufacturer.

**Step 4** If the optical power level is good, verify that optical receive levels are within the acceptable range.

**Step 5** If receive levels are good, clean the fibers at both ends according to site practice. If no site practice exists, complete the procedure in the "Maintain the Node" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Step 6** If the condition does not clear, verify that single-mode fiber is used.

**Step 7** If the fiber is of the correct type, verify that a single-mode laser is used at the far-end node.

**Step 8** Clean the fiber connectors at both ends for a signal degrade according to site practice.

**Step 9** Verify that a single-mode laser is used at the far end.

**Step 10** If the problem does not clear, the transmitter at the other end of the optical line could be failing and require replacement. Refer to the "2.9.3 Physical Card Reseating, Resetting, and Replacement" section on page 2-153.

**Step 11** If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.201 UNREACHABLE-TARGET-POWER

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: OCH

The Unreachable Port Target Power alarm occurs on WSS32 cards during startup as the card laser attains its correct power level. The condition disappears when the card successfully boots.

**Note** Card power levels are listed in the "Hardware Specifications" appendix of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Note** UNREACHABLE-TARGET-POWER is an informational condition. It only requires troubleshooting if it does not clear.

## 2.7.202 UT-COMM-FAIL

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: TRUNK

The Universal Transponder (UT) Module Communication Failure alarm is raised on MXP_2.5G_10E and TXP_MR_10E cards when there is a universal transponder communication failure because the universal transponder (UT) has stopped responding to the TCC2/TCC2P.

### Clear the UT-COMM-FAIL Alarm

**Step 1** Double-click the card to open the card view.

**Step 2** Request a laser restart:

a. Click the **Maintenance > ALS** tabs.

b. Check the **Request Laser Restart** check box.

c. Click **Apply**.

**Step 3** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

## 2.7.203 UT-FAIL

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: TRUNK

The Universal Transponder Module Hardware Failure alarm is raised against MXP_2.5G_10E and TXP_MR_10E cards when a UT-COMM-FAIL alarm persists despite being reset.

### Clear the UT-FAIL Alarm

**Step 1** Complete the "Physically Replace a Card" procedure on page 2-154 for the alarmed card.

**Step 2** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

## 2.7.204 VOA-HDEG

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Objects: AOTS, OCH, OMS, OTS

The VOA High Degrade alarm is raised on DWDM cards when an equipped VOA exceeds the setpoint due to an internal problem. The alarm indicates that the attenuation has crossed the high degrade threshold. The alarmed card should be replaced at the next opportunity.

**Note** For more information about provisioning VOA setpoints, refer to the "Network Reference" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For general information about DWDM cards, refer to the "Card Reference" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

### Clear the VOA-HDEG Alarm

**Step 1** Complete the "Physically Replace a Card" procedure on page 2-154 for the alarmed card.

**Step 2** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.205 VOA-HFAIL

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Objects: AOTS, OCH, OMS, OTS

The VOA High Fail alarm is raised on DWDM cards when an equipped VOA exceeds the setpoint due to an internal problem. The alarm indicates that the attenuation has crossed the high fail threshold. The card must be replaced.

**Note** For more information about provisioning VOA setpoints, refer to the "Network Reference" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For general information about DWDM cards, refer to the "Card Reference" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

### Clear the VOA-HFAIL Alarm

**Step 1** Complete the "Physically Replace a Card" procedure on page 2-154 for the alarmed card.

**Step 2** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

## 2.7.206 VOA-LDEG

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Objects: AOTS, OCH, OMS, OTS

The VOA Low Degrade alarm is raised on DWDM cards when an equipped VOA does not reach the setpoint due to an internal problem. The alarm indicates that the attenuation has crossed the low degrade threshold. The alarmed card should be replaced at the next opportunity.

**Note** For more information about provisioning VOA setpoints, refer to the "Network Reference" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For general information about DWDM cards, refer to the "Card Reference" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

### Clear the VOA-LDEG Alarm

**Step 1** Complete the "Physically Replace a Card" procedure on page 2-154 for the alarmed card.

**Step 2** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.207 VOA-LFAIL

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Objects: AOTS, OCH, OMS, OTS

The VOA Low Fail alarm is raised on DWDM cards when an equipped VOA does not reach the setpoint due to an internal problem. The alarm indicates that the attenuation has crossed the low fail threshold. The card must be replaced.

**Note** For more information about provisioning VOA setpoints, refer to the "Network Reference" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For general information about DWDM cards, refer to the "Card Reference" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

### Clear the VOA-LFAIL Alarm

**Step 1** Complete the "Physically Replace a Card" procedure on page 2-154 for the alarmed card.

**Step 2** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

## 2.7.208 VOLT-MISM

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: PWR

The Power Monitoring Mismatch Between Control Cards alarm is raised against the shelf when the power voltages of both TCC2/TCC2Ps are out of range of each other by more than 5 VDC.

### Clear the VOLT-MISM Condition

**Step 1** Check the incoming voltage level to the shelf using a voltmeter. Follow site practices or refer to the "Install the Shelf and Common Control Cards" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide* for power installation procedures.

**Step 2** Correct any incoming voltage issues.

**Step 3** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

## 2.7.209 WKSWPR (2R, EQPT, ESCON, FC, GE, ISC)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Objects: 2R, EQPT, ESCON, FC, GE, ISC

This condition is raised when you use the FORCE SPAN, FORCE RING, or MANUAL SPAN command at for a Y-Cable-protected MXP or TXP client port (set for one the above-listed client configurations). WKSWPR is visible on the network view Alarms, Conditions, and History tabs.

**Note** For more information about protection schemes, refer to the "Manage the Node" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

## 2.7.210 WKSWPR (TRUNK)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: TRUNK

This condition is raised when you use the FORCE SPAN, FORCE RING, or MANUAL SPAN command at for a splitter-protection enabled MXP or TXP trunk port. WKSWPR is visible on the network view Alarms, Conditions, and History tabs.

**Note** For more information about protection schemes, refer to the "Manage the Node" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

## 2.7.211 WTR (2R, EQPT, ESCON, FC, GE, ISC)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Objects: 2R, EQPT, ESCON, FC, GE, ISC

The Wait To Restore condition occurs for client ports in the above-listed types of configuration in a Y-cable protection group when the "WKSWPR (TRUNK)" condition, page 2-146, is raised. The condition occurs when the wait-to-restore time has not expired, meaning that the active protect path cannot revert to the working path. The condition clears when the timer expires and traffic switches back to the working path.

**Note** WTR is an informational condition and does not require troubleshooting.

## 2.7.212 WTR (TRUNK)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: TRUNK

The Wait To Restore condition occurs when the "WKSWPR (TRUNK)" condition, page 2-146, is raised for MXP or TXP splitter protection scheme ports. The condition occurs when the wait-to-restore time has not expired, meaning that the active protect path cannot revert to the working path. The condition clears when the timer expires and traffic switches back to the working path.

**Note** WTR is an informational condition and does not require troubleshooting.

## 2.7.213 WVL-MISMATCH

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: TRUNK

The Equipment Wavelength Mismatch alarm applies to the TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G cards. It occurs when you provision the card in CTC with a wavelength that the card does not support.

**Note** For more information about supported card wavelengths, refer to the "Hardware Specifications" appendix in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

### Clear the WVL-MISMATCH alarm

**Step 1** In node view, double-click the TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G card to open the card view.

**Step 2** Click the **Provisioning > Card** tabs.

**Step 3** In the Wavelength field, view the provisioned card wavelength.

**Step 4** If you have access to the site, compare the wavelength listed on the card faceplate with the provisioned wavelength. If you are remote, compare this wavelength with the card identification in the inventory:

a. In node view, click the **Inventory** tab.

b. Locate the slot where the TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G card is installed and view the card wavelength in the name.

**Step 5** If the card was provisioned for the wrong wavelength, double-click the card in node view to open the card view.

**Step 6** Click the **Provisioning > Card** tabs.

**Step 7** In the Wavelength field, click the drop-down list and choose the correct wavelength.

**Step 8** Click **Apply**.

**Step 9** If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

# 2.8 DWDM Card LED Activity

The following sections list the DWDM card LED sequences during card insertion and reset.

## 2.8.1 DWDM Card LED Activity After Insertion

When an DWDM card is inserted in the shelf, the following LED activities occur:

1. The FAIL LED illuminates for approximately 35 seconds.
2. The FAIL LED blinks for approximately 40 seconds.
3. All LEDs illuminate and then turn off within 5 seconds.
4. If new software is being downloaded to the card, the ACT and SF LEDs blink for 20 seconds to 3.5 minutes, depending on the card type.
5. The ACT LED illuminates.
6. The SF LED stays illuminated until all card ports connect to their far-end counterparts and a signal is present.

## 2.8.2 DWDM Card LED Activity During Reset

When an DWDM card resets (by software or hardware), the following LED activities occur:

1. The FAIL LED switches on for few seconds.

2. The FAIL LED on the physical card blinks and turns off.
3. The white LED with the letters "LDG" appears on the reset card in CTC.
4. The green ACT LED appears in CTC.

# 2.9 Frequently Used Alarm Troubleshooting Procedures

This section gives common procedures that are frequently used when troubleshooting alarms. Most of these procedures are summarized versions of fuller procedures existing elsewhere in the ONS system documentation. They are included in this chapter for the user's convenience. For further information, please refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

## 2.9.1 Protection Switching, Lock Initiation, and Clearing

The following sections give instructions for port switching and switch-clearing commands.

### Initiate a 1+1 Protection Port Force Switch Command

This procedure switches 1+1 protection group traffic from one port in the group to the other using a Force switch.

**Caution** The Force command overrides normal protective switching mechanisms. Applying this command incorrectly can cause traffic outages.

**Caution** Traffic is not protected during a Force protection switch.

**Note** A Force command switches traffic on a working path even if the path has signal degrade (SD) or signal fail (SF) conditions. A Force switch does not switch traffic on a protect path. A Force switch preempts a Manual switch.

**Step 1** In node view, click the **Maintenance > Protection** tabs.

**Step 2** In the Protection Groups area, select the protection group with the port you want to switch.

**Step 3** In the Selected Groups area, select the port belonging to the card you are replacing. You can carry out this command for the working or protect port. For example, if you need to replace the card with the Protect/Standby port, click this port.

**Step 4** In the Switch Commands area, click **Force**.

**Step 5** Click **Yes** in the Confirm Force Operation dialog box.

**Step 6** If the switch is successful, the group says "Force to working" in the Selected Groups area.

## Initiate a 1+1 Manual Switch Command

This procedure switches 1+1 protection group traffic from one port in the group to the other using a Manual switch.

**Note** A Manual command switches traffic if the path has an error rate less than the signal degrade. A Manual switch is preempted by a Force switch.

**Step 1** In node view, click the **Maintenance > Protection** tabs.

**Step 2** In the Protection Groups area, select the protection group with the port you want to switch.

**Step 3** In the Selected Groups area, select the port belonging to the card you are replacing. You can carry out this command for the working or protect port. For example, if you need to replace the card with the protect/standby port, click this port.

**Step 4** In the Switch Commands area, click **Manual**.

**Step 5** Click **Yes** in the Confirm Force Operation dialog box.

**Step 6** If the switch is successful, the group now says "Manual to working" in the Selected Groups area.

## Clear a 1+1 Force or Manual Switch Command

**Note** If the 1+1 protection group is configured as revertive, clearing a Force switch to protect (or working) moves traffic back to the working port. In revertive operation, the traffic always switches back to working. There is no revert to the protect. If ports are not configured as revertive, clearing a Force switch to protect does not move traffic back.

**Note** If the Force Switch was user-initiated, the reversion occurs immediately when the clear command is issued. The five-minute WTR period is not needed in this case. If the Force was system-initiated, allow the five-minute waiting period (during WTR) before the reversion occurs.

**Step 1** In node view, click the **Maintenance > Protection** tabs.

**Step 2** In the Protection Groups area, choose the protection group containing the port you want to clear.

**Step 3** In the Selected Group area, choose the port you want to clear.

**Step 4** In the Switching Commands area, click **Clear**.

**Step 5** Click **Yes** in the Confirmation Dialog box.

The Force switch is cleared. Traffic immediately reverts to the working port if the group was configured for revertive switching.

## Initiate a Lock-On Command

**Note** For 1:1 and 1:N electrical protection groups, working or protect cards can be placed in the Lock On state. For a 1+1 optical protection group, only the working port can be placed in the Lock On state.

**Step 1** In node view, click the **Maintenance > Protection** tabs.

**Step 2** In the Protection Groups list, click the protection group where you want to apply a lock-on.

**Step 3** If you determine that the protect card is in standby mode and you want to apply the lock-on to the protect card, make the protect card active if necessary:

a. In the Selected Group list, click the protect card.

b. In the Switch Commands area, click **Force**.

**Step 4** In the Selected Group list, click the active card where you want to lock traffic.

**Step 5** In the Inhibit Switching area, click **Lock On**.

**Step 6** Click **Yes** in the confirmation dialog box.

## Initiate a Card or Port Lockout Command

**Note** For 1:1 or 1:N electrical protection groups, working or protect cards can be placed in the Lock Out state. For a 1+1 optical protection group, only the protect port can be placed in the Lock Out state.

**Step 1** In node view, click the **Maintenance > Protection** tabs.

**Step 2** In the Protection Groups list, click the protection group that contains the card you want to lockout.

**Step 3** In the Selected Group list, click the card where you want to lock out traffic.

**Step 4** In the Inhibit Switching area, click **Lock Out**.

**Step 5** Click **Yes** in the confirmation dialog box.

The lockout has been applied and traffic is switched to the opposite card.

## Clear a Lock-On or Lockout Command

**Step 1** In node view, click the **Maintenance > Protection** tabs.

**Step 2** In the Protection Groups list, click the protection group that contains the card you want to clear.

**Step 3** In the Selected Group list, click the card you want to clear.

**Step 4** In the Inhibit Switching area, click **Unlock**.

**Step 5** Click **Yes** in the confirmation dialog box.

The lock-on or lockout is cleared.

## 2.9.2 CTC Card Resetting and Switching

This section gives instructions for resetting traffic cards and TCC2/TCC2Ps.

**Caution** For TXP and MXP cards placed in a Y-cable protection group, do not perform a software reset on both cards simultaneously. Doing so will cause a traffic hit of more than one minute. For more information about Y-cable protection groups, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Caution** Resetting the active card in a Y-cable group will cause a traffic outage if the standby card is down for any reason.

**Note** When an AIC-I card is rest in CTC, any subsequent user client operations (such as CTC or TL1 activity) is paused for approximately 5-10 seconds. The reset does not cause any conditions to be raised.

**Note** For more information about MXP and TXP cards, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

### Reset a Card in CTC

**Step 1** Log into a node on the network. If you are already logged in, continue with Step 2.

**Step 2** In node view, position the cursor over the optical or electrical traffic card slot reporting the alarm.

**Step 3** Right-click the card. Choose **Reset Card** from the shortcut menu.

**Step 4** Click **Yes** in the Resetting Card dialog box.

### Reset an Active TCC2/TCC2P Card and Activate the Standby Card

**Caution** Resetting an active TCC2/TCC2P can be service-affecting.

**Note** Before you reset the TCC2/TCC2P, you should wait at least 60 seconds after the last provisioning change you made to avoid losing any changes to the database.

**Step 1** Log into a node on the network. If you are already logged in, continue with Step 2.

**Step 2** Identify the active TCC2/TCC2P:

If you are looking at the physical ONS system shelf, the ACT/SBY LED of the active card is green. The ACT/STBLY LED of the standby card is amber.

**Step 3** Right-click the active TCC2/TCC2P in CTC.

**Step 4** Choose **Reset Card** from the shortcut menu.

**Step 5** Click **Yes** in the Confirmation Dialog box.

The card resets, the FAIL LED blinks on the physical card, and connection to the node is lost. CTC switches to network view.

**Step 6** Verify that the reset is complete and error-free and that no new related alarms appear in CTC.

**Step 7** Double-click the node and ensure that the reset TCC2/TCC2P is in standby mode and that the other TCC2/TCC2P is active. Verify the following:

- If you are looking at the physical ONS system shelf, the ACT/SBY LED of the active card is green. The ACT/STBLY LED of the standby card is amber.
- No new alarms appear in the Alarms window in CTC.

## 2.9.3 Physical Card Reseating, Resetting, and Replacement

This section gives instructions for physically reseating and replacing TCC2/TCC2Ps and traffic cards.

**Caution** Do not physically replace a card without first making provisions to switch or move traffic to a different card or circuit. General procedures for this are located in the "2.9.1 Protection Switching, Lock Initiation, and Clearing" section on page 2-149. In-depth traffic switching procedures and information can be found in the "Maintain the Node" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

### Remove and Reinsert (Reseat) the Standby TCC2/TCC2P Card

**Caution** Always use the supplied electrostatic discharge wristband when working with a powered ONS system. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

**Caution** Do not perform this action without the supervision and direction of Cisco TAC (1 800 553-2447).

**Caution** The TCC2/TCC2P reseat could be service-affecting. Refer to the "2.9.1 Protection Switching, Lock Initiation, and Clearing" section on page 2-149 for traffic-switching procedures.

**Note** Before you reset the TCC2/TCC2P, you should wait at least 60 seconds after the last provisioning change you made to avoid losing any changes to the database.

**Note** When a standby TCC2/TCC2P card is removed and reinserted (reseated), all three fan lights could momentarily turn on, indicating that the fans have also reset.

**Step 1** Log into a node on the network.

Ensure that the TCC2/TCC2P you want to reseat is in standby mode. A standby card has an amber ACT/SBY (Active/Standby) LED illuminated.

**Step 2** When the TCC2/TCC2P is in standby mode, unlatch both the top and bottom ejectors on the TCC2/TCC2P.

**Step 3** Physically pull the card at least partly out of the slot until the lighted LEDs turn off.

**Step 4** Wait 30 seconds. Reinsert the card and close the ejectors.

**Note** The TCC2/TCC2P requires several minutes to reboot and display the amber standby LED after rebooting. Refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide* for more information about LED behavior during a card reboot.

## Remove and Reinsert (Reseat) Any Card

**Caution** Always use the supplied electrostatic discharge wristband when working with a powered ONS system. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

**Step 1** Open the card ejectors.

**Step 2** Slide the card halfway out of the slot along the guide rails.

**Step 3** Slide the card all the way back into the slot along the guide rails.

**Step 4** Close the ejectors.

## Physically Replace a Card

**Caution** Always use the supplied electrostatic discharge wristband when working with a powered ONS system. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

**Caution** Removing an active card can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "2.9.1 Protection Switching, Lock Initiation, and Clearing" section on page 2-149 for commonly used traffic-switching procedures.

When you replace a card with the identical type of card, you do not need to make any changes to the database.

**Step 1** Open the card ejectors.

**Step 2** Slide the card out of the slot.

**Step 3** Open the ejectors on the replacement card.

**Step 4** Slide the replacement card into the slot along the guide rails.

**Step 5** Close the ejectors.

## 2.9.4 Generic Signal and Circuit Procedures

This section gives instructions for verify BER thresholds, deleting circuits, provisioning SDCC (or MS DCC) terminations, and clearing loopbacks.

### Verify the Signal BER Threshold Level

**Step 1** Log into a node on the network.

**Step 2** In node view, double-click the card reporting the alarm to open the card view.

**Step 3** Click the **Provisioning > Line** tabs.

**Step 4** Under the **SD BER** (or **SF BER**) column in the Provisioning window, verify that the cell entry is consistent with the originally provisioned threshold. The default setting is 1E-7.

**Step 5** If the entry is consistent with the original provisioning, go back to your original procedure.

**Step 6** If the entry is not consistent with what the system was originally provisioned for, click the cell to reveal the range of choices and click the original entry.

**Step 7** Click **Apply**.

### Delete a Circuit

**Step 1** Log into a node on the network.

**Step 2** In node view, click the **Circuits** tab.

**Step 3** Click the circuit row to highlight it and click **Delete**.

**Step 4** Click **Yes** in the Delete Circuits dialog box.

### Verify or Create Node Section DCC Terminations

**Note** Portions of this procedure are different for ONS system DWDM nodes.

**Step 1** Log into a node on the network.

**Step 2** In node view, click the **Provisioning > Comm Channels > SDCC (or Provisioning > Comm Channels > MS DCC**) tabs.

**Step 3** View the Port column entries to see where terminations are present for a node. If terminations are missing, proceed to Step 4.

**Step 4** If necessary, create a DCC termination:

a. Click **Create**.

b. In the Create SDCC Terminations (or Create MS-DCC Terminations) dialog box, click the ports where you want to create the DCC termination. To select more than one port, press the Shift key.

c. In the port state area, click the **Set to IS** , or **Unlocked** radio button.

d. Verify that the Disable OSPF on Link check box is unchecked.

e. Click **OK**.

### Clear an MXP or TXP Card Loopback Circuit

**Step 1** Log into a node on the network.

**Step 2** Double-click the reporting card in CTC to open the card view.

**Step 3** Click the **Maintenance > Loopback** tabs.

**Step 4** In the Loopback Type column, determine whether any port row shows a state other than None.

**Step 5** If a row contains another state besides None, click in the column cell to display the drop-down list and select None.

**Step 6** In the Admin State column, determine whether any port row shows an administrative state other than IS (or Unlocked), for example, OOS,MT (or Locked,maintenance).

**Step 7** If a row shows an administrative state other than IS, click in the column cell to display the drop-down list and select **IS** , or **Unlocked**.

**Step 8** Click **Apply**.

## 2.9.5 Air Filter and Fan Procedures

This section gives instructions for cleaning or replacing the air filter and reseating or replacing the fan tray assembly.

### Inspect, Clean, and Replace the Reusable Air Filter

To complete this task, you need a vacuum cleaner or detergent and water faucet, a spare filter, and a pinned hex key.

**Warning** **Do not reach into a vacuant slot or chassis while you install or remove a module or a fan. Exposed circuitry could constitute an energy hazard.** Statement 206

Although the filter works if it is installed with either side facing up, Cisco recommends that you install it with the metal bracing facing up to preserve the surface of the filter.

**Caution** Always use the supplied electrostatic discharge wristband when working with a powered ONS system. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

**Step 1** Verify that you are replacing a reusable air filter. The reusable filter is made of a gray, open-cell, polyurethane foam that is specially coated to provide fire and fungi resistance. NEBS 3E and later versions of the ONS system use a reusable air filter.

**Step 2** If the air filter is installed in the external filter brackets, slide the filter out of the brackets while being careful not to dislodge any dust that could have collected on the filter. If the filter is installed beneath the fan tray and not in the external filter brackets, open and remove the front door assembly by completing the following steps:

**a.** Open the front door of the shelf assembly by completing the following substeps.(If it is already open or if the shelf assembly does not have a front door, continue with Step 3.)

- Open the front door lock.
- Press the door button to release the latch.
- Swing the door open.

**b.** Remove the front door by completing the following substeps (optional):

- Detach the ground strap from either the door or the chassis by removing one of the Kepnuts.
- Place the Kepnut back on the stud after the ground strap is removed to avoid misplacement.
- Secure the dangling end of the ground strap to the door or chassis with tape.

**Step 3** Push the outer side of the handles on the fan-tray assembly to expose the handles.

**Step 4** Pull the handles and slide the fan-tray assembly one inch (25.4 mm) out of the shelf assembly and wait until the fans stop.

**Step 5** When the fans have stopped, pull the fan-tray assembly completely out of the shelf assembly.

**Step 6** Gently remove the air filter from the shelf assembly. Be careful not to dislodge any dust that could have collected on the filter.

**Step 7** Visually inspect the air filter material for dirt and dust.

**Step 8** If the reusable air filter has a concentration of dirt and dust, either vacuum or wash the air filter. Prior to washing the air filter, replace the dirty air filter with a clean air filter and also reinsert the fan-tray assembly. Wash the dirty air filter under a faucet with a light detergent.

Spare ONS system filters should be kept in stock for this purpose.

**Note** Cleaning should take place outside the operating environment to avoid releasing dirt and dust near the equipment.

**Step 9** If you washed the filter, allow it to completely air dry for at least eight hours.

**Caution** Do not put a damp filter back in the ONS system.

**Step 10** If the air filter should be installed in the external filter brackets, slide the air filter all the way to the back of the brackets to complete the procedure.

**Step 11** If the filter should be installed beneath the fan-tray assembly, remove the fan-tray assembly and slide the air filter into the recessed compartment at the bottom of the shelf assembly. Put the front edge of the air filter flush against the front edge of the recessed compartment. Push the fan tray back into the shelf assembly.

**Caution** If the fan tray does not slide all the way to the back of the shelf assembly, pull the fan tray out and readjust the position of the reusable filter until the fan tray fits correctly.

**Note** On a powered-up ONS system, the fans start immediately after the fan-tray assembly is correctly inserted.

**Step 12** To verify that the tray is plugged into the backplane, ensure that the LCD on the front of the fan-tray assembly is activated and displays node information.

**Step 13** Rotate the retractable handles back into their compartments.

**Step 14** Replace the door and reattach the ground strap.

## Remove and Reinsert a Fan-Tray Assembly

**Step 1** Use the retractable handles embedded in the front of the fan-tray assembly to pull it forward several inches.

**Step 2** Push the fan-tray assembly firmly back into the ONS system.

**Step 3** Close the retractable handles.

## Replace the Fan-Tray Assembly

**Caution** The 15454-FTA3 fan-tray assembly can only be installed in ONS 15454 R3.1 and later shelf assemblies (15454-SA-ANSI, P/N: 800-19857; 15454-SA-HD, P/N: 800-24848). It includes a pin that does not allow it to be installed in ONS 15454 shelf assemblies released before ONS 15454 R3.1 (15454-SA-NEBS3E, 15454-SA-NEBS3, and 15454-SA-R1, P/N: 800-07149). Equipment damage can result from attempting to install the 15454-FTA3 in a incompatible shelf assembly.

**Caution** Do not force a fan-tray assembly into place. Doing so can damage the connectors on the fan tray and/or the connectors on the backplane.

**Caution** Always use the supplied electrostatic discharge wristband when working with a powered ONS system. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

To replace the fan-tray assembly, it is not necessary to move any of the cable management facilities.

---

**Step 1** Open the front door of the shelf assembly by completing the following steps. If the shelf assembly does not have a front door, continue with Step 3.

**a.** Open the front door lock.

**b.** Press the door button to release the latch.

**c.** Swing the door open.

**Step 2** Remove the front door (optional):

**a.** Detach the ground strap from either the door or the chassis by removing one of the Kepnuts.

**b.** Place the Kepnut back on the stud after the ground strap is removed to avoid misplacement.

**c.** Secure the dangling end of the ground strap to the door or chassis with tape.

**Step 3** Push the outer side of the handles on the fan-tray assembly to expose the handles.

**Step 4** Fold out the retractable handles at the outside edges of the fan tray.

**Step 5** Pull the handles and slide the fan-tray assembly one inch (25.4 mm) out of the shelf assembly and wait until the fans stop.

**Step 6** When the fans have stopped, pull the fan-tray assembly completely out of the shelf assembly.

**Step 7** If you are replacing the fan-tray air filter and it is installed beneath the fan-tray assembly, slide the existing air filter out of the shelf assembly and replace it before replacing the fan-tray assembly.

If you are replacing the fan-tray air filter and it is installed in the external bottom bracket, you can slide the existing air filter out of the bracket and replace it at anytime. For more information on the fan-tray air filter, see the "Inspect, Clean, and Replace the Reusable Air Filter" section on page 2-156.

**Step 8** Slide the new fan tray into the shelf assembly until the electrical plug at the rear of the tray plugs into the corresponding receptacle on the backplane.

**Step 9** To verify that the tray has plugged into the backplane, check that the LCD on the front of the fan tray is activated.

**Step 10** If you replace the door, be sure to reattach the ground strap.

---

CHAPTER 3

# Transients Conditions

This chapter gives a description, entity, SNMP number, and trap for each commonly encountered Cisco ONS 15454 transient condition.

## 3.1 Transients Indexed By Alphabetical Entry

Table 3-1 alphabetically lists all ONS 15454 transient conditions and their entity, SNMP number, and SNMP trap.

**Note** The CTC default alarm profile might contain conditions that are not currently implemented but are reserved for future use.

*Table 3-1 ONS 15454 Transient Condition Alphabetical Index*

| Transient Condition | Entity | SNMP Number | SNMP Trap |
|---|---|---|---|
| 3.3.1 ADMIN-DISABLE, page 3-4 | NE | 5270 | disableInactiveUser |
| 3.3.2 ADMIN-DISABLE-CLR, page 3-4 | NE | 5280 | disableInactiveClear |
| 3.3.3 ADMIN-LOCKOUT, page 3-4 | NE | 5040 | adminLockoutOfUser |
| 3.3.4 ADMIN-LOCKOUT-CLR, page 3-4 | NE | 5050 | adminLockoutClear |
| 3.3.5 ADMIN-LOGOUT, page 3-4 | NE | 5020 | adminLogoutOfUser |
| 3.3.6 ADMIN-SUSPEND, page 3-4 | NE | 5340 | suspendUser |
| 3.3.7 ADMIN-SUSPEND-CLR, page 3-5 | NE | 5350 | suspendUserClear |
| 3.3.8 AUTOWDMANS, page 3-5 | NE | 5690 | automaticWdmAnsFinished |
| 3.3.9 BLSR-RESYNC, page 3-5 | OCN | 2100 | blsrMultiNodeTableUpdateCompleted |
| 3.3.10 DBBACKUP-FAIL, page 3-5 | EQPT | 3724 | databaseBackupFailed |
| 3.3.11 DBRESTORE-FAIL, page 3-5 | EQPT | 3726 | databaseRestoreFailed |
| 3.3.12 EXERCISING-RING, page 3-6 | OCN | 3400 | exercisingRingSuccessfully |
| 3.3.13 FIREWALL-DIS, page 3-6 | NE | 5230 | firewallHasBeenDisabled |

*Table 3-1 ONS 15454 Transient Condition Alphabetical Index (continued)*

| Transient Condition | Entity | SNMP Number | SNMP Trap |
|---|---|---|---|
| 3.3.14 FRCDWKSWBK-NO-TRFSW, page 3-6 | OCN | 5560 | forcedSwitchBackToWorkingResultedInNoTrafficSwitch |
| 3.3.15 FRCDWKSWPR-NO-TRFSW, page 3-6 | OCn | 5550 | forcedSwitchToProtectResultedInNoTrafficSwitch |
| 3.3.16 INTRUSION, page 3-6 | NE | 5250 | securityIntrusionDetUser |
| 3.3.17 INTRUSION-PSWD, page 3-6 | NE | 5240 | securityIntrusionDetPwd |
| 3.3.18 IOSCFG-COPY-FAIL, page 3-7 | — | 3660 | iosConfigCopyFailed |
| 3.3.19 LOGIN-FAILURE-LOCKOUT, page 3-7 | NE | 5080 | securityInvalidLoginLockedOutSeeAuditLog |
| 3.3.20 LOGIN-FAILURE-ONALRDY, page 3-7 | NE | 5090 | securityInvalidLoginAlreadyLoggedOnSeeAuditLog |
| 3.3.21 LOGIN-FAILURE-PSWD, page 3-7 | NE | 5070 | securityInvalidLoginPasswordSeeAuditLog |
| 3.3.22 LOGIN-FAILURE-USERID, page 3-7 | NE | 3722 | securityInvalidLoginUsernameSeeAuditLog |
| 3.3.23 LOGOUT-IDLE-USER, page 3-7 | — | 5110 | automaticLogoutOfIdleUser |
| 3.3.24 MANWKSWBK-NO-TRFSW, page 3-8 | OCN | 5540 | manualSwitchBackToWorkingResultedInNoTrafficSwitch |
| 3.3.25 MANWKSWPR-NO-TRFSW, page 3-8 | OCN | 5530 | manualSwitchToProtectResultedInNoTrafficSwitch |
| 3.3.26 PARAM-MISM, page 3-8 | OTS, OMS, OCH, AOTS | 5840 | pluginModuleRangeSettingsMismatch |
| 3.3.27 PM-TCA, page 3-8 | — | 2120 | performanceMonitorThresholdCrossingAlert |
| 3.3.28 PS, page 3-8 | EQPT | 2130 | protectionSwitch |
| 3.3.29 PSWD-CHG-REQUIRED, page 3-8 | NE | 6280 | userPasswordChangeRequired |
| 3.3.30 RMON-ALARM, page 3-8 | — | 2720 | rmonThresholdCrossingAlarm |
| 3.3.31 RMON-RESET, page 3-9 | — | 2710 | rmonHistoriesAndAlarmsResetReboot |
| 3.3.32 SESSION-TIME-LIMIT, page 3-9 | NE | 6270 | sessionTimeLimitExpired |
| 3.3.33 SFTWDOWN-FAIL, page 3-9 | EQPT | 3480 | softwareDownloadFailed |
| 3.3.34 SPANLENGTH-OUT-OF-RANGE, page 3-9 | OTS | 6150 | spanLengthOutOfRange |
| 3.3.35 SWFTDOWNFAIL, page 3-9 | EQPT | 3480 | softwareDownloadFailed |

*Table 3-1 ONS 15454 Transient Condition Alphabetical Index (continued)*

| Transient Condition | Entity | SNMP Number | SNMP Trap |
|---|---|---|---|
| 3.3.36 USER-LOCKOUT, page 3-9 | NE | 5030 | userLockedOut |
| 3.3.37 USER-LOGIN, page 3-10 | NE | 5100 | loginOfUser |
| 3.3.38 USER-LOGOUT, page 3-10 | NE | 5120 | logoutOfUser |
| 3.3.39 WKSWBK, page 3-10 | EQPT, OCN | 2640 | switchedBackToWorking |
| 3.3.40 WKSWPR, page 3-10 | 2R, TRUNK, EQPT, ESCON, FC, GE, ISC, OCN, STSMON, VT-MON | 2650 | switchedToProtection |
| 3.3.41 WRMRESTART, page 3-10 | NE | 2660 | warmRestart |
| 3.3.42 WTR-SPAN, page 3-10 | — | 3420 | spanIsInWaitToRestoreState |

# 3.2 Trouble Notifications

The ONS 15454 system reports trouble by using standard condition characteristics that follow the rules in Telcordia GR-253 and graphical user interface (GUI) state indicators.

The ONS 15454 uses standard Telcordia categories to characterize levels of trouble. The system reports trouble notifications as alarms and reports status or descriptive notifications (if configured to do so) as conditions in the CTC Alarms window. Alarms typically signify a problem that you need to remedy, such as a loss of signal. Conditions do not necessarily require troubleshooting.

## 3.2.1 Condition Characteristics

Conditions include any problem detected on an ONS 15454 shelf. They can include standing or transient notifications. You can retrieve a snapshot of all currently raised conditions on the network, node, or card in the CTC Conditions window or by using the RTRV-COND commands in TL1.

**Note** Some cleared conditions are found on the History tab.

For a comprehensive list of conditions, refer to the *Cisco ONS SONET TL1 Command Guide*.

## 3.2.2 Condition States

The History tab state (ST) column indicates the disposition of the condition, as follows:

- A raised (R) event is active.
- A cleared (C) event is no longer active.

- A transient (T) event is automatically raised and cleared in CTC during system changes such as user login, log out, and loss of connection to node view. Transient events do not require user action.

# 3.3 Transient Conditions

This section lists in alphabetical order all the transient conditions encountered in Software Release 6.0. The description, entity, SNMP number, and SNMP trap accompany each condition.

## 3.3.1 ADMIN-DISABLE

The ADMIN-DISABLE (Disable Inactive User) condition occurs when the administrator disables the user or the account is inactive for a specified period.

This transient condition does not result in a standing condition.

## 3.3.2 ADMIN-DISABLE-CLR

The ADMIN-DISABLE-CLR (Disable Inactive Clear) condition occurs when the administrator clears the disable flag on the user account.

This transient condition does not result in a standing condition.

## 3.3.3 ADMIN-LOCKOUT

The ADMIN-LOCKOUT (Admin Lockout of User) condition occurs when the administrator locks a user account.

This transient condition does not result in a standing condition.

## 3.3.4 ADMIN-LOCKOUT-CLR

The ADMIN-LOCKOUT-CLR (Admin Lockout Clear) condition occurs when the administrator unlocks a user account or the lockout time expires.

This transient condition does not result in a standing condition.

## 3.3.5 ADMIN-LOGOUT

The ADMIN-LOGOUT (Admin Logout of User) condition occurs when the administrator logs off a user session.

This transient condition does not result in a standing condition.

## 3.3.6 ADMIN-SUSPEND

The ADMIN-SUSPEND (Suspend User) condition occurs when the password for a user account expires.

This transient condition does not result in a standing condition.

## 3.3.7 ADMIN-SUSPEND-CLR

The ADMIN-SUSPEND-CLR (Suspend User Clear) condition occurs when the user or administrator changes the password.

This transient condition does not result in a standing condition.

## 3.3.8 AUTOWDMANS

The AUTOWDMANS (Automatic WDM ANS Finish) condition indicates that an automatic node setup command has been initiated. It normally occurs when you replace DWDM cards; the condition is an indication that the system has regulated the card.

This transient condition does not result in a standing condition.

## 3.3.9 BLSR-RESYNC

The BLSR-RESYNC (BLSR Multinode Table Update Completed) condition might occur when you create or delete circuits on a bidirectional line switched ring (BLSR), change a ring topology (for example, add or delete a BLSR node), or change the BLSR circuit state and ring ID.

This transient condition does not result in a standing condition.

## 3.3.10 DBBACKUP-FAIL

The DBBACKUP-FAIL (Database Backup Failed) condition occurs when the system fails to back up the database when the backup command is initiated.

This condition can occur when the server is not able to handle the backup operation due to network or server issues. Repeat the same operation again and check to see if it is successful. If the backup fails, it could be due to a network issue or software program failure. Contact TAC for assistance.

## 3.3.11 DBRESTORE-FAIL

The DBRESTORE-FAIL (Database Restore Failed) condition occurs when the system fails to restore the backed up database when the restore command is initiated.

This condition can be due to server issues, network issues, or human error (pointing to a file that does not exist, wrong file name, etc.). Retrying the database restore with the correct file will usually succeed. If the network issue persists, you must contact network lab support. If the condition is caused by a network element (NE) failure, contact TAC for assistance.

## 3.3.12 EXERCISING-RING

The EXERCISING-RING (Exercising Ring Successfully) condition occurs whenever you issue an Exercise-Ring command from CTC or TL1. This condition indicates that a command is being executed. You must issue another command to clear the exercise and the condition.

## 3.3.13 FIREWALL-DIS

The FIREWALL-DIS (Firewall Has Been Disabled) condition occurs when you provision the firewall to Disabled.

This transient condition does not result in a standing condition.

## 3.3.14 FRCDWKSWBK-NO-TRFSW

The FRCDWKSWBK-NO-TRFSW (Forced Switch Back to Working Resulted in No Traffic Switch) condition occurs when you perform a Force Switch to the working port/card and the working port/card is already active.

This transient condition might result in a Force Switch (Ring or Span) standing condition for a BLSR.

## 3.3.15 FRCDWKSWPR-NO-TRFSW

The FRCDWKSWPR-NO-TRFSW (Forced Switch to Protection Resulted in No Traffic Switch) condition occurs when you perform a Force Switch to the protect port/card, and the protect port/card is already active.

This transient condition does not result in a standing condition.

## 3.3.16 INTRUSION

The INTRUSION (Invalid Login Username) condition occurs when you attempt to log in with an invalid user ID.

This transient condition does not result in a standing condition.

## 3.3.17 INTRUSION-PSWD

The INTRUSION -PSWD (Security Intrusion Attempt Detected) condition occurs when you attempt to login with an invalid password.

This transient condition does not result in a standing condition.

## 3.3.18 IOSCFG-COPY-FAIL

The IOSCFG-COPY-FAIL (IOS Config Copy Failed) condition occurs on ML-Series Ethernet cards when the software fails to upload or download the Cisco IOS startup configuration file to or from an ML-Series card. This condition is similar to the "SFTWDOWN-FAIL" condition on page 3-9, but the IOSCFG-COPY-FAIL condition applies to ML-Series Ethernet cards rather than the TCC2/TCC2P card.

## 3.3.19 LOGIN-FAILURE-LOCKOUT

The LOGIN-FAILURE-LOCKOUT (Invalid Login–Locked Out) condition occurs when you attempt to log into a locked account.

This transient condition does not result in a standing condition.

## 3.3.20 LOGIN-FAILURE-ONALRDY

The LOGIN-FAILURE-ONALRDY (Security: Invalid Login–Already Logged On) condition occurs when you attempt to log in with an existing session and SUPN policy.

This transient condition does not result in a standing condition.

## 3.3.21 LOGIN-FAILURE-PSWD

The LOGIN-FAILURE-PSWD (Invalid Login–Password) condition occurs when you attempt to log in with an invalid password.

This transient condition does not result in a standing condition.

## 3.3.22 LOGIN-FAILURE-USERID

The LOGIN-FAILURE-USERID (Invalid Login–Username) condition occurs when a user login (CTC, CTM, or TL1) fails because the login username is not present on the node database. You must log in again with an existing user ID.

This transient condition is equivalent to a security warning. You must check the security log (audit log) for other security-related actions that have occurred.

## 3.3.23 LOGOUT-IDLE-USER

The LOGOUT-IDLE-USER (Automatic Logout of Idle User) condition occurs when a user session is idle for too long (the idle timeout expires) and the session terminates as a result. You must log in again to restart your session.

## 3.3.24 MANWKSWBK-NO-TRFSW

The MANWKSWBK-NO-TRFSW (Manual Switch Back To Working Resulted in No Traffic Switch) condition occurs when you perform a Manual switch to the working port/card and the working port/ card is already active.

This transient condition does not result in a standing condition.

## 3.3.25 MANWKSWPR-NO-TRFSW

The MANWKSWPR-NO-TRFSW (Manual Switch to Protect Resulted in No Traffic Switch) condition occurs when you perform a Manual switch to the protect port/card and the protect port/card is already active.

This transient condition results in a BLSR Manual Switch (Span or Ring) standing condition.

## 3.3.26 PARAM-MISM

The PARAM-MISM (Plug-in Module Range Settings Mismatch) condition occurs when the parameter range values stored on a small-form factor pluggable (SFP) device are different from the parameters stored in the TCC2/TCC2P database.

The transient condition is not user-serviceable.

## 3.3.27 PM-TCA

The PM-TCA (Performance Monitor Threshold Crossing Alert) condition occurs when network collisions cross the rising threshold for the first time.

## 3.3.28 PS

The PS (Protection Switch) condition occurs when the traffic switches from a working/active card to a protect/standby card.

## 3.3.29 PSWD-CHG-REQUIRED

The PSWD-CHG-REQUIRED (User Password Change Required) condition occurs when you are denied login for a shell function such as telnet or FTP because you did not change the login password. You can change the password through CTC or TL1.

## 3.3.30 RMON-ALARM

The RMON-ALARM (RMON Threshold Crossing Alarm) condition occurs when the remote monitoring variable crosses the threshold.

## 3.3.31 RMON-RESET

The RMON-RESET (RMON Histories and Alarms Reset Reboot) condition occurs when the time-of-day settings on the TCC2/TCC2P card are increased or decreased by more than five seconds. This invalidates all the history data and remote monitoring (RMON) must restart. It can also occur when you reset a card.

## 3.3.32 SESSION-TIME-LIMIT

The SESSION-TIME-LIMIT (Session Time Limit Expired) condition occurs when a login session exceeds the time limit and you are logged out of the session. You must login again.

## 3.3.33 SFTWDOWN-FAIL

The SFTDOWN-FAIL (Software Download Failed) condition occurs when the system fails to download the required software.

An incorrect input that points to the wrong place or file, network issues, or a bad (corrupt) package can cause this failure. Retrying the operation with the correct name/location will usually succeed. If network issues persist, you must contact the network lab support. If the package is corrupt, contact Cisco TAC.

## 3.3.34 SPANLENGTH-OUT-OF-RANGE

The SPANLENGTH-OUT-OF-RANGE (Span Length Out of Range) condition occurs when the measured span loss does not fall within the limits of minimum and maximum expected span loss. It can also occur when the difference between MaxExpSpanLoss and MinExpSpanLoss is greater than 1dB.

When you perform a Calculate Span Loss operation on a DWDM node, the software measures the real span loss in the field by comparing the far-end POSC power and the near-end OSC power.

## 3.3.35 SWFTDOWNFAIL

The SFTDOWN-FAIL (Software Download Failed) condition occurs when the system fails to download the required software.

An incorrect input that points to the wrong place or file, network issues, or a bad (corrupt) package can cause this failure. Retrying the operation with the correct name/location will usually succeed. If network issues persist, you must contact the network lab support. If the package is corrupt, contact Cisco TAC.

## 3.3.36 USER-LOCKOUT

The USER-LOCKOUT (User Locked Out) condition occurs when the system locks an account because of a failed login attempt. To proceed, the administrator must unlock the account or the lockout time must expire.

## 3.3.37 USER-LOGIN

The USER-LOGIN (Login of User) occurs when you begin a new session by verifying your User ID and password.

This transient condition does not result in a standing condition.

## 3.3.38 USER-LOGOUT

The USER-LOGOUT (Logout of User) condition occurs when you stop a login session by logging out of your account.

This transient condition does not result in a standing condition.

## 3.3.39 WKSWBK

The WKSWBK (Switched Back to Working) condition occurs when traffic switches back to the working port/card in a non-revertive protection group.

This transient condition does not result in a standing condition.

## 3.3.40 WKSWPR

The WKSWPR (Switched to Protection) condition occurs when traffic switches to the protect port/card in a non-revertive protection group.

This transient condition does not result in a standing condition.

## 3.3.41 WRMRESTART

The WRMRESTART (Warm Restart) condition occurs when the node restarts while powered up. A restart can be caused by provisioning, such as database-restore and IP changes, or software defects. A WRMRESTART is normally accompanied by MANRESET or AUTORESET to indicate whether the reset was initiated manually (MAN) or automatically (AUTO).

This is the first condition that appears after a TCC2/TCC2P card is powered up. The condition changes to COLD-START if the TCC2/TCC2P card is restarted from a physical reseat or a power loss.

## 3.3.42 WTR-SPAN

The WTR-SPAN (Span is in Wait To Restore State) condition occurs when a BLSR switches to another span due to a Signal Failure-Span command or a fiber is pulled from a four-fiber BLSR configuration. The condition is raised until the WaitToRestore (WTR) period expires.

This transient condition clears when the BLSR returns to a normal condition or the IDLE state.


# Error Messages

**Note** The terms "Unidirectional Path Switched Ring" and "UPSR" may appear in Cisco literature. These terms do not refer to using Cisco ONS 15xxx products in a unidirectional path switched ring configuration. Rather, these terms, as well as "Path Protected Mesh Network" and "PPMN," refer generally to Cisco's path protection feature, which may be used in any topological network configuration. Cisco does not recommend using its path protection feature in any particular topological network configuration.

This chapter lists the Cisco ONS 15454, 15454 SDH, 15600, 15327 and 15310-CL error messages. The error dialog box in Figure 4-1 consists of three parts: the error title, error ID, and error message. The table lists two types of messages: error messages (EID-*nnnn*) and warning messages (WID-*nnnn*). Error messages are alerts that an unexpected or undesirable operation has occurred which either indicates the risk of loss of traffic or an inability to properly manage devices in the network. Warnings are alerts that the requested operation could lead to an error. Warnings are sometimes used to convey important information.

***Figure 4-1 Error Dialog Box***

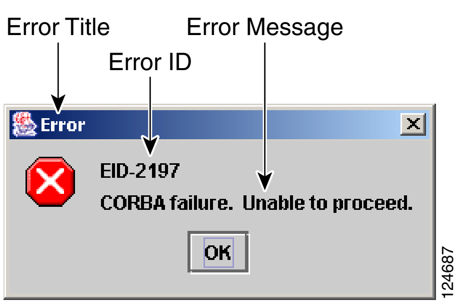



Table 4-1 gives a list of all error or warning message numbers, the messages, and a brief description of each message.

*Table 4-1 Error Messages*

| Error or Warning ID | Error or Warning Message | Description |
|---|---|---|
| EID-0 | Invalid error ID. | The error ID is invalid. |
| EID-1 | Null pointer encountered in {0}. | Cisco Transport Controller (CTC) encountered a null pointer in the area described by the specified item. |
| EID-1000 | The host name of the network element cannot be resolved to an address. | Refer to error or warning message text. |
| EID-1001 | Unable to launch CTC due to applet security restrictions. Please review the installation instructions to make sure that the CTC launcher is given the permissions it needs. Note that you must exit and restart your browser in order for the new permissions to take effect. | Refer to error or warning message text. |
| EID-1002 | The host name (e.g., for the network element) was successfully resolved to its address, but no route can be found through the network to reach the address. | The node is not reachable from CTC client station. |
| EID-1003 | An error was encountered while attempting to launch CTC. {0} | Unexpected exception or error while launching CTC from the applet. |
| EID-1004 | Problem Deleting CTC Cache: {0} {1} | Unable to delete the CTC cached JARs, because another application may have the JAR files running; for example, another instance of CTC. |
| EID-1005 | An error occurred while writing to the {0} file. | CTC encountered an error while writing to log files, preference files, etc. |
| EID-1006 | The URL used to download {0} is malformed. | The URL used to download the Launcher.jar file is malformed. |
| EID-1007 | An I/O error occurred while trying to download {0}. | An input or output exception was encountered when CTC tried to download the GUI launcher. |
| EID-1018 | Password must contain at least 1 alphabetic, 1 numeric, and 1 special character (+, # or %).<br>Password shall not contain the associated user-ID. | The password is invalid. |
| EID-1019 | Could not create {0}.<br>Please enter another filename. | CTC could not create the file due to an invalid filename. |
| EID-1020 | Fatal exception occurred, exiting CTC.<br>Unable to switch to the Network view. | CTC was unable to switch from the node or card view to the network view, and is now shutting down. |
| EID-1021 | Unable to navigate to {0}. | Failed to display the indicated view—node or network. |
| EID-1022 | A session cannot be opened right now with this slot. Most likely someone else (using a different CTC) already has a session opened with this slot.<br>Please try again later. | Refer to error message text. |

*Table 4-1 Error Messages (continued)*

| Error or Warning ID | Error or Warning Message | Description |
|---|---|---|
| EID-1023 | This session has been terminated. This can happen if the card resets, the session has timed out, or if someone else (possibly using a different CTC) already has a session open with this slot. | Refer to error message text. |
| EID-1025 | Unable to create Help Broker. | CTC was unable to create the help broker for the online help. |
| EID-1026 | Unable to locate HelpSet. | CTC was unable to locate the help set for the online help. |
| EID-1027 | Unable to locate Help ID: {0} | CTC was unable to locate the help ID for the online help. |
| EID-1028 | Error saving table. {0} | There was an error while saving the specified table. |
| EID-1031 | CTC cannot locate the online user manual files. The files may have been moved, deleted, or not installed. To install online user manuals, run the CTC installation wizard on the software or documentation CD. | Refer to error message text. |
| EID-1032 | CTC cannot locate Acrobat Reader. If Acrobat Reader is not installed, you can install the Reader using the CTC installation wizard provided on the software or documentation CD. | Refer to error message text. |
| EID-1034 | Unable to locate HelpSet when searching for Help ID "{0}". | CTC is unable to locate the specified help ID of the context sensitive help files. |
| EID-1035 | CTC experienced an I/O error while working with the log files. Usually this means that the computer has run out of disk space. This problem may or may not cause CTC to stop responding. Ending this CTC session is recommended, but not required. | Refer to error message text. |
| WID-1036 | WARNING: Deleting the CTC cache may cause any CTC running on this system to behave in an unexpected manner. | Refer to warning message text. |
| EID-1037 | Could not open {0}. Please enter another filename. | Invalid file name. CTC is unable to open the file. |
| EID-1038 | The file {0} does not exist. | The specified file does not exist. |
| EID-1039 | The version of the browser applet does not match the version required by the network element. Please close and restart your browser in order to launch the Cisco Transport Controller. | Refer to error message. |
| WID-1040 | WARNING: Running the CTC with a JRE version other than the recommended JRE version might cause the CTC to behave in an unexpected manner. | Refer to warning message. |
| EID-2001 | No rolls selected. {0} | No rolls were selected for the bridge and roll. |
| EID-2002 | The Roll must be completed or cancelled before it can be deleted. | You cannot delete the roll unless it has been completed or cancelled. |
| EID-2003 | Error deleting roll. | There was an error when CTC tried to delete the roll. |
| EID-2004 | No IOS slot selected. | You did not select a Cisco IOS slot. |

*Table 4-1 Error Messages (continued)*

| Error or Warning ID | Error or Warning Message | Description |
|---|---|---|
| EID-2005 | CTC cannot find the online help files for {0}. The files may have been moved, deleted, or not installed. To install online help, run the setup program on the software or documentation CDs. | CTC cannot find the online help files for the specified window. The files might have been moved, deleted, or not installed. To install online help, run the setup program on the software or documentation CDs. |
| EID-2006 | Error editing circuit(s). {0} {1}. | An error occurred when CTC tried to open the circuit for editing. |
| EID-2007 | Unable to save preferences. | CTC cannot save the preferences. |
| EID-2008 | Unable to store circuit preferences: {0} | CTC cannot find the file needed to save the circuit preferences. |
| EID-2009 | Unable to download package:<br>{0} | Refer to error message text. |
| EID-2010 | Delete destination failed. | CTC could not delete the destination. |
| EID-2011 | Circuit destroy failed. | CTC could not destroy the circuit. |
| EID-2012 | Reverse circuit destroy failed. | CTC could not reverse the circuit destroy. |
| EID-2013 | Circuit creation error. Circuit creation cannot proceed due to changes in the network which affected the circuit(s) being created. The dialog will close. Please try again. | Refer to error message text. |
| EID-2014 | No circuit(s) selected. {0} | You must select a circuit to complete this function. |
| EID-2015 | Unable to delete circuit {0}as it has one or more rolls. | You must delete the rolls in the circuit before deleting the circuit itself. |
| EID-2016 | Unable to delete circuit. | CTC could not delete the tunnel as there are circuits that use the tunnel. |
| EID-2017 | Error mapping circuit. {0} | There was an error mapping the circuit. |
| EID-2018 | Circuit roll failure. The circuit has to be in the DISCOVERED state in order to perform a roll. | There was a failure in circuit roll. Change the circuit state to DISCOVERED and proceed. |
| EID-2019 | Circuit roll failure. Bridge and roll is not supported on a DWDM circuit. | Refer to error message text. |
| EID-2020 | Circuit roll failure. The two circuits must have the same direction. | Refer to error message text. |
| EID-2021 | Circuit roll failure. The two circuits must have the same size. | Refer to error message text. |
| EID-2022 | Circuit roll failure. A maximum of two circuits can be selected for a bridge and roll operation. | Refer to error message text. |
| EID-2023 | Unable to create new user account. | Refer to error message text. |
| EID-2024 | Node selection error. | There was an error during node selection. |

*Table 4-1 Error Messages (continued)*

| Error or Warning ID | Error or Warning Message | Description |
|---|---|---|
| EID-2025 | This feature cannot be used. Verify that each of the endpoints of this circuit are running software that supports this feature. | Refer to error or warning message text. This error is generated from the AnsOpticsParamsPane to indicate that the selected ring type is not supported by the endpoints of the circuit. In the VLAN tab it indicates that the back-end spanning tree protocol (STP) disabling is not supported. |
| EID-2026 | Unable to apply {0} request. {1} | Error occurred while attempting to switch a path protection circuit away from a span. |
| EID-2027 | Error deleting circuit drop. | CTC could not delete the circuit drop. |
| EID-2028 | Error removing circuit node. | CTC could not remove the circuit node. |
| EID-2029 | The requested operation is not supported. | The task you are trying to complete is not supported by CTC. |
| EID-2030 | Provisioning error. | There was an error during provisioning. |
| EID-2031 | Error adding node. | There was an error while adding a node. |
| EID-2032 | Unable to rename circuit. {0} | CTC could not rename the circuit. |
| EID-2033 | An error occurred during validation. {0} | There was an internal error while validating the user changes after the Apply button was pressed. This error can occur in the Edit Circuit dialog box or in the BLSR table in the shelf view (rare condition). |
| EID-2034 | Unable to add network circuits:<br>{0} | Refer to error message text. |
| EID-2035 | The source and destination nodes are not connected. | Refer to error message text. |
| EID-2036 | Cannot delete this {0}.<br>LAN Access has been disabled on this node and this {0} is needed to access the node. | You cannot delete the DCC/GCC link as it is needed to access the node. |
| EID-2037 | Application error. Cannot find attribute for {0}. | CTC cannot find an attribute for the specified item. |
| EID-2038 | Invalid protection operation. | The protection operation you tried to execute is invalid. |
| EID-2040 | Please select a node first. | You must select a node before performing the task. |
| EID-2041 | No paths are available on this link. Please make another selection. | You must select a link that has paths available. |
| EID-2042 | This span is not selectable. Only the green spans with an arrow may be selected. | Refer to error message text. |
| EID-2043 | This node is not selectable. Only the source node and nodes attached to included spans (blue) are selectable. Selecting a selectable node will enable its available outgoing spans. | Refer to error message text. |

*Table 4-1 Error Messages (continued)*

| Error or Warning ID | Error or Warning Message | Description |
|---|---|---|
| EID-2044 | This link may not be included in the required list. Constraints only apply to the primary path. Each node may have a maximum of one incoming signal and one outgoing link. | You must select only one link going in and out of a node. Selecting more than one link is contradictory to the path selection algorithm. |
| EID-2045 | This link may not be included in the required list. Only one outgoing link may be included for each node. | Refer to error message text. |
| EID-2047 | Error validating slot number. Please enter a valid value for the slot number. | There was an error due to an invalid slot number. |
| EID-2048 | Error validating port number. Please enter a valid value for the port number. | There was an error due to an invalid port number. |
| EID-2050 | New circuit destroy failed. | CTC could not destroy the new circuit. |
| EID-2051 | Circuit cannot be downgraded. {0} | The specified circuit cannot be downgraded. |
| EID-2052 | Error during circuit processing. | There was an error during the circuit processing. |
| EID-2054 | Endpoint selection error. | There was an error during the endpoint selection. |
| EID-2055 | No endpoints are available for this selection. Please make another selection. | This error occurs in the circuit creation dialog only during a race condition that has incorrectly allowed entities without endpoints to be displayed in the combo boxes. |
| EID-2056 | Communication error. {0} | An internal error occurred in Network Alarm tab while synchronizing alarms with the nodes. |
| EID-2059 | Node deletion Error. {0} | There was an error during the node deletion. |
| EID-2060 | No PCA circuits found. | CTC could not find any protection channel access (PCA) circuits for this task. |
| EID-2061 | Error provisioning VLAN. | There was an error defining the VLAN. |
| EID-2062 | Cannot delete VLAN. No VLAN(s) are selected. Please select a VLAN. | Cannot delete VLAN. No VLAN(s) are selected. Please select a VLAN. |
| EID-2063 | Cannot delete default VLAN. | The selected VLAN is the default VLAN, and cannot be deleted. |
| EID-2064 | Error deleting VLANs.<br>{0} | There was an error deleting the specified VLAN. |
| EID-2065 | Cannot import profile. Profile "{0}" exists in the editor and the maximum number of copies (ten) exists in the editor. Aborting the import. The profile has already been loaded eleven times. | Cannot import the profile as the profile has reached the maximum number of copies in the editor. |
| EID-2066 | Unable to store profile. Error writing to {0}. | CTC encountered an error while trying to store the profile. |
| EID-2067 | File write error. {0} | CTC encountered an error while writing the specified file. |

*Table 4-1 Error Messages (continued)*

| Error or Warning ID | Error or Warning Message | Description |
|---|---|---|
| EID-2068 | Unable to load alarm profile from node. | CTC encountered an error trying to load the alarm profile from the node. |
| EID-2069 | File not found or I/O exception.<br>(No such file or directory) | Either the specified file was not found, or there was an input/output exception. |
| EID-2070 | Failure deleting profile. {0} | There was a failure in deleting the specified profile. |
| EID-2071 | Only one column may be highlighted. | You cannot select more than one column during clone action. |
| EID-2072 | Only one profile may be highlighted. | You cannot select more than one profile. |
| EID-2073 | This column is permanent and may not be removed. | You cannot delete a permanent column. |
| EID-2074 | Select one or more profiles. | You have not selected any profile or column. Reset operation is done by right-clicking the selected column. |
| EID-2075 | This column is permanent and may not be reset. | A permanent column is non resettable. |
| EID-2077 | This column is permanent and may not be renamed. | You cannot rename a permanent column. |
| EID-2078 | At least two columns must be highlighted. | You connot compare two profiles unless you select two columns. |
| EID-2079 | Cannot load alarmables into table. There are no reachable nodes from which the list of alarmables may be loaded. Please wait until such a node is reachable and try again. | Refer to error message text. |
| EID-2080 | Node {0} has no profiles. | The specified node does not have any profiles. |
| EID-2081 | Error removing profile {0} from node {1}. | There was an error while removing the specified profile from the specified node. |
| EID-2082 | Cannot find profile {0} on node {1}. | CTC cannot find the specified profile from the specified node. |
| EID-2083 | Error adding profile {0} to node {1}. | There was an error adding the specified profile to the specified node. |
| EID-2085 | Invalid profile selection. No profiles were selected. | You tried to select an invalid profile. Select another profile. |
| EID-2086 | Invalid node selection. No nodes were selected. | You tried to select an invalid node. Select another node. |
| EID-2087 | No profiles were selected. Please select at least one profile. | Refer to error message text. |
| EID-2088 | Invalid profile name. | The profile name cannot be empty. |
| EID-2089 | Too many copies of {0} exist. Please choose another name. | Select a unique name. |
| EID-2090 | No nodes selected. Please select the node(s) on which to store the profile(s). | You must select one or more nodes on which you can store the profile. |
| EID-2091 | Unable to switch to node {0}. | CTC is unable to switch to the specified node. |

*Table 4-1 Error Messages (continued)*

| Error or Warning ID | Error or Warning Message | Description |
|---|---|---|
| EID-2092 | General exception error. | CTC encountered a general exception error while trying to complete the task. |
| EID-2093 | Not enough characters in name. {0} | The name must have a minimum of six characters. |
| EID-2094 | Password and confirmed password fields do not match. | You must make sure the two fields have the same password. |
| EID-2095 | Illegal password.<br>{0} | The password you entered is not allowed. |
| EID-2096 | The user must have a security level. | You must have an assigned security level to perform this task. |
| EID-2097 | No user name specified. | You did not specify a user name. |
| EID-2099 | Ring switching error. | There was an error during the ring switch. |
| EID-2100 | Please select at least one profile to delete. | You have not selected the profile to delete. |
| EID-2101 | Protection switching error. | There was an error during the protection switching. |
| EID-2102 | The forced switch could not be removed for some circuits. You must switch these circuits manually. | The forced switch could not be removed for some circuits. You must switch these circuits manually. |
| EID-2103 | Error upgrading span. | There was an error during the span upgrade. |
| EID-2104 | Unable to switch circuits back as one or both nodes are not reachable. | This error occurs during the path protection span upgrade procedure. |
| EID-2106 | The node name cannot be empty. | You must supply a name for the node. |
| EID-2107 | Error adding {0}, unknown host. | There was an error adding the specified item. |
| EID-2108 | {0} is already in the network. | The specified item exists in the network. |
| EID-2109 | The node is already in the current login group. | The node you are trying to add is already present in the current login group. |
| EID-2110 | Please enter a number between 0 and {0}. | You must enter a number in the range between 0 and the specified value. |
| EID-2111 | This node ID is already in use. Please choose another. | Select a node ID that is not in use. |
| EID-2113 | Cannot set extension byte for ring.<br>{0} | CTC cannot set the extension byte. |
| EID-2114 | Card communication failure. Error applying operation. | This error can occur during an attempt to apply a BLSR protection operation to a line. |
| EID-2115 | Error applying operation.<br>{0} | There was an error in applying the specified operation. |
| EID-2116 | Invalid extension byte setting for ring.<br>{0} | The extension byte set for the specified ring is invalid. |
| EID-2118 | Cannot delete ring. There is a protection operation set. All protection operations must be clear for ring to be deleted. | Delete all the protection operations for the ring before it can be deleted. |

*Table 4-1 Error Messages (continued)*

| Error or Warning ID | Error or Warning Message | Description |
|---|---|---|
| EID-2119 | Cannot delete {0} because a protection switch is in effect. Please clear any protection operations, make sure that the reversion time is not "never" and allow any protection switches to clear before trying again. | Clear all protection operations or switches before deleting the ring. |
| EID-2120 | The following nodes could not be unprovisioned<br>{0}<br>Therefore you will need to delete this {1} again later. | The specified nodes could not be unprovisioned. Try deleting this BLSR or MS-SPRing later. |
| EID-2121 | Cannot upgrade ring.<br>{0} | CTC cannot upgrade the specified ring. |
| EID-2122 | Inadequate ring speed for upgrade. Only {0} (or higher) {1} can be upgraded to 4-fiber. | You have selected an incorrect ring speed for upgrade. Only rings within the specified parameters can be upgraded to 4-fiber BLSR. |
| EID-2123 | Verify that the following nodes have at least two in-service ports with the same speed as the 2-fiber {0}. The ports cannot serve as a timing reference, and they cannot have DCC terminations or overhead circuits. {1} | Nonupgradable nodes. Verify that the specified nodes have at least two IS-NR ports with the same speed as the 2-fiber BLSR.<br>The specified ports cannot serve as a timing reference, and they cannot have data communications channel (DCC) terminations or overhead circuits. |
| EID-2124 | You cannot add this span because it is connected to a node that already has the east and west ports defined. | Refer to error message text. |
| EID-2125 | You cannot add this span as it would cause a single card to host both the east span and the west span. A card cannot protect itself. | Refer to error message text. |
| EID-2126 | OSPF area error.<br>{0} | There is an Open Shortest Path First (OSPF) area error. |
| EID-2127 | You cannot add this span. It would cause the following circuit(s) to occupy different STS regions on different spans.<br>{0}<br>Either select a different span or delete the above circuit(s). | A circuit cannot occupy different STS regions on different spans. You may add a different span or delete the specified circuit. |
| EID-2128 | Illegal state error. | An internal error occurred while trying to remove a span from a BLSR.<br>This alarm occurs in the network-level BLSR creation dialog box. |
| EID-2129 | This port is already assigned. The east and west ports must be different. | Refer to error message text. |
| EID-2130 | The ring ID value, {0}, is not valid. Please enter a valid number between 0 and 9999. | Enter a ring ID value between 0 and 9999. |
| EID-2131 | Cannot set reversion to INCONSISTENT. | You must select another reversion type. |

*Table 4-1 Error Messages (continued)*

| Error or Warning ID | Error or Warning Message | Description |
|---|---|---|
| EID-2135 | Unable to store overhead circuit preferences: {0} | Input/Output error. Unable to store overhead circuit preferences. |
| EID-2137 | Circuit merge error. {0} | There was an error while merging the circuits. |
| EID-2138 | Cannot delete all destinations. Please try again. | Refer to error message text. |
| EID-2139 | Error updating destinations. | There was an error in updating the circuit destinations. |
| EID-2143 | No online help version selected. Cannot delete the online help book. | Select the version of online help, and proceed. |
| EID-2144 | Error deleting online help book(s). {0} | You cannot delete the specified online help. |
| EID-2145 | Unable to locate a node with an IOS card. | Refer to error message. |
| EID-2146 | Security violation. You may only logout your own account. | You cannot logout of an account other than your own. |
| EID-2147 | Security violation. You may only change your own account. | You cannot change an account other than your own. |
| EID-2148 | Security violation. You may not delete the account under which you are currently logged in. | You cannot delete the account you are currently loggd in. |
| WID-2149 | There is nothing exportable on this view. | Refer to error message text. |
| WID-2150 | Node {0} is not initialized. Please wait and try again. | Wait till the specified node is initialized and try again. |
| WID-2152 | Spanning tree protection is being disabled for this circuit. | Refer to warning message text. |
| WID-2153 | Adding this drop makes the circuit a PCA circuit. | Refer to warning message text. |
| WID-2154 | Disallow creating monitor circuits on a port grouping circuit. | Refer to warning message text. |
| WID-2155 | Only partial switch count support on some nodes. {0} | The specified nodes do not support switch counts completely. |
| WID-2156 | Manual roll mode is recommended for dual rolls. For auto dual rolls, please verify that roll to facilities are in service and error free. | Refer to warning message text. |
| WID-2157 | Cannot complete roll(s). {0} | CTC could not complete the roll because roll is destroyed, roll is in incomplete state, roll is in TL1_roll state, roll is cancelled, or roll is not ready to complete. |
| EID-2158 | Invalid roll mode. {0} | There are two roll modes such as auto and manual. For one way circuit source roll, the roll mode must be auto and for one way circuit destination roll, the roll mode must be manual. |
| EID-2159 | Roll not ready for completion. {0} | The roll is not ready for completion. |

*Table 4-1 Error Messages (continued)*

| Error or Warning ID | Error or Warning Message | Description |
|---|---|---|
| EID-2160 | Roll not connected.<br>{0} | Refer to error messge text. |
| EID-2161 | Sibling roll not complete.<br>{0} | One of the rolls is not completed for the dual roll. If it is auto roll, it will be completed when a valid signal is detected. If it is manual roll, you must complete the roll from CTC if Bridge and Roll is operated from CTC, or from TL1 if Bridge and Roll is operated from TL1. |
| EID-2162 | Error during roll acknowledgement.<br>{0} | Refer to error message text. |
| EID-2163 | Cannot cancel roll.<br>{0} | CTC cannot cancel the roll. |
| EID-2164 | Roll error.<br>{0} | CTC encountered a roll error. |
| WID-2165 | The MAC address of node {0} has been changed. All circuits originating from or dropping at this node will need to be repaired. | Repair the circuits that originate from or drop at the specified node, with the new MAC address. |
| WID-2166 | Unable to insert node into the domain as the node is not initialized. | Initialize the node and proceed. |
| WID-2167 | Insufficient security privilege to perform this action. | You do not have the previlege to perform this action. |
| WID-2168 | Warnings loading{0}. {1} | CTC encountered warnings while loading the alarm profile import file. |
| WID-2169 | One or more of the profiles selected do not exist on one or more of the nodes selected. | The profile selected does not exist on the node. Select another profile. |
| WID-2170 | The profile list on node {0} is full. Please delete one or more profiles if you wish to add profile.<br>{1} | The number of profile that can exist on a node has reached the limit. To add a profile, delete any of the existing profiles. |
| WID-2171 | You have been logged out. Click OK to exit CTC. | Refer to warning message text. |
| WID-2172 | The CTC CORBA (IIOP) listener port setting of {0} will be applied on the next CTC restart. | The Internet Inter-ORB Protocol (IIOP) listener port setting for the CTC Common Object Request Broker Architecture (CORBA) will be applied on the next CTC restart. |
| EID-2173 | Port unavailable. The desired CTC CORBA (IIOP) listener port, {0}, is already in use or you do not have permission to listen on it. Please select an alternate port. | Select an alternate port, as the current port is either in use or you do not have enough permission on it. |
| EID-2174 | Invalid number entered. Please check it and try again. | You entered an invalid firewall port number. Try again. |
| WID-2175 | Extension byte mismatch.<br>{0} | There is a mismatch with the extension byte. |

*Table 4-1 Error Messages (continued)*

| Error or Warning ID | Error or Warning Message | Description |
|---|---|---|
| WID-2176 | Not all spans have the same OSPF Area ID. This will cause problems with protection switching. To determine the OSPF Area for a given span, click on the span and the OSPF Area will be displayed in the pane to the left of the network map. | Refer to warning message text. |
| WID-2178 | Only one edit pane can be opened at a time. The existing pane will be displayed. | Refer to warning message text. |
| WID-2179 | There is no update as the circuit has been deleted. | Refer to warning message text. |
| EID-2180 | CTC initialization failed in step {0}. | CTC initialization has failed in the specified step. |
| EID-2181 | This link may not be included as it originates from the destination. | You must not include this link as it originates from destination of a circuit. It is against the path selection algorithm. |
| EID-2182 | The value of {0} is invalid. | The value of the specified item is invalid. |
| EID-2183 | Circuit roll failure. Current version of CTC does not support bridge and roll on a VCAT circuit. | Refer to error message text. |
| EID-2184 | Cannot enable the STP on some ports because they have been assigned an incompatible list of VLANs. You can view the VLAN/Spanning Tree table or reassign ethernet ports VLANs. | Refer to error message text. |
| EID-2185 | Cannot assign the VLANs on some ports because they are incompatible with the Spanning Tree Protocol. You can view the VLAN/Spanning Tree table or reassign VLANs. | Refer to error message text. |
| EID-2186 | Software download failed on node {0}. | The software could not be downloaded onto the specified node. |
| EID-2187 | The maximum length for the ring name that can be used is {0}. Please try again. | You must shorten the length of the ring name. |
| EID-2188 | The nodes in this ring do not support alphanumeric IDs. Please use a ring ID between {0} and {1}. | The ring ID should not contain alphanumeric characters, and must be in the specified range. |
| EID-2189 | TL1 keyword "all" can not be used as the ring name. Please provide another name. | Refer to error message text. |
| EID-2190 | Adding this span will cause the ring to contain more nodes than allowed. | You have reached the maximum number of nodes allowed. |
| EID-2191 | Ring name must not be empty. | You must supply a ring name. |
| EID-2192 | Cannot find a valid route for the circuit creation request. | CTC could not complete the circuit creation request either beacuse there are no physical links, or the bandwidth of the available links are already reserved. |
| EID-2193 | Cannot find a valid route for the circuit drop creation request. | Refer to error message text. |
| EID-2194 | Cannot find a valid route for the roll creation request. | Refer to error message text. |
| EID-2195 | The circuit VLAN list cannot be mapped to one spanning tree. You can view the VLAN/Spanning Tree table or reassign VLANs. | Refer to error message text. |

*Table 4-1 Error Messages (continued)*

| Error or Warning ID | Error or Warning Message | Description |
|---|---|---|
| EID-2196 | Unable to relaunch the CTC. {0} | There is an error relaunching CTC. |
| EID-2197 | CORBA failure. Unable to proceed. | There was a CORBA failure, and the task cannot proceed. Verify the Java version. |
| EID-2198 | Unable to switch to the {0} view. | CTC is unable to switch to the specified view. |
| EID-2199 | Login failed on {0} {1} | The login failed on the specified tasks. |
| EID-2200 | CTC has detected a jar file deletion. The jar file was used to manage one or more nodes. This CTC session will not be able to manage those nodes and they will appear gray on the network map. It is recommended that you exit this CTC session and start a new one. | Refer to error message text. |
| EID-2202 | Intra-node circuit must have two sources to be Dual Ring Interconnect. | Intranode circuit must have two sources to be a dual ring interconnect (DRI). |
| EID-2203 | No member selected. | You must select a member. |
| EID-2204 | Number of circuits must be a positive integer | The number of circuits cannot be zero or negative. |
| EID-2205 | Circuit Type must be selected. | You must select a circuit type. |
| EID-2206 | Unable to autoselect profile! Please select profile(s) to store and try again. | Refer to error message text. |
| EID-2207 | You cannot add this span. Either the ring name is too big (i.e., ring name length is greater than {0}) or the endpoints do not support alphanumeric IDs. | Reduce the length of the ring name, or remove the alphanumberic characters from the end points. |
| EID-2208 | This is an invalid or unsupported JRE. | The version of Java Runtime Environment (JRE) is either invalid or unsupported. |
| EID-2209 | The user name must be at least {0} characters long. | The user name must be at least of the specified character length. |
| EID-2210 | No package name selected. | You must select a package name. |
| EID-2211 | No node selected for upgrade. | You must select a node for the upgrade. |
| EID-2212 | Protected Line is not provisionable. | The protected line cannot be provisioned. Choose another line. |
| WID-2213 | The current type or state of some drops does not allow the new circuit state of {0} to be applied to them indirectly. | The circuit state, specified by {0} cannot be applied to the selected drops. |
| EID-2214 | The node is disconnected. Please wait till the node reconnects. | Refer to error message text. |
| EID-2215 | Error while leaving {0} page. | There was an error while leaving the specified page. |
| EID-2216 | Error while entering {0} page. | There was an error while entering the specified page. |
| EID-2217 | Some conditions could not be retrieved from the network view | Refer to error message text. |
| EID-2218 | Bandwidth must be between {0} and {1} percent. | The bandwidth must be within the specified parameters. |

*Table 4-1 Error Messages (continued)*

| Error or Warning ID | Error or Warning Message | Description |
|---|---|---|
| EID-2219 | Protection operation failed, XC loopback is applied on cross-connection. | As the protection operation failed, a cross-connect (XC) loopback will be applied on cross-connection. |
| EID-2220 | The tunnel status is PARTIAL. CTC will not be able to change it. Please try again later | Refer to error message text. |
| EID-2221 | Cannot find a valid route for the unprotected to {0} upgrade request. | Refer to error message text. |
| EID-2222 | One or more of the following nodes are currently part of a 4-fiber {0}. Only a single 4-fiber {0} is supported per node. {1} | The nodes, specified by {1}, are already part of a 4-fiber ring type, specified by {0}. |
| EID-2223 | Only one circuit can be upgraded at a time. | Refer to error message text. |
| EID-2224 | This link may not be included as it terminates on the source. | Refer to error message text. |
| EID-2225 | No valid signal while trying to complete the roll. (0) | Roll can be completed only when a valid signal is detected. If not, the roll completion may result in an error. |
| EID-2226 | Circuit roll failure.<br>{0} | Refer to error message text. |
| EID-2320 | This VCAT circuit does not support deletion of its member circuits. | You can not delete a circuit that is a member of VCAT circuit. |
| EID-2321 | Error deleting member circuits.<br>{0} | Refer to error message text. |
| WID-2322 | Not all cross-connects from selected circuits could be merged into the current circuit. They may appear as partial circuits. | Refer to warning message text. |
| EID-2323 | Circuit roll failure.<br>Bridge and roll is not supported on a monitor circuit. | A monitor circuit does not support Bridge and Roll. |
| EID-2324 | Circuit upgrade error.<br>{0} | Refer to error message text. |
| EID-2325 | You have failed {0} times to unlock this session. CTC will exit after you click OK or close this dialog box. | The maximum amount of attempts to unlock this session has been reached. |
| WID-2326 | Currently, CTC does not support bridge and roll on circuits that are entirely created by TL1. To continue with bridge and roll in CTC, selected circuits must be upgraded.<br>OK to upgrade selected circuits and continue bridge and roll operation? | Refer to warning message text. |
| WID-2327 | Currently, CTC does not support bridge and roll on circuits that are partially created by TL1. To continue with bridge and roll in CTC, selected circuits must be upgraded.<br>OK to upgrade selected circuits and continue bridge and roll operation? | Refer to warning message text. |
| EID-2328 | Circuit reconfigure error.<br>{0} | The attempt to reconfigure the specified circuit has failed. |

*Table 4-1 Error Messages (continued)*

| Error or Warning ID | Error or Warning Message | Description |
|---|---|---|
| EID-2329 | {0} of {1} circuits could not be successfully created. | A few circuits could not be created. |
| EID-2330 | Circuit verification: selected {0} invalid!<br>{1} | The selected item, specified by {0}, is invalid as per the details, specified in {1}. |
| EID-2331 | Deleting {0} may be service affecting. | Deleting the item can affect the service of CTC. |
| EID-2332 | Hold-off timer validation error in row [0].<br>{1} hold-off timer for {2} must be between {3}-10,000 ms, in steps of 100 ms. | Refer to error message text. |
| EID-3001 | An Ethernet RMON threshold with the same parameters already exists. Please change one or more of the parameters and try again. | Change a few parameters in an Ethernet remote monitoring (RMON) threshold and try again. |
| EID-3002 | Error retrieving defaults from the node: {0} | There was an error while retrieving the defaults from the specified node. |
| EID-3003 | Cannot load file {0}. | CTC cannot load the specified file. |
| EID-3004 | Cannot load properties from the node | Refer to error message text. |
| EID-3005 | Cannot save NE Update values to file {0} | CTC cannot save the network element (NE) update values to the specified file. |
| EID-3006 | Cannot load NE Update properties from the node | Refer to error message text. |
| EID-3007 | Provisioning Error for {0} | There was a provisioning error for the specified item. |
| EID-3008 | Not a valid Card | You cannot perform DWDM automatic node setup (ANS) from the Card view. Please navigate to the Node view and try again. |
| EID-3009 | No {0} selected | Select the specified item, for example, VLAN, port, slot, etc. |
| EID-3010 | Unable to create bidirectional optical link | Refer to error message text. |
| EID-3011 | The file {0} doesn't exist or cannot be read. | The specified file does not exist or cannot be read. |
| EID-3012 | The size of {0} is zero. | The size of the specified item is zero. |
| EID-3013 | {0} encountered while restoring database. | The specified item was encountered while restoring the database. |
| EID-3014 | The operation was terminated due to the following error:<br>{0} | Refer to error message text. |
| EID-3015 | {0} encountered while performing DB backup. | The specified item or condition was encountered while performing the DB backup. |
| EID-3016 | Invalid subnet address. | Refer to error message text. |
| EID-3017 | Subnet address already exists. | Refer to error message text. |

*Table 4-1 Error Messages (continued)*

| Error or Warning ID | Error or Warning Message | Description |
|---|---|---|
| EID-3018 | Standby TSC not ready. | The standby Timing and Shelf Control card (TSC) not ready. |
| EID-3019 | Incomplete internal subnet address. | Enter the complete internal subnet address. |
| EID-3020 | TSC One and TSC Two subnet addresses cannot be the same. | A node's internal subnet must be different from one another as each TSC is on separate ethernet buses, isolated by broadcast domains. |
| EID-3021 | An error was encountered while retrieving the diagnostics: {0} | Refer to error message text. |
| EID-3022 | Requested action not allowed. | The requested action is not allowed. |
| EID-3023 | Unable to retrieve low order cross connect mode. | Refer to error message text. |
| EID-3024 | Unable to switch {0} cross connect mode.<br>Please verify that the type and/or number of circuits provisioned does not exceed the criterion for switching modes. | CTC cannot switch the cross-connect mode for the specified item, as the type or the number of circuits does not match with the criterion for switching modes. |
| EID-3025 | Error while retrieving thresholds. | There was an error retrieving the thresholds. |
| EID-3026 | Cannot modify send DoNotUse. | You cannot modify the Send DoNotUse field. |
| EID-3027 | Cannot modify SyncMsg. | You cannot modify the SyncMsg field. |
| EID-3028 | Cannot change port type. | You cannot change the port type. |
| EID-3029 | Unable to switch to the byte because an overhead change is present on this byte of the port. | Refer to error message text. |
| EID-3031 | Error hard-resetting card. | There was an error while resetting card hardware. |
| EID-3032 | Error resetting card. | There was an error while resetting the card. |
| EID-3033 | The lamp test is not supported on this shelf. | Refer to error message text. |
| EID-3035 | The cross connect diagnostics cannot be performed | Refer to error message text. |
| EID-3036 | The cross connect diagnostics test is not supported on this shelf. | The cross-connect diagnostics test is not supported on this shelf. |
| EID-3037 | A software downgrade cannot be performed to the selected version while a SSXC card is inserted in this shelf. Please follow the steps to replace the SSXC with a CXC card before continuing the software downgrade. | Refer to error message text. |
| EID-3038 | A software downgrade cannot be performed at the present time. | Refer to error message text. |
| EID-3039 | Card change error. | There was an error while changing the card. |
| EID-3040 | Invalid card type. | The selected card type is invalid. |
| EID-3041 | Error applying changes. | CTC is unable to create a protection group. Check if the protect port supports circuits, a timing reference, SONET SDCC, orderwire, or a test access point. |

*Table 4-1 Error Messages (continued)*

| Error or Warning ID | Error or Warning Message | Description |
|---|---|---|
| EID-3042 | The flow control low value must be less than the flow control high value for all ports in the card. | Refer to error message text. |
| EID-3043 | Error while retrieving line info settings. | Refer to error message text. |
| EID-3044 | Error while retrieving line admin info settings. | Refer to error message text. |
| EID-3045 | Error while retrieving transponder line admin info settings. | Refer to error message text. |
| EID-3046 | The flow control water mark value must be between {0} and {1}, inclusive. | The flow control watermark value must be between the two specified values. |
| EID-3047 | The file named {0} could not be read. Please check the name and try again. | Refer to error message text. |
| EID-3048 | There is no IOS startup config file available to download. | CTC could not find the configuration file for IOS startup. |
| EID-3049 | There is an update in progress so the download cannot be done at this time. | Refer to error message text. |
| EID-3050 | An exception was caught trying to save the file to your local file system. | Check whether the file already exists and cannot be over written, or there isa space constraint in the file system. |
| EID-3051 | The maximum size for a config file in bytes is: {0} | The size of the configuration file should not exceed the specified number of bytes. |
| EID-3052 | There was an error saving the config file to the TCC. | Refer to error message text. |
| EID-3053 | The value of {0} must be between {1} and {2} | The value of the item must be between the specified values. |
| EID-3054 | Cannot remove provisioned input/output ports or another user is updating the card, please try later. | Another user may be updating the card. You can try again later. |
| EID-3055 | Cannot create soak maintance pane. | Refer to error message text. |
| EID-3056 | Cannot save defaults to file {0} | CTC cannot save the defaults to the specified file. |
| EID-3057 | Cannot load default properties from the node. | Refer to error message text. |
| EID-3058 | File {0} does not exist. | Refer to error message text. |
| EID-3059 | Error encountered while refreshing. | There was an error while refreshing. |
| EID-3060 | The ALS Recovery Pulse Interval must be between {0} seconds and {1} seconds. | The automatic laser shutdown (ALS) Recovery Interval must be between the specified range of seconds. |
| EID-3061 | The ALS Recovery Pulse Duration must be between {0} seconds and {1} seconds. | The automatic laser shutdown (ALS) Recovery Duration must be between the specified range of seconds. |
| EID-3062 | Error encountered while setting values. | Refer to error message text. |
| EID-3063 | Unable to retriever bridge port settings. | Refer to error message text. |
| EID-3064 | Not a G1000 Card. | This card is not a G1000-4 card. |

*Table 4-1 Error Messages (continued)*

| Error or Warning ID | Error or Warning Message | Description |
|---|---|---|
| EID-3065 | An error was encountered while attempting to create RMON threshold: {0} | You must wait some time before you try again. |
| EID-3066 | Minimum sample period must be greater than or equal to 10. | Refer to error message text. |
| EID-3067 | Rising Threshold: Invalid Entry, valid range is from 1 to {0} | This is an invalid rising threshold entry. The valid range is from 1 to the specified value. |
| EID-3068 | Falling Threshold: Invalid Entry, valid range is from 1 to {0} | This is an invalid falling threshold entry. The valid range is from 1 to the specified value. |
| EID-3069 | Rising threshold must be greater than or equal to falling threshold. | Refer to error message text. |
| EID-3070 | Error in data for ports {0} Exactly one VLAN must be marked untagged for each port. These changes will not be applied. | CTC encountered data error for the specified ports. Only one VLAN should be marked untagged for each port. |
| EID-3071 | Get Learned Address | Unable to retrieve the learned MAC address from the NE. |
| EID-3072 | Clear Learned Address | Failure attempting to clear the learned MAC address from a specific card or Ether group. |
| EID-3073 | Clear Selected Rows | Failure attempting to clear the learned MAC address from a specific card or Ether group. |
| EID-3074 | Clear By {0} | Error encountered trying to clear the learned MAC address from either a VLAN or a port. |
| EID-3075 | At least one row in param column needs to be selected. | Refer to error message text. |
| EID-3076 | CTC lost its connection with this node. The NE Setup Wizard will exit. | Refer to error message text. |
| EID-3077 | No optical link selected. | Refer to error message text. |
| EID-3078 | Unable to create optical link. | Refer to error message text. |
| EID-3079 | Cannot apply defaults to node: {0} | CTC cannot apply the defaults to the specified node. |
| EID-3080 | Cannot go to the target tab {0} | CTC cannot go to the specified target tab. |
| EID-3081 | Port type cannot be changed. | Refer to error message text. |
| EID-3082 | Cannot modify the {0} extension byte. | You cannot modify the specified extension byte. |
| EID-3083 | Error while retrieving stats. | Error in getting statistics. |
| EID-3084 | Error encountered while trying to retrieve laser parameters for {0} | There is no card, or there was an internal communications error when attempting to get the laser parameters for the card. |
| EID-3085 | No OSC Terminations selected | Select an OSC termination and proceed. |
| EID-3086 | One or more Osc terminations could not be created. | Refer to error message text. |

*Table 4-1 Error Messages (continued)*

| Error or Warning ID | Error or Warning Message | Description |
|---|---|---|
| EID-3087 | OSC termination could not be edited. | Refer to error message text. |
| EID-3088 | No {0} card to switch. | No card of the specified type to switch. |
| EID-3089 | Cannot use/change {0} state when {1} is failed or missing. | Cannot use or change the specified state when the card is failed or missing. |
| EID-3090 | Cannot perform operation as {0} is {1}LOCKED_ON/LOCKED_OUT. | Cannot perform operation. |
| EID-3091 | Cannot perform the operation as protect is active. | Refer to error message text. |
| EID-3092 | Invalid service state. The requested action cannot be applied. | Select another service state and proceed. |
| EID-3093 | Cannot perform the operation as duplex pair is {0}locked. | Refer to error message text. |
| EID-3094 | Cannot perform the operation as no XC redundancy is available. | You cannot perform the requested operation on the cross connect card without having a backup cross connect card. |
| EID-3095 | Deletion failed since the circuit is in use | Refer to error message text. |
| WID-3096 | Internal communication error encountered while trying to retrieve laser parameters. This can happen when equipment is not present or when equipment is resetting. Check the equipment state and try to refresh the values again. | Refer to warning message text. |
| EID-3097 | The ring termination is in use. | The ring termination you are trying to access is in use. Try after sometime. |
| EID-3098 | No ring terminations selected. | Select one of the ring terminations. |
| EID-3099 | Sorry, entered key does not match existing authentication key. | Check the authentication key and reenter. |
| EID-3100 | Error encountered during authentication. | There was an error in authentication. Verify that the key does not exceed the character limit . |
| EID-3101 | DCC Metric is not in the range 1 - 65535. | The DCC metric should be in the range of 1 to 65535. |
| EID-3102 | Invalid DCC Metric | There was an invalid DCC metric. |
| EID-3103 | Invalid IP Address: {0} | The IP address is invalid. |
| EID-3104 | Router priority is not in the range of 0 - 255 | The router priority should be in the range of 0 to 255. |
| EID-3105 | Invalid Router Priority | The router priority is invalid. |
| EID-3106 | Hello Interval is not in the range of 1 - 65535 | The hello interval should be in the range of 1 to 65535. |
| EID-3107 | Invalid Hello Interval | The hello interval is invalid. |
| EID-3109 | Invalid Dead Interval value. Valid range is 1 - 2147483647 | The dead interval value must be between 1 and 2147483647. |
| EID-3110 | Dead Interval must be larger than Hello Interval | Refer to error message text. |
| EID-3111 | LAN transit delay is not in the range of 1 - 3600 seconds | The LAN transit delay should be in the range of 1 to 3600 seconds. |

*Table 4-1 Error Messages (continued)*

| Error or Warning ID | Error or Warning Message | Description |
|---|---|---|
| EID-3112 | Invalid Transmit Delay | The transmit delay is invalid. |
| EID-3113 | Retransmit Interval is not in the range 1 - 3600 seconds | The retransmit interval should be in the range of 1 to 3600 seconds. |
| EID-3114 | Invalid Retransit Interval | The retransmit interval is invalid. |
| EID-3115 | LAN Metric is not in the range 1 - 65535. | The LAN metric should be in the range of 1 to 65535. |
| EID-3116 | Invalid LAN Metric | The LAN metric is invalid. |
| EID-3117 | If OSPF is active on LAN, no DCC Area Ids may be 0.0.0.0. Please change all DCC Area Ids to non-0.0.0.0 values before enabling OSPF on the LAN. | Refer to error message text. |
| EID-3118 | If OSPF is active on LAN, LAN Area ID may not be the same as DCC Area Id. | LAN must be part of a different OSPF area other than the DCC network. |
| EID-3119 | Validation Error | CTC was unable to validate the values entered by the user. This error message is common to several different provisioning tabs within CTC (examples include the SNMP provisioning tab, the General> Network provisioning tab, the Security > Configuration provisioning tab, etc.). |
| EID-3120 | No object of type {0} selected to delete. | Choose an object of the specified type to delete. |
| EID-3121 | Error Deleting {0} | There is an error deleting the item. |
| EID-3122 | No object of type {0} selected to edit. | Choose an object of the specified type to edit. |
| EID-3123 | Error Editing {0} | There was an error editing the item. |
| EID-3124 | {0} termination is in use.<br>Delete the associated OSPF Range Table Entry and try again | Refer to error message text. |
| EID-3125 | No {0} Terminations selected. | No specified terminations are selected. |
| EID-3126 | {0} termination could not be edited. | CTC could not edit the specified termination. |
| EID-3127 | Unable to provision orderwire because E2 byte is in use by {0}. | Refer to error message text. |
| EID-3128 | The authentication key may only be {0} characters maximum | The authentication key cannot exceed the specified number of characters. |
| EID-3129 | The authentication keys do not match! | Refer to error message text. |
| EID-3130 | Error creating OSPF area virtual link. | CTC encountered an error while creating the area virtual link. |
| EID-3131 | Error creating OSPF virtual link. | CTC encountered an error creating the virtual link. |
| EID-3132 | Error setting OSPF area range: {0}, {1}, false. | CTC encountered an error while setting the area range for the specified values. |

*Table 4-1 Error Messages (continued)*

| Error or Warning ID | Error or Warning Message | Description |
|---|---|---|
| EID-3133 | Max number of OSPF area ranges exceeded. | OSPF area ranges exceeded the maximum number. |
| EID-3134 | Invalid Area ID. Use DCC OSPF Area ID, LAN Port Area ID, or 0.0.0.0. | Refer to error message text. |
| EID-3135 | Invalid Mask | Refer to error message text. |
| EID-3136 | Invalid Range Address | The range address is invalid. Try again. |
| EID-3137 | Your request has been rejected because the timing source information was updated while your changes were still pending. Please retry. | Refer to error message text. |
| EID-3138 | Invalid clock source for switching. | You have selected an invalid clock source. Choose another clock. |
| EID-3139 | Cannot switch to a reference of inferior quality. | Refer to error message text. |
| EID-3140 | Higher priority switch already active. | You cannot switch the timing source manually when a higher priority switch is already active. |
| EID-3141 | Attempt to access a bad reference. | Refer to error message text. |
| EID-3142 | No Switch Active. | None of the switches are active. |
| EID-3143 | Error creating static route entry. | CTC encountered an error while a creating static route entry. |
| EID-3144 | Max number of static routes exceeded. | The number of static routes has exceeded its limit. |
| EID-3145 | RIP Metric is not in the range 1-15. | The Routing Information Protocol (RIP) metric should be in the range of 1 to 15. |
| EID-3146 | Invalid RIP Metric | Refer to error message text. |
| EID-3147 | Error creating summary address. | There was an error while creating the summary address. |
| EID-3148 | No Layer 2 domain has been provisioned. | You must provision any one of the layer 2 domain. |
| EID-3149 | Unable to retrieve MAC addresses. | Refer to error message text. |
| EID-3150 | The target file {0} is not a normal file. | The specified target file is not a normal file. |
| EID-3151 | The target file {0} is not writeable. | The target file is not writeable. Specify another file. |
| EID-3152 | Error creating Protection Group | CTC encountered an error creating Protection Group. |
| EID-3153 | Cannot delete card, it is in use. | Cannot delete card. It is in use. |
| EID-3154 | Cannot {0} card, provisioning error. | CTC cannot perform the task on the card. |
| EID-3155 | Error Building Menu | CTC encountered an error building the menu. |

*Table 4-1 Error Messages (continued)*

| Error or Warning ID | Error or Warning Message | Description |
|---|---|---|
| EID-3156 | Error on building menu (cards not found for {0} group) | CTC encountered an error while building the menu, as cards could not be found for the specified group). |
| EID-3157 | Unable to set selected model: unexpected model class {0} | CTC encountered an unexpected model class while trying to complete the task. |
| EID-3158 | Unable to switch, a similar or higher priority condition exists on peer or far-end card. | Refer to error message text. |
| EID-3159[1] | Error applying operation. | CTC encountered an error while applying this operation. |
| EID-3160 | {0} error encountered. | CTC encountered the specified error. |
| EID-3161 | Ring Upgrade Error | An error was encountered while attempting to upgrade the BLSR. Refer to the details portion of the error dialog box for more information. |
| EID-3162 | This protection operation cannot be set because the protection operation on the other side has been changed but not yet applied. | Refer to error message text. |
| EID-3163 | Cannot validate data for row {0} | CTC cannot validate the data for the specified row. |
| EID-3164 | New Node ID ({0}) for Ring ID {1} duplicates ID of node {2} | The new specified node ID for the specified ring ID is the same as another node ID. |
| EID-3165 | The Ring ID provided is already in use. Ring IDs must be unique | Refer to error message text. |
| EID-3166 | Error refreshing {0} table | CTC encountered an error while refreshing the specified table. |
| EID-3167 | Slot already in use | Refer to error message text. |
| EID-3168 | Provisioning Error | An error was encountered while attempting the specified provisioning operation. Refer to the details portion of the error dialog box for more information. |
| EID-3169 | Error Adding Card | CTC encountered an error while adding the card. |
| EID-3170 | Cannot delete card, {0} | Refer to error message text. |
| EID-3171 | Error creating Trap Destination | CTC encountered an error creating the trap destination. |
| EID-3172 | No RMON Thresholds selected | Select an RMON threshold. |
| EID-3173 | The contact “{0}” exceeds the limit of {1} characters. | The specified contact exceeds the specified character limit. |
| EID-3174 | The location “{0}” exceeds the limit of {1} characters. | The specified location exceeds the specified character limit. |

*Table 4-1 Error Messages (continued)*

| Error or Warning ID | Error or Warning Message | Description |
|---|---|---|
| EID-3175 | The operator identifier "{0}" exceeds the limit of {1} characters. | The specified operator identifier exceeds the specified character limit. |
| EID-3176 | The operator specific information "{0}" exceeds the limit of {1} characters. | The specified operator specific information exceeds the specified character limit. |
| EID-3177 | The node name cannot be empty. | The specified name is empty. |
| EID-3178 | The name "{0}" exceeds the limit of {1} characters. | The specified name exceeds the specified character limit. |
| EID-3179 | Protect card is in use. | Refer to error message text. |
| EID-3180 | 1+1 Protection Group does not exist. | Create a 1+1 protection group. |
| EID-3181 | Y Cable Protection Group does not exist. | Refer to error message text. |
| EID-3182 | The Topology Element is in use and cannot be deleted as requested | You cannot delete the topology element which is in use. |
| EID-3183 | Error Deleting Protection Group | CTC encountered an error while deleting the protection group. |
| EID-3184 | No {0} selected. | You must select an item before completing this task. |
| EID-3185 | There is a protection switch operation on this ring. Therefore, it cannot be deleted at this time. | Refer to error message text. |
| EID-3186 | Busy: {0} is {1} and cannot be deleted as requested. | The request cannot be completed. |
| EID-3187 | Error deleting trap destination. | CTC encountered an error deleting the trap destination. |
| EID-3214 | Could not get number of HOs for line. | The number of High Orders for line is not available. |
| EID-3215 | Error in refreshing. | Used frequently in pane classes to indicate a general error condition when trying to refresh from the model. |
| EID-3216 | Invalid proxy port. | Refer to error message text. |
| EID-3217 | Could not refresh stats. | CTC could not refresh statistics values. |
| EID-3218 | Unable to launch automatic node setup. | Refer to error message text. |
| EID-3219 | Unable to refresh automatic node setup information. | Failure trying to retrieve automatic node setup information. |
| EID-3220 | Error refreshing row {0} | Error refreshing the specified row. |
| EID-3222 | Could not clear stats. | Refer to error message text. |
| EID-3223 | Error cancelling software upgrade. | CTC encountered an error while cancelling the upgrade. Software is not upgraded. |
| EID-3224 | Error accepting load. | Refer to error message text. |
| EID-3225 | Error while refreshing pane. | Used frequently in pane classes to indicate a general error condition when trying to refresh from the model. |

*Table 4-1 Error Messages (continued)*

| Error or Warning ID | Error or Warning Message | Description |
|---|---|---|
| EID-3226 | {0} termination(s) could not be deleted. {1} | Refer to error message text. |
| EID-3227 | Unable to record a baseline, performance metrics will remain unchanged. | CTC failed to set the baseline values while provisioning NE. Previous values remain unchanged. |
| EID-3228 | {0} termination(s) could not be created.<br>{1} | Refer to error message text. |
| EID-3229 | RIP is active on the LAN. Please disable RIP before enabling OSPF. | Turn off the Routing Information Protocol (RIP) on the LAN, before enabling OSPF. |
| EID-3230 | OSPF is active on the LAN. Please disable OSPF before enabling RIP. | Turn off the OSPF on the LAN before enabling RIP. |
| EID-3231 | Error in Set OPR | An error was encountered while attempting to provision the optical power received (OPR). |
| WID-3232 | Cannot transition port state indirectly because the port is still providing services: if the port state should be changed, edit it directly via port provisioning. | Edit the port state while provisioning the port. |
| EID-3233 | Current loopback provisioning does not allow this state transition. | Refer to error message text. |
| EID-3234 | Current synchronization provisioning does not allow this state transition | You cannot transition the port state to the target date while in the current synchonization state. |
| EID-3235 | Cannot perform requested state transition on this software version. | Refer to error message text. |
| EID-3236 | Database Restore failed. {0} | CTC failed to restore the specified database. |
| EID-3237 | Database Backup failed. {0} | CTC failed to backup the specified database. |
| EID-3238 | Send PDIP setting on {0} is inconsistent with that of control node {1} | The send payload defect indicator path (PDI-P) setting on the specified item should be consistent with that of the specified control node. |
| EID-3239 | The overhead termination is invalid | Refer to error message text. |
| EID-3240 | The maximum number of overhead terminations has been exceeded. | Overhead terminations have exceeded the limit. |
| EID-3241 | The {0} termination port is in use. | The specified termination port is in use. Select another port. |
| EID-3242 | {1} exists on the selected ports. Please create {0} one by one. | The specified DCC already exists on the selected port. You may create a DCC of another type. |

*Table 4-1 Error Messages (continued)*

| Error or Warning ID | Error or Warning Message | Description |
|---|---|---|
| WID-3243 | The port you have chosen as an {0} endpoint already supports an {1}. The port cannot support both DCCs. After the {0} is created, verify that no EOC alarms are present and then delete the {1} to complete the downgrade. | The same port can not be used by multiple DCCs. |
| EID-3244 | {0} exists on the selected ports. Please create {1} one by one. | The specified DCC already exists on the selected port. You may create a DCC of another type. |
| WID-3245 | The port you have chosen as an {1} endpoint already supports an {0}. The port cannot support both DCCs. After the {1} is created, verify that no EOC alarms are present and then delete the {0} to complete the upgrade. | The port selected as a DCC endpoint already supports another DCC. Refer to warning message text. |
| EID-3246 | Wizard unable to validate data: {0} | CTC encountered an error. |
| EID-3247 | Ordering error. The absolute value should be {0} | The absolute value entered was wrong. |
| EID-3248 | Wrong parameter is changed: {0} | CTC changed the incorrect parameter. |
| EID-3249 | Invalid voltage increment value. | Refer to error message text. |
| EID-3250 | Invalid power monitor range. | Refer to error message text. |
| EID-3251 | Unable to complete requested action. {0} | CTC could not complete the specified action. |
| EID-3252 | No download has been initiated from this CTC session. | Refer to error message text. |
| EID-3253 | Reboot operation failed. {0} | Refer to error message text. |
| EID-3254 | Validation Error. {0} | The Cisco Transport Controller (CTC) was unable to validate the values entered by the user, specified by {0}. This error message is common to several different provisioning tabs within the CTC. |
| EID-3255 | Cannot change timing configuration, manual/force operation is performed. | Refer to error message text. |
| WID-3256 | Could not assign timing reference(s) because - at least one timing reference has already been used and/or - a timing reference has been attempted to be used twice. Please use the “Reset” button and verify the settings. | Refer to warning message text. |
| EID-3257 | Duplicate DCC number detected: {0}. | CTC detected more than one occurene of the a DCC number. Remove one of them. |
| EID-3258 | There was a software error attempting to download the file. Please try again later. | Refer to error message text. |
| EID-3259 | Create FC-MR Threshold | You must create a Fibre Channel Multirate (FC_MR) card threshold. |
| EID-3260 | An error was encountered while provisioning the internal subnet:<br>{0} | The specified internal subnet could not be provisoned. |
| EID-3261 | The port rate provisioning cannot be changed while circuits exist on this port. | Refer to error message text. |

*Table 4-1 Error Messages (continued)*

| Error or Warning ID | Error or Warning Message | Description |
|---|---|---|
| EID-3262 | The port provisioning cannot be changed when the port status is not OOS. | You must provision the ports only when the port is Out of Service. |
| WID-3263 | You are using Java version {0}. CTC should run with Java version {1}. It can be obtained from the installation CD or http://java.sun.com/j2se/ | CTC is being launched with the wrong version of the JRE {0}. This version of CTC requires a particular version of the JRE {1}. The CTC and browser must be closed and restarted to allow the correct Java version to be loaded. |
| EID-3264 | The port provisioning cannot be changed while the port is {0}. | You must modify the port provisioning only when the port is out of service. |
| EID-3265 | Error modifying Protection Group | Protection Group could not be modified. |
| EID-3266 | Conditions could not be retrieved from the shelf or card view. | Refer to error message text. |
| WID-3267 | Cannot edit XTC protection group. | Refer to warning message text. |
| WID-3268 | Invalid entry. {0} | The specified entry is invalid. |
| WID-3269 | {0} was successfully initiated for {1} but its completion status was not able to be obtained from the node. {0} may or may not have succeeded. When the node is accessible, check its software version. | Refer to error message text. |
| WID-3270 | The file {0} does not exist. | The specified file does not exist. |
| WID-3271 | The value entered must be greater than {0}. | The value entered must be greater than the specified value. |
| WID-3272 | Entry required | An entry is required to complete this task. |
| WID-3273 | {0} already exists in the list. | The specified item already exists in the list. |
| WID-3274 | A software upgrade is in progress. Network configuration changes that results a node reboot can not take place during software upgrade. Please try again after software upgrade is done. | Refer to warning message text. |
| WID-3275 | Make sure the Remote Interface ID and the Local Interface ID on the two sides are matched. (Local Interface ID on this node should equal Remote Interface ID on the neighbor node and vice-versa.) | Refer to warning message text. |
| WID-3276 | Both {0} and {1} exist on the same selected port. {2} | The specified port has both SDCC and LDCC. |
| WID-3277 | The description cannot contain more than {0} characters. Your input will be truncated. | The input exceeds the character limit. The value will be truncated to the maximum chacter limit. |
| WID-3279 | Card deleted, returning to shelf view. | CTC returns to node view. |
| WID-3280 | ALS will not engage until both the protected trunk ports detect LOS. | Refer to warning message text. |
| WID-3281 | A software upgrade is in progress. {0} can not proceed during a software upgrade. Please try again after the software upgrade has completed. | Refer to warning message text. |

*Table 4-1 Error Messages (continued)*

| Error or Warning ID | Error or Warning Message | Description |
|---|---|---|
| WID-3282 | Performing a software upgrade while TSC 5 is active could result in a service disruption. It is recommended that you make TSC 10 the active TSC by performing a soft reset of TSC 5. The following 15600s are currently unsafe to upgrade... | Refer to warning message text. |
| WID-3283 | Before activating a new version, make sure you have a database backup from the current version. | Refer to warning message text. |
| WID-3284 | Reverting to an older version. | CTC is being reverted to an older version of application. |
| WID-3285 | Applying FORCE or LOCKOUT operations may result in traffic loss. | Refer to warning message text. |
| WID-3286 | The ring status is INCOMPLETE. CTC cannot determine if there are existing protection operations or switches in other parts of the ring. Applying a protection operation at this time could cause a traffic outage. Please confirm that no other protection operations or switches exist before continuing. | Refer to warning message text. |
| WID-3287 | There is a protection operation or protection switch present on the ring. Applying this protection operation now will probably cause a traffic outage. | Refer to warning message text. |
| WID-3288 | This ring status is INCOMPLETE. CTC will not be able to apply this change to all of the nodes in the {0}. | Change the ring status to apply the change to all nodes in the ring type. |
| EID-3290 | Unable to delete specified provisionable patchcord(s). | Refer to error message text. |
| EID-3291 | Cannot change revertive behavior due to an active protection switch. | Protection switch should not be active to change the revertive behaviour. |
| EID-3292 | Error resetting shelf. | CTC encountered an error while resetting the node. |
| EID-3293 | No such provisionable patchcord. | You are attempting to delete a provisionable patchcord that does not exist. This happens when multiple instances of CTC are running and attempting to delete the same provisionable patchcord concurrently. |
| EID-3294 | No RMON thresholds available for selected port. | Refer to error message text. |
| EID-3295 | This card does not support RMON thresholds. | Refer to error message text. |
| EID-3296 | Buffer-to-buffer credit is only supported for Fibre Channel (FC) and FICON. | Refer to error message text. |
| EID-3298 | ALS Auto Restart is not supported by this interface. | Refer to error message text. |
| EID-3300 | Can not have duplicate OSPF area IDs. | OSPF area IDs should be unique. |
| EID-3301 | LAN metric may not be zero. | Refer to error message text. |
| EID-3302 | Standby {0} not ready. | Standby controller card is not ready. |
| EID-3303 | DCC Area ID and {0} conflict.<br>{1} | DCC Area ID and ring type, specified by {0}, conflict each other due to the details specified by {1}. |

*Table 4-1 Error Messages (continued)*

| Error or Warning ID | Error or Warning Message | Description |
|---|---|---|
| EID-3304 | DCC number is out of range. | Enter a DCC number that is within the range |
| EID-3305 | Can not have OSPF turned on on the LAN interface and the back bone area set on a DCC interface. | You cannot have the default OSPF area on a DCC while OSPF is enabled on the LAN. |
| EID-3306 | Ethernet circuits must be bidirectional. | Refer to error message text. |
| EID-3307 | Error while creating connection object at {0}. | CTC encountered an error at the specified connection while creating the connection. |
| EID-3308 | DWDM Link can be used only for optical channel circuits. | Refer to error message text. |
| EID-3309 | OCH-NC circuit: link excluded - wrong direction. | The optical channel (circuit) does not allow the specified link to be included because it is in the wrong optical direction. |
| EID-3310 | DWDM Link does not have wavelength available. | Refer to error message text. |
| EID-3311 | Laser already on. | Refer to error message text. |
| EID-3312 | Unable to change the power setpoint {0} {1} | CTC cannot change change the power setpoint. The new setpoint would either make the thresholds inconsistent or set the fail threshold outside the range. |
| EID-3313 | Unable to modify offset. Amplifier port is in service state. | Refer to error message text. |
| EID-3314 | Requested action not allowed. Invalid state value. | Refer to error message text. |
| EID-3315 | Unable to perform operation. | CTC is unable to perform operation. |
| EID-3316 | Wrong node side. | This task was applied to the wrong node side. |
| EID-3317 | Name too long. | Reduce the number of charcters in the name. |
| EID-3318 | Illegal name. | The name you entered is illegal. |
| EID-3319 | Wrong line selection. | Select another line |
| EID-3320 | Unable to delete optical link. | CTC cannot delete the optical link. |
| EID-3321 | This feature is unsupported by this version of software. | Refer to error message text. |
| EID-3322 | Equipment is not plugged-in. | Plug-in the equipment and proceed. |
| EID-3323 | APC system is busy. | Automatic Power Control (APC) system is busy. |
| EID-3324 | No path to regulate. | There is no circuit path to regulate. |
| EID-3325 | Requested action not allowed. | Generic DWDM provisioning failure message. |
| EID-3326 | Wrong input value. | The input value is incorrect. |
| EID-3327 | Error in getting thresholds. | There was an error retrieving the thresholds. This message is displayed only for the OSCM/OSC-CSM line thresholds. |
| EID-3328 | Error applying changes to row {0}.Value out of range. | There was an error applying the changes to the specified row. The value is out of range. |

*Table 4-1 Error Messages (continued)*

| Error or Warning ID | Error or Warning Message | Description |
|---|---|---|
| EID-3330 | Unable to switch to the byte because an overhead channel is present on this byte of the port. | Refer to error message text. |
| EID-3331 | Error applying changes to row. | Refer to error message text. |
| EID-3334 | Cannot change timing parameters on protect port. | You cannot change timing parameters on protect port. |
| EID-3335 | The type of this port cannot be changed: SDH validation check failed. Check if this port is part of a circuit, protection group, SONET DCC, orderwire, or UNI-C interface. | Refer to error message text. |
| EID-3336 | Error on reading a control mode value. | The Control Mode must be retrieved. |
| EID-3337 | Error on setting a set point gain value. | The Gain Set Point must be set. |
| EID-3338 | Error on reading a set-point gain value. | The Gain Set Point must be retrieved. |
| EID-3339 | Error on setting a tilt calibration value. | The tilt calibration must be set. |
| EID-3340 | Error on setting expected wavelength. | The expected wavelength must be set. |
| EID-3341 | Error on reading expected wavelength. | The expected wavelength must be retrieved. |
| EID-3342 | Error on reading actual wavelength. | The actual wavelength must be retrieved. |
| EID-3343 | Error on reading actual band. | The actual band must be retrieved. |
| EID-3344 | Error on reading expected band. | The expected band must be retrieved. |
| EID-3345 | Error on setting expected band. | The expected band must be set. |
| EID-3346 | Error retrieving defaults from the node: {0}. | There was an error retrieving defaults from the specified node. |
| EID-3347 | Cannot load file {0}. | CTC cannot load the specified file. |
| EID-3348 | Cannot load properties from the node. | Refer to error message text. |
| EID-3349 | Cannot save NE Update values to file. | Check your file system for space constraint or any other problem. |
| EID-3350 | Cannot load NE Update properties from the node: | Refer to error message text. |
| EID-3351 | File {0} does not exist. | The specified file does not exist. |
| EID-3352 | Error on setting value at {0}. | There was an error while setting the value at the specified location. |
| EID-3353 | There is no such interface available. | The interface specified is not present in CTC. |
| EID-3354 | Specified endpoint is in use. | Select another endpoint that is not in use. |
| EID-3355 | Specified endpoint is incompatible. | Refer to error message text. |
| EID-3357 | Unable to calculate connections. | Refer to error message text. |
| EID-3358 | Optical link model does not exist for specified interface. | Create an optical linkmodel for the interface, and proceed. |
| EID-3359 | Unable to set optical parameters for the node. | Refer to error message text. |
| EID-3361 | Ring termination is in use. Error deleting ring termination | You cannot delete a ring in use. |

*Table 4-1 Error Messages (continued)*

| Error or Warning ID | Error or Warning Message | Description |
|---|---|---|
| EID-3362 | Error deleting ring termination. | There was an error while deleting ring termination. |
| EID-3363 | No ring terminations selected. | You must select a ring termination. |
| EID-3364 | Error creating ring ID. | There was an error while creating the ring ID. |
| EID-3365 | OSC termination is in use. | Select another optical service channel (OSC) which is not in use. |
| EID-3366 | Unable to delete OSC termination. | There was an error deleting the OSC termination. |
| EID-3370 | No optical link has been selected | You must select an optical link. |
| EID-3371 | Error while calculating automatic optical link list. | Refer to error message text. |
| EID-3372 | Attempt to access an OCH-NC connection that has been destroyed. | CTC destroyed an external attempt to access an optical channel network connection. |
| EID-3375 | Expected span loss must be set. | Refer to error message text. |
| EID-3376 | Unable to retrieve measured span loss. | Refer to error message text. |
| EID-3377 | Wrong interface used. | The interface used for the card is wrong. |
| EID-3378 | Duplicate origination patchcord identifier. | The provisionable patchcord identifier to the patchcord you are attempting to provision is already in use by another patchcord on the origination node. |
| EID-3379 | Duplicate termination patchcord identifier. | The provisionable patchcord identifier to the patchcord you are attempting to provision is already in use by another patchcord on the remote node. |
| EID-3380 | Unable to locate host. | Refer to error message text. |
| EID-3381 | Maximum Frame size must be between {0} and {1} and may be increased in increments of {2}. | The frame size must be in the specified range. This can incremented by the specified value. |
| EID-3382 | Number of credits must be between {0} and {1}. | The number of credits must be between the specified values. |
| EID-3383 | GFP Buffers Available must be between {0} and {1} and may be increased in increments of {2}. | The GFP buffers must be in the specified range. This can incremented by the specified value. |
| WID-3384 | You are about to force the use of Secure Mode for this chassis. You will not be able to undo this operation. OK to continue? | Refer to warning message text. |
| EID-3385 | {0}. Delete circuits, then try again. | Refer to error message text. |
| EID-3386 | Unable to provision transponder mode:<br>{0} | The specified transponder mode canot be provisioned. |

*Table 4-1 Error Messages (continued)*

| Error or Warning ID | Error or Warning Message | Description |
|---|---|---|
| EID-3387 | You must change port{0} to an out-of-service state before changing card parameters. Click Reset to revert the changes. | All the card ports should be changed to out-of-service before changing the parameters. |
| EID-3388 | Unable to change the card mode because the card has circuits. | Refer to error message text. |
| EID-3389 | Error encountered while changing the card mode. | Refer to error message text. |
| EID-3390 | Port is in use. | Refer to error message text. |
| EID-3391 | Unable to change the port rate because the port has been deleted. | You cannot change the port rate of a card that has been deleted. |
| WID-3392 | Could not assign timing reference(s) because - with external timing, only a single protected, or two unprotected timing references per BITS Out may be selected. Please use the “Reset” button and verify the settings. | Refer to warning message text. |
| WID-3393 | Could not assign timing reference(s) because - with line or mixed timing, only a single unprotected timing reference per BITS Out may be selected. Please use the “Reset” button and verify the settings. | Refer to warning message text. |
| EID-3394 | Error refreshing Power Monitoring values. | Refer to error message text. |
| EID-3395 | Invalid Configuration: {0} | CTC encountered an error in IP address, net mask length, or default router, or a restricted IIOP port was selected. |
| EID-3396 | Invalid Configuration: The standby controller card is not a TCC2P card. | The standby controller card should be a TCC2P card. |
| EID-3397 | Wrong version for file {0}. | The specified file is of wrong version. |
| EID-3398 | Cannot delete PPM. | Refer to error message text. |
| EID-3399 | Cannot delete PPM. It has port(s) in use. | Remove the ports coonected to the Pluggable Port Module before it can be deleted. |
| EID-3400 | Unable to switch, force to Primary Facility not allowed. | Refer to error message text. |
| EID-3401 | {0} cannot be provisioned for the port while {1} is enabled. | The relationship between parameters {0} and {1} are such that enabling either one, prevents the provisioning of the other. |
| EID-3402 | Unable to complete the switch request. The protect card is either not present or is not responding. Try again after ensuring that the protect card is present and is not resetting. | Refer to error message text. |
| EID-3403 | Admin state transition has not been attempted on the monitored port. | Refer to error message text. |

*Table 4-1 Error Messages (continued)*

| Error or Warning ID | Error or Warning Message | Description |
|---|---|---|
| EID-3404 | The far end IP address could not be set on the {0} termination. The IP address cannot be:<br>loopback (127.0.0.0/8)<br>class D (224.0.0.0/4)<br>class E (240.0.0.0/4)<br>broadcast (255.255.255.255/32)<br>internal {1} | Refer to error message text. |
| EID-4000 | The {0} ring name cannot be changed now. A {0} switch is active. | You cannot change the ring name because a switch of the same ring type is active. |
| EID-4001 | The {0} ring ID cannot be changed now. A {0} switch is active. | You cannot change the ring ID because a switch of the same ring type is active. |
| WID-4002 | CAUTION: Reverting to an earlier software release may result in TRAFFIC LOSS and loss of connectivity to the node. It may require onsite provisioning to recover.<br>If the node was running 7.0.0 before, reverting will restore the 7.0.0 provisioning, losing any later provisioning. If the node was running some other version, reverting will LOSE ALL PROVISIONING.<br>Also, any FPGA downgrades that occur while reverting might affect traffic.<br>OK to continue? | Refer to warning message text. |
| EID-5000 | Cannot find a valid route for tunnel change request. | Refer to error message text. |
| EID-5001 | Tunnel could not be changed. | Refer to error message text. |
| EID-5002 | Tunnel could not be restored and must be recreated manually. | Refer to error message text. |
| EID-5003 | Circuit roll failure.<br>{0} | Refer to error message text. |
| EID-5004 | There is already one 4F {0} provisioned on the set of nodes involved in {1}. The maximum number of 4F {0} rings has been reached for that node. | There is already one 4F BLSR provisioned on the set of nodes involved in the ring. The maximum number of 4F BLSR rings has been reached for that node. |
| WID-5005 | A non-zero hold-off time can violate switching time standards, and should only be used for a circuit with multiple path selectors. | Refer to warning message text. |
| WID-5006 | Warning: Different secondary {0} node should only be used for DRI or Open-ended path protected circuits. | You should use different secondary end point only for DRI or open-ended path protected circuits. |
| WID-5007 | If you change the scope of this view, the contents of this profile editor will be lost. | Refer to warning message text. |
| WID-5008 | Please make sure all the protection groups are in proper state after the cancellation. | Refer to warning message text. |

*Table 4-1 Error Messages (continued)*

| Error or Warning ID | Error or Warning Message | Description |
|---|---|---|
| WID-5009 | Circuit {0} not upgradable. No {1} capable {2}s are available at node {3}. | No VT capable STSs are available at the node. |
| EID-5010 | Domain name already exists. | Refer to error message text. |
| EID-5011 | Domain name may not exceed {0} characters. | You may have reached the maximum number of charcters. |
| WID-5012 | Software load on {0} does not support the addition of a node to a 1+1protection group. | Refer to warning message text. |
| EID-5013 | {0} doesn't support Bridge and Roll Feature. Please select a different port. | The specified port does not support Bridge and Roll. |
| EID-5014 | An automatic network layout is already in progress, please wait for it to complete for running it again. | You must for the automatic network layout to complete before running it again. |
| WID-5015 | {0} cannot be applied to {1}. | You cannot apply the admin state operation, specified by {0}, to port count, specified by {1}. |
| EID-5016 | An error was encountered while attempting to provision the {0}. {1} | CTC encountered an error while provisioning the card. |
| EID-5017 | Unable to rollback provisioning, the {0} may be left in an INCOMPLETE state and should be manually removed. | You may have to remove the BLSR manually as it was left incomplete. |
| EID-5018 | {0} is {1} node and cannot be added to {2} network. | You cannot add the node {0} of type {1} to the host node of type {2}. This prevents you from hosting both SONET and SDH nodes in the same session. |
| EID-5019 | Manual mode for this equipment does not support an expected string consisting of all null characters. Please change the expected string or the path trace mode. | The path trace mode does not support strings that consist of null characters. You must either change the expected string or the path trace mode. |
| WID-5020 | Unable to transition port state indirectly because the port aggregates low order circuits: if the port state should be changed, edit it directly via port provisioning | Refer to warning message text. |
| EID-5021 | No nodes are selected. Please choose a node. | Refer to error message text. |
| WID-5022 | Warning: Ethergroup circuits are stateless (i.e., always in service).<br>Current state selection of {0} will be ignored. | Refer to warning message text. |
| EID-5023 | Unable to communicate with node.<br>Operation failed. | CTC encountered a network communication error. Connectivity between CTC and the NE was disrupted, either transiently or permanently. |
| EID-5024 | Overhead circuit will not be upgraded. | Refer to error message text. |
| WID-5025 | The path targeted for this switch request is already active. The switch request can be applied, but traffic will not switch at this time. | Refer to warning message text. |

*Table 4-1 Error Messages (continued)*

| Error or Warning ID | Error or Warning Message | Description |
|---|---|---|
| EID-5026 | A 15600 cannot serve as the primary or secondary node in a 4 Fiber {0} circuit. Please change your ring and/or node selections so that a 15600 is not chosen as the primary or secondary node in this 4 Fiber {1} circuit. | Refer to error message text. |
| WID-5027 | The {0} Edit Window for {1} has been closed due to significant provisioning changes. These changes may only be transitory, so you may re-open the {0} Edit Window to view the updated state. | Re-open the BLSR/MS-SPRing edit window to view the updated state of the node. |
| WID-5028 | Warning: This operation should only be used to clean up rolls that are stuck. It may also affect completeness of the circuit. Continue with deletion? | Refer to warning message text. |
| EID-5033 | Unable to load profile. Error decoding characters. | CTC detected an error while decoding characters and could not load the profile. |
| EID-5034 | Unable to load profile. File format error. | CTC detected an error and could not load the profile. |
| EID-5035 | Unable to load profile. File read error. | CTC could not read the file ad hence not able to load the profile. |
| EID-6000 | Platform does not support power monitoring thresholds | Refer to error message text. |
| EID-6001 | One of the XC cards has failures or is missing. | Check whether all the cross connect cards are installed and are working. |
| EID-6002 | One of the XC cards is locked. | Unlock the cross connect card. |
| EID-6003 | Unable to create OSC termination.<br>Ring ID already assigned. | Enter a new ID for the ring and proceed. |
| EID-6004 | Unable to perform a system reset while a BLSR ring is provisioned on the node. | Remove the BLSR ring from the node and proceed with the reset procedure. |
| EID-6005 | Could not assign timing references:<br>- Only two DS1 or BITS interfaces can be specified.<br>- DS1 interfaces cannot be retimed and used as a reference<br>- BITS-2 is not supported on this platform. | Refer to error message text. |
| EID-6006 | Could not assign timing references:<br>- NE reference can only be used if timing mode is LINE.<br>- A BITS reference can only be used if timing mode is not LINE.<br>- A line reference can only be used if timing mode is not EXTERNAL. | Refer to error message text. |
| WID-6007 | Cancelling a software upgrade during standby TSC clock acquisition may result in a traffic outage. | Refer to warning message text. |
| EID-6008 | SF BER and SD BER are not provisionable on the protect line of a protection group. | SF BER and SD BER cannot be provisioned in a protect card as these values are inherited by the protect card or group from the card for which it is offering protection. |

*Table 4-1 Error Messages (continued)*

| Error or Warning ID | Error or Warning Message | Description |
|---|---|---|
| WID-6009 | If Autoadjust GFP Buffers is disabled, GFP Buffers Available must be set to an appropriate value based on the distance between the circuit end points. | Refer to warning message text. |
| WID-6010 | If Auto Detection of credits is disabled, Credits Available must be set to a value less than or equal to the number of receive credits on the connected FC end point. | Refer to warning message text. |
| WID-6011 | Idle filtering should be turned off only when required to operate with non-Cisco Fibre Channel/FICON-over-SONET equipment. | Refer to warning message text. |
| EID-6012 | Could not change the retiming configuration. There are circuits on this port. | You cannot change the timing configuration on this port unless the circuits on this port are deleted. |
| EID-6013 | NTP/SNTP server could not be changed.<br>{1} | Refer to error message text. |
| EID-6014 | Operation failed. The reference state is OOS. | Change the Out-of-service state to Active. |
| EID-6015 | Distance Extension cannot be disabled if the port media type is FICON 1Gbps ISL or FICON 2Gbps ISL. | Refer to error message text. |
| EID-6016 | Card mode cannot be changed to Fibre Channel Line Rate if the port media type is FICON 1Gbps ISL or FICON 2Gbps ISL. | Refer to error message text. |
| EID-6017 | The destination of a {0} route cannot be a node IP address. | A node IP address cannot be the destination for a static route. |
| EID-6018 | The destination of a {0} route cannot be the same as the subnet used by the node. | Refer to error message text. |
| EID-6019 | The destination of a static route cannot be 255.255.255.255 | The network address such as 255.255.255.255 is not valid. Enter a valid address. |
| EID-6020 | The destination of a static route cannot be the loopback network (127.0.0.0/8) | Refer to error message text. |
| EID-6021 | The subnet mask length for a non-default route must be between 8 and 32. | Length of subnet mask must be within the specified range. |
| EID-6022 | The subnet mask length for a default route must be 0. | Refer to error message text. |
| EID-6023 | The destination of a {0} route cannot be an internal network{1}. | The destination of a static route must not be an internal network. |
| EID-6024 | The destination of a {0} route cannot be a class D (224.0.0.0/4) or class E (240.0.0.0/4) address. | The destination of a static route must not be a class D or class E address. |
| EID-6025 | The destination of a {0} route cannot be a class A broadcast address (x.255.255.255/8) | The destination of a static route must not be a class A broadcast address. It should be (xxx.0.0.0). |
| EID-6026 | The destination of a {0} route cannot be a class B broadcast address (x.x.255.255/16) | The destination of a static route must not be a class B broadcast address. |

*Table 4-1 Error Messages (continued)*

| Error or Warning ID | Error or Warning Message | Description |
|---|---|---|
| EID-6027 | The destination of a {0} route cannot be a class C broadcast address (x.x.x.255/24) | The destination of a static route must not be a class C broadcast address. |
| EID-6028 | The destination of a {0} route cannot be the subnet broadcast address associated with a node IP address. | The destination of a static route must not be a subnet broadcast address of a node IP. |
| EID-6029 | The next hop of a static route cannot be the same as the destination of the route or an internal network{0}. | Static route must have the default route as the next hop, and not destination of the route or internal network. |
| EID-6030 | The next hop of a static default route must be the provisioned default router. | The default route is selected for networks that do not have a specific route. |
| EID-6031 | No more static routes can be created. | You have reached the maximum number of static routes. |
| EID-6032 | This static route already exists. | Refer to error message text. |
| EID-6033 | Previous operation is still in progress. | Another operation is in progress. You must try after sometime. |
| EID-6035 | Parent entity does not exist. | Refer to error message text. |
| EID-6036 | Parent PPM entity does not exist. | Create a parent entity for PPM. |
| EID-6037 | Equipment type is not supported. | CTC does not support this equipment. |
| EID-6038 | Invalid PPM port. | Refer to error message text. |
| EID-6039 | Card is part of a regeneration group. | Select another card. |
| EID-6040 | Out of memory. | Refer to error message text. |
| EID-6041 | Port is already present. | Refer to error message text. |
| EID-6042 | Port is used as timing source. | Choose another port as the selected port is being used as timing source. |
| EID-6043 | DCC or GCC is present. | Refer to error message text. |
| EID-6044 | Card or port is part of protection group. | Refer to error message text. |
| EID-6045 | Port has overhead circuit(s). | Refer to error message text. |
| EID-6046 | G.709 configuration is not compatible with data rate. | Refer to error message text. |
| EID-6047 | Port cannot be deleted because its service state is OOS-MA,LPBK&MT. | To delete the port, you must change the port state to OOS-DSBLD. |
| EID-6048 | {0} is {1}. | Trunk port is in the wrong state to carry out the action. |
| EID-6049 | Mode {0} is not supported. | CTC does not support the mode of operation requested on the card. |
| EID-6050 | Some {0} terminations were not {1}d.<br>{2} | Refer to error message text. |
| WID-6051 | All {0} terminations were {1}d successfully.<br>{2} | Refer to warning message text. |
| EID-6052 | The authentication key can not be blank. | Enter an authentication key. |

*Table 4-1 Error Messages (continued)*

| Error or Warning ID | Error or Warning Message | Description |
|---|---|---|
| EID-6053 | No more SNMP trap destinations can be created. | You have reached the maximum number of SNMP trap destinations. |
| EID-6054 | {0} is not a valid IP address for an SNMP trap destination. | The IP address specified is invalid as the receiver of SNMP traps |
| EID-6055 | The IP address is already in use. | Refer to error message text. |
| EID-6056 | Invalid SNMP trap destination. {0} | The specified SNMP trap destination is invalid. Choose another destination. |
| WID-6057 | Changing the card mode will result in an automatic reset. | Refer to warning message text. |
| EID-6058 | Max number of GRE tunnels exceeded. | Refer to error message text. |
| EID-6059 | The specified GRE tunnel already exists! | Specify another GRE tunnel. |
| EID-6060 | Cannot {0} GRE tunnel entry:<br>{1}. | Refer to error message text. |
| EID-6061 | Error deleting GRE tunnel entry. | CTC encountered an error while deleting the GRE tunnel entry. |
| EID-6062 | Selected GRE tunnel does not exist. | Create a GRE tunnel and proceed. |
| EID-6063 | Selected router does not exist. | Create a router and proceed. |
| EID-6064 | MAA address list is full. | Refer to error message text. |
| EID-6065 | Selected area address is duplicated. | Enter another area address. |
| EID-6066 | Primary area address can not be removed. | Refer to error message text. |
| EID-6067 | Selected area address does not exist. | Choose another area address. |
| EID-6068 | The GRE NSEL may not be modified while there are GRE Tunnel Routes provisioned. | You can not change the NSEL address if there are tunnels provisioned. |
| EID-6069 | The node is currently in ES mode. Only router #1 may be provisioned. | An End System needs only one provisioned router. |
| EID-6070 | No router selected. | Select a router. |
| EID-6071 | Cannot flush TARP data cache. | You cannot flush the cache in the Tunnel identifier Address Resolution Protocol (TARP) state. |
| EID-6072 | Cannot add TARP data cache entry:<br>{0} | You cannot add the specified cache entry. |
| WID-6073 | TARP request has been initiated.<br>Try refreshing TARP data cache later. | Refer to warning message text. |
| EID-6074 | End System mode only supports one subnet. | Refer to error message text. |
| EID-6075 | Trying to remove MAT entry that does not exit. | CTC is removing the non-existant MAT entry. |
| EID-6076 | Cannot {0} TARP manual adjacency entry:<br>{1} | CTC can not add the specified adjacency entry for reasons unknown. |
| EID-6077 | Area address shall be 1 to 13 bytes long. | Area address should not be more than 13 characters. |

*Table 4-1 Error Messages (continued)*

| Error or Warning ID | Error or Warning Message | Description |
|---|---|---|
| EID-6078 | TDC entry with TID {0} does not exist in the table. | The specified Tunnel Identifier does not exist. |
| EID-6079 | Unable to remove TDC entry with TID {0}.<br>Please verify that TARP is enabled. | You must enable TARP inorder to remove the TDC entry. |
| WID-6080 | Router #{0} does not have an area address in common with router #1. Switching from IS L1/L2 to IS L1 in this case will partition your network. | Refer to warning message text. |
| EID-6081 | The limit of 10 RADIUS server entries has been reached. | CTC does not allow more than 10 RADIUS servers. |
| EID-6082 | {0} cannot be empty. | The Shared Secrets field should not be empty. |
| EID-6083 | The entry you selected for editing has been altered by other. Changes cannot be committed. | Refer to error message text. |
| EID-6084 | The RADIUS server entry already exists. | Specify another RADIUS server entry. |
| WID-6085 | Disabling shell access will prevent Cisco TAC from connecting to the vxWork shell to assist users. | Refer to warning message text. |
| EID-6086 | Cannot change card. Card resources are in use. | The card you are trying to remove is being used. Cannot change the card. |
| EID-6087 | Cannot change card. The new card type is invalid or incompatible. | Refer to error message text. |
| EID-6088 | This line cannot be put into loopback while it is in use as a timing source | Refer to error message text. |
| EID-6089 | Interface not found. {0} | CTC cannot find the specified interface. |
| EID-6090 | Interface type not valid for operation. {0} | Choose another interface. |
| EID-6091 | The interface's current state prohibits this operation. {0} | The port is in an invalid state to set loopback. |
| EID-6092 | Operation prohibited for this interface. {0} | CTC does not allow this operation for the specified interface. |
| EID-6093 | Max number of Tarp Data Cache entry exceeded. | You have exceeded the allowed number of characters. |
| EID-6094 | Max number of Manual Adjacency Table entry exceeded. | Refer to error message text. |
| EID-6095 | Invalid Ais/Squelch mode. | Refer to error message text. |
| EID-6096 | Default GRE tunnel route is only allowed on a node without a default static route and a default router of 0.0.0.0 | Refer to error message text. |
| EID-6097 | The authorization key does not comply with IOS password restrictions.<br>{0} | Specify another authorization key. |
| EID-6098 | Default static route is not allowed when default GRE tunnel exists | Refer to error message text. |
| EID-6099 | You cannot create a subnet on a disabled router. | Create the subnet on an active router. |

*Table 4-1 Error Messages (continued)*

| Error or Warning ID | Error or Warning Message | Description |
|---|---|---|
| WID-6100 | Disabling a router that has a provisioned subnet is not recommended. | Refer to warning message text. |
| EID-6101 | The MAT entry already exists. | Refer to error message text. |
| WID-6102 | The new card has less bandwidth than the current card. Circuits using VT15 and higher will be deleted. | Refer to warning message text. |
| EID-6103 | The TDC entry already exists. | Specify another entry for TARP Data Cache. |
| EID-6104 | APC ABORTED. | Automatic Power Control is aborted. |
| EID-6105 | The 'Change Card' command is valid for MRC cards only when port 1 is the sole provisioned port. | Refer to error message text. |
| EID-6106 | To delete all RADIUS server entries, RADIUS authentication must be disabled. | Disable Radius authentication and proceed. |
| EID-6107 | The node failed to restart the TELNET service on the selected port. Try using another unreserved port that is not being used within the following ranges:<br>23, 1001-9999. | Refer to error message text. |
| EID-6108 | There is an active TELNET session. | Restart a TELNET session. |

1. EID-3159 can appear if you attempt to perform another switching operation within a certain time interval. This interval is an algorithm of three seconds per working card in the protection group. The maximum interval is 10 seconds.


# Performance Monitoring

Performance monitoring (PM) parameters are used by service providers to gather, store, set thresholds for, and report performance data for early detection of problems. In this chapter, PM parameters and concepts are defined for transponder, muxponder, and dense wavelength division multiplexing (DWDM) cards in the Cisco ONS 15454 including optical amplifier, multiplexer, demutiplexer, optical add/drop multiplexer (OADM), and optical service channel (OSC) cards.

**Note** Unless otherwise specified, “ONS 15454” refers to both ANSI and ETSI shelf assemblies.

For information about enabling and viewing PM values, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Chapter topics include:



**Note** For additional information regarding PM parameters, refer to ITU G.826, ITU-T G.8021, ITU G.709, Telcordia documents GR-1230-CORE, GR-820-CORE, GR-499-CORE, and GR-253-CORE, and the ANSI T1.231 document entitled *Digital Hierarchy - Layer 1 In-Service Digital Transmission Performance Monitoring*.

# 5.1 Threshold Performance Monitoring

Thresholds are used to set error levels for each PM parameter. You can set individual PM threshold values from the Cisco Transport Controller (CTC) card view Provisioning tab. For procedures about provisioning card thresholds, such as line and path thresholds, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

During the accumulation cycle, if the current value of a PM parameter reaches or exceeds its corresponding threshold value, a threshold crossing alert (TCA) is generated by the node and is displayed by CTC. TCAs provide early detection of performance degradation. When a threshold is crossed, the node continues to count the errors during a given accumulation period. If zero is entered as the threshold value, generation of TCAs is disabled but performance monitoring continues.

**Note** Due to limitations of memory and the number of TCAs generated by different platforms, you can manually add or modify the following two properties to the platform property file (CTC.INI for Windows and .ctcrc for UNIX) to fit the need:

- **ctc.15***xxx***.node.tr.lowater=***yyy* (where *xxx* is platform and *yyy* is the number of the lowater mark. The default lowater mark is 25.)
- **ctc.15***xxx***.node.tr.hiwater=***yyy* (where *xxx* is platform and *yyy* is the number of the hiwater mark. The default hiwater mark is 50.)

If the number of the incoming TCA is greater than the hiwater mark, it will keep the latest lowater mark and discard older ones.

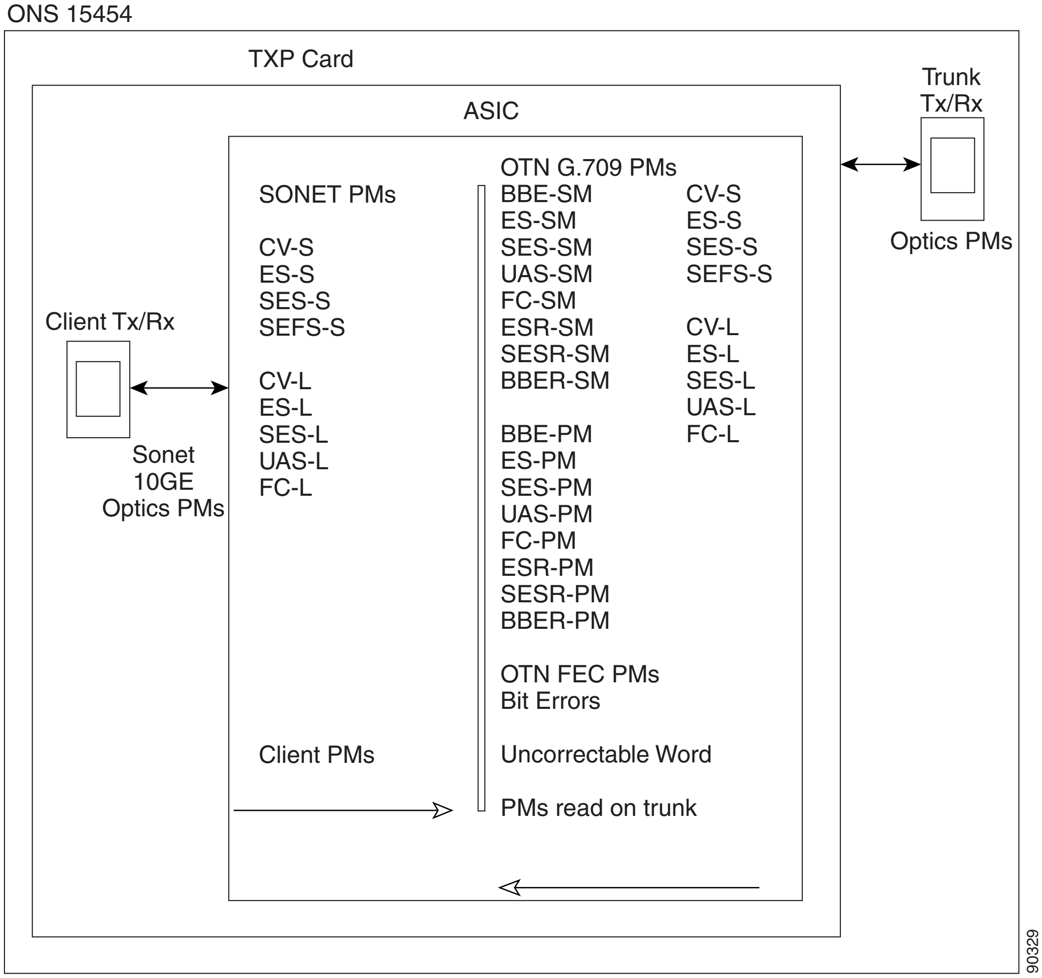
Change the threshold if the default value does not satisfy your error monitoring needs. For example, customers with a critical OC192/STM64 transponder installed for 911 calls must guarantee the best quality of service on the line; therefore, they lower all thresholds on the client side so that the slightest error raises a TCA.

# 5.2 Transponder and Muxponder Card Performance Monitoring

This section lists PM parameters for transponder cards (TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, and TXP_MR_10E), and muxponder cards (MXP_2.5G_10G, MXP_25G_10E, MXP_MR_2.5G, and MXPP_MR_2.5G). The transponder and muxponder PM parameters are divided into Optics PM, Payload PM, and OTN PM tabs. The tabs displayed vary depending on the card installed. For more information, see the "5.2.1 Optics PM Window" section on page 5-4, the "5.2.2 Payload PM Window" section on page 5-5, or the "5.2.3 OTN PM Window" section on page 5-11.

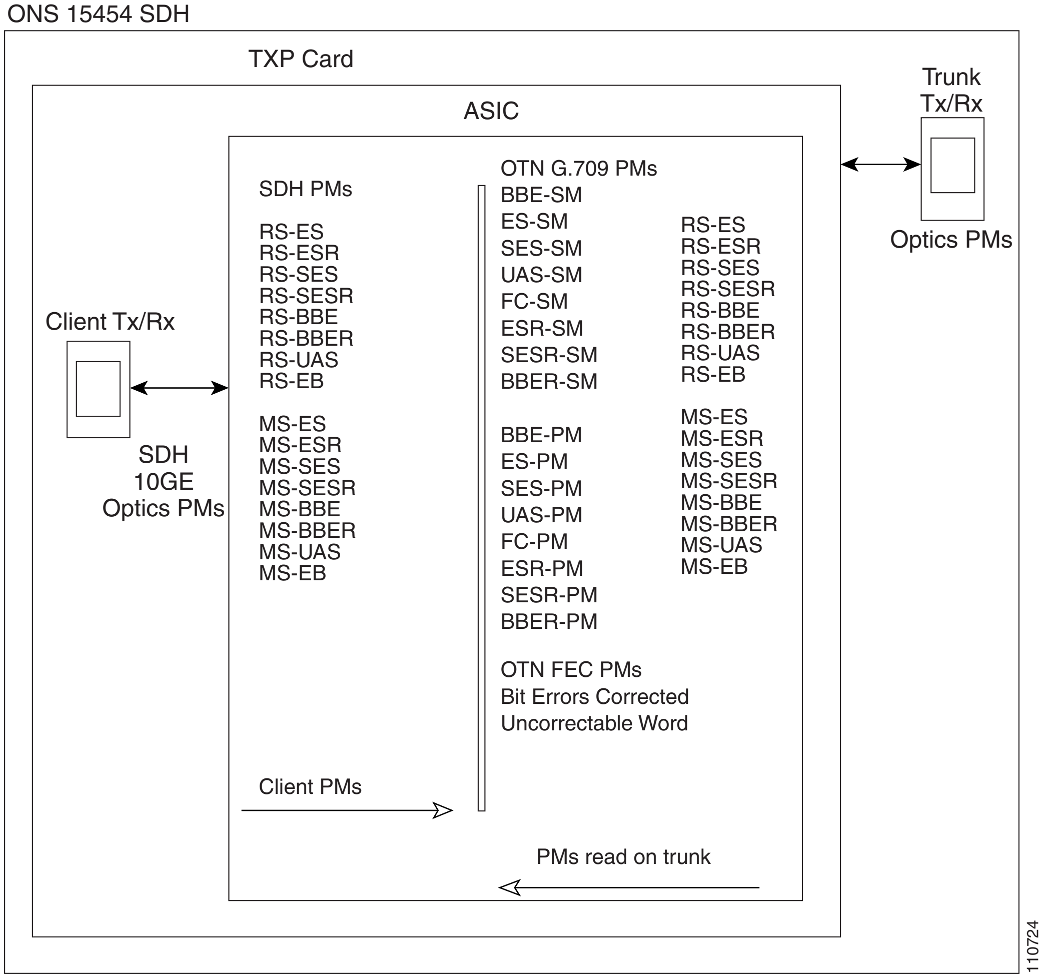
For ONS 15454 ANSI nodes, Figure 5-1 shows where overhead bytes detected on the application-specific integrated circuits (ASICs) produce PM parameters for the TXP_MR_10G card. The remaining transponder and muxponder cards perform similarly to this illustration.

*Figure 5-1 ONS 15454 ANSI Node PM Read Points for TXP_MR_10G Card*




For ONS 15454 ETSI nodes, Figure 5-2 shows where overhead bytes detected on the ASICs produce PM parameters for the TXP_MR_10G card. The remaining transponder and muxponder cards perform similarly to this illustration.

*Figure 5-2 ONS 15454 ETSI Node PM Read Points on TXP_MR_10G Cards*




## 5.2.1 Optics PM Window

The Optics PM window lists parameters at the trunk and client side for all transponder and muxponder cards. The Optics PM window provides buttons to change the statistical values shown. The Refresh button manually refreshes statistics. Auto-Refresh sets a time interval at which automatic refresh occurs. In the Historical PM subtab, the Clear button sets the values on the card to zero. All counters on the card are cleared. The Help button activates context sensitive help. Table 5-1 lists the trunk-side and client-side optics PM parameters.

*Table 5-1 Trunk-Side and Client-Side Optics PM Parameters*

| Trunk-Side/Client-Side Optics PM Parameters | Definition |
|---|---|
| Laser Bias (Avg,%) | Average Laser Bias Current (Laser Bias Avg) is the average percentage of laser bias current during the PM time interval. |
| Laser Bias (Max,%) | Maximum Laser Bias Current (Laser Bias Max) is the maximum percentage of laser bias current during the PM time interval. |
| Laser Bias (Min,%) | Minimum Laser Bias Current (Laser Bias Min) is the minimum percentage of laser bias current during the PM time interval. |
| Link Status | Indicates if the Fibre Channel link is receiving a valid Fibre Channel signal (carrier) from the attached Fibre Channel device. Up means present, and down means not present. |
| Rx Optical Pwr (Min,dBm) | Minimum Receive Optical Power (Rx Optical Pwr Min, dBm) is the minimum received optical power during the PM time interval. |
| Rx Optical Pwr (Avg,dBm) | Average Receive Optical Power (Rx Optical Pwr Avg, dBm) is the average received optical power during the PM time interval. |
| Rx Optical Pwr (Max,dBm) | Maximum Receive Optical Power (Rx Optical Pwr Max, dBm) is the maximum received optical power during the PM time interval. |
| Tx Optical Pwr (Min,dBm)[1] | Minimum Transmit Optical Power (Tx Optical Pwr Min, dBm) is the minimum optical power transmitted during the PM time interval. |
| Tx Optical Pwr (Avg,dBm)[1] | Average Transmit Optical Power (Tx Optical Pwr Avg, dBm) is the average optical power transmitted during the PM time interval. |
| Tx Optical Pwr (Max,dBm)[1] | Maximum Transmit Optical Power (Tx Optical Pwr Max, dBm) is the maximum optical power transmitted during the PM time interval. |

1. On the trunk side, this PM is not available for the following cards: TXP_MR_2.5G, TXPP_MR_2.5G, MXP_MR_2.5G, and MXPP_MR_2.5G.

## 5.2.2 Payload PM Window

The Payload PM window subtabs change depending on the card provisioning. For more information about provisioning TXP and MXP cards, refer to the "Provision Transponder and Muxponder Cards" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*. Possible Payload PM subtabs are: SONET, SDH, Statistics, Utilization, and History. The following buttons function the same on all of the tabs. Not all tabs have all of these buttons.

- The Refresh button manually refreshes statistics.
- Auto-Refresh sets a time interval at which automatic refresh occurs.
- The Baseline button resets the displayed statistics values to zero.
- (Statistics window only) The Clear button allows you to set the values to zero for displayed statistics, all statistics for a port, and all statistics for all optical ports on a card.

- The Help button activates context sensitive help.

For a list of the payload PM provisioning options for all transponder and muxponder cards, refer to the "Provision the Optical Line Rate" task in the *Cisco ONS 15454 DWDM Installation and Operations Guide*. The options selected in the Provisioning tab can affect the parameters displayed in the Performance > Payload PM tab.

Table 5-2 lists the PM parameter types that appear when a particular port type is provisioned for a transponder or muxponder card.

*Table 5-2 Transponder and Muxponder Port Type PM Provisioning Options*

| If this Port Type is Provisioned[1] | The Following PM Types are Activated[2] |
|---|---|
| SONET/SDH (including 10G Ethernet WAN Phy)<br>OC3/STM1<br>OC12/STM4<br>OC48/STM16 | SONET or SDH PMs |
| 10G Ethernet LAN Phy<br>10G FiberChannel<br>ONE_GE<br>FC1G<br>FC2G<br>FC1G ISL<br>FC2G ISL<br>FICON1G<br>FICON2G<br>FICON1G ISL<br>FICON2G ISL<br>ISC COMPAT<br>ISC PEER | Full remote monitoring (RMON) statistics |
| ESCON<br>DV6000<br>SDI_D1_VIDEO<br>HDTV<br>PASS_THRU<br>ETR_CLO | Payload PMs are not applicable to 2R port types. |

1. The port type is provisioned from card view on the Provisioning > Pluggable Port Modules tab. For pluggable port module (PPM) provisioning procedures, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.
2. Performance monitoring parameters are displayed from the card view on the Performance tab.

### 5.2.2.1 Payload PM SONET Window

Table 5-3 lists SONET layer near-end and far-end PM parameters listed in the card view on the Performance > Payload PM > SONET tab. SONET layer PMs are available when the client type is set to OC3, OC12, or OC48 on the TXP_MR_2.5G or when OC192 is set on the TXP_MR_10G or TXP_MR_10E on ONS 15454 SONET nodes. OC48 trunk PMs are available on MXP_MR_2.5G and MXPP_MR_2.5G cards on ONS 15454 SONET nodes. OC48 client PMs are available on MXP_2.5G_10G and MXP_2.5G_10E cards on ONS 15454 SONET nodes. For PM definitions, see Table 5-28 on page 5-24.

*Table 5-3 ONS 15454 SONET Layer Far-End and Near-End PMs*

| SONET Layer Far-End (FE)[1, 2] | SONET Layer Near-End[1, 2] | Note |
|---|---|---|
| CV-LFE<br>ES-LFE<br>FC-LFE<br>SES-LFE<br>UAS-LFE | CV-L<br>CV-S<br>ES-L<br>ES-S<br>FC-L<br>SES-L<br>SES-S<br>SEF-S<br>UAS-L | Applicable standard is Telcordia GR-253. |

1. Applicable to optical channel (OCH) and Client (CLNT) facilities.
2. For MXP_MR_2.5G and MXPP_MR_2.5G cards, these parameters are shown in the Performance > Payload PM > SONET PM tabs in the card view.

### 5.2.2.2 Payload PM SDH Window

Table 5-4 lists SDH layer near-end and far-end PM parameters listed in the card view on the Performance > Payload PM > SDH tab. SDH layer PMs are available when the client type is set to STM1, STM4, or STM16 on the TXP_MR_2.5G, or when STM64 is set on the TXP_MR_10G/TXP_MR_10E on ONS 15454 SDH nodes. STM16 trunk PMs are available on MXP_MR_2.5G and MXPP_MR_2.5G cards on ONS 15454 SDH nodes. STM16 client PMs are available on MXP_2.5G_10G and MXP_2.5G_10E cards on ONS 15454 SDH nodes. For PM definitions, see Table 5-29 on page 5-25.

*Table 5-4 ONS 15454 SDH Node SDH Layer FE and NE PMs*

| SDH Far-End[1, 2] | SDH Near-End[1, 2] |
|---|---|
| MS-BBE<br>MS-BBER<br>MS-EB<br>MS-ES<br>MS-ESR<br>MS-SES<br>MS-SESR<br>MS-UAS | RS-BBE<br>RS-BBER<br>RS-EB<br>RS-ES<br>RS-ESR<br>RS-SES<br>RS-SESR<br>RS-UAS<br>MS-BBE<br>MS-BBER<br>MS-EB<br>MS-ES<br>MS-ESR<br>MS-SES<br>MS-SESR<br>MS-UAS |

1. Applicable to OCH and CLNT facilities.
2. For MXP_MR_2.5G and MXPP_MR_2.5G cards, these parameters are shown in the Performance > Payload PM > SDH PM tabs in the card view.

### 5.2.2.3 Payload PM Statistics Window

Table 5-5 lists the 10 Gigabit Ethernet (10 GE) payload statistics that are available on the TXP_MR_10G and TXP_MR_10E cards. PPM provisioning must be completed under the card view Provisioning > Pluggable Port Modules tab for 10 GE to be enabled. For PPM provisioning procedures, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*. The parameters are listed under card view on the Performance > Payload PM > Statistics tab. For 10 GE payload definitions, see Table 5-26 on page 5-20.

**Note** Utilization PMs are also available per port.

*Table 5-5 Full RMON Statistics on TXP_MR_10G and TXP_MR_10E cards*

| Full RMON Statistics | |
|---|---|
| dot3StatsFCSErrors<br>dot3StatsFrameTooLong<br>ifInBroadcastPkts<br>ifInErrors<br>ifInErrorsBytePkts<br>ifInFramingErrorPkts<br>ifInJunkInterPkts<br>ifInMulticastPkts<br>ifInOctets<br>ifOutBroadcastPkts<br>ifOutMulticastPkts<br>ifOutOctets<br>rxTotalPkts<br>Time Last Cleared<br>txTotalPkts | etherStatsBroadcastPkts<br>etherStatsCRCAlignErrors<br>etherStatsFragments<br>etherStatsJabbers<br>etherStatsMulticastPkts<br>etherStatsOctets<br>etherStatsOversizePkts<br>etherStatsPkts64Octets<br>etherStatsPkts65to127Octets<br>etherStatsPkts128to255Octets<br>etherStatsPkts256to511Octets<br>etherStatsPkts512to1023Octets<br>etherStatsPkts1024to1518Octets<br>etherStatsUndersizePkts<br>rxControlFrames<br>rxPauseFrames<br>rxUnknownOpcodeFrames |

Table 5-6 lists the payload PM parameters that are available on the TXP_MR_2.5G and the TXPP_MR_2.5G cards when the ONE_GE or FC1G client type is enabled. For PPM provisioning procedures, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For payload definitions, see the "5.4 Optics and 8b10b PM Parameter Definitions" section on page 5-17 and the "5.6 Full RMON Statistics PM \ Parameter Definitions" section on page 5-20.

**Note** Payload PM is not available for the 2FC client type.

*Table 5-6 Gigabit Ethernet (GE) or Fibre Channel (FC) Payload PMs for the TXP_MR_2.5G and TXPP_MR_2.5G Cards*

| GE or FC Payload Performance Parameters |
|---|
| 8b/10bDataOrderedSets<br>8b/10bIdleOrderedSets<br>8b/10bNonIdleOrderedSets<br>8b/10bStatsEncodingDispErrors<br>ifInErrors<br>rxTotalPkts |

Table 5-7 lists the payload PM parameters that are available on the MXP_MR_2.5G and the MXPP_MR_2.5G cards when the ONE_GE or the FC1G client type is enabled. For PPM provisioning procedures, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For payload definitions, see the "5.4 Optics and 8b10b PM Parameter Definitions" section on page 5-17 and the "5.6 Full RMON Statistics PM \ Parameter Definitions" section on page 5-20.

*Table 5-7 ONE_GE or FC1G Payload PMs for the MXP_MR_2.5G and MXP_MR_2.5G Cards*

| ONE_GE or FC1G Payload Performance Parameters |
|---|
| 8b10bInvalidOrderedSets<br>8b10bStatsEncodingDispErrors<br>ifInDiscards<br>ifInErrors<br>ifInOctets<br>ifOutDiscards<br>ifOutOctets<br>mediaIndStatsRxFramesBadCRC<br>mediaIndStatsRxFramesTooLong<br>mediaIndStatsRxFramesTruncated<br>mediaIndStatsTxFramesBadCRC<br>rxTotalPkts<br>txTotalPkts |

Table 5-8 lists the FC client-side payload PM parameters. FC payload PMs are available on the FC port on both the MXP_MR_2.5G and the MXPP_MR_2.5G cards when the FC1G client type is enabled. For PPM provisioning procedures, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For payload definitions, see the "5.6 Full RMON Statistics PM \ Parameter Definitions" section on page 5-20.

*Table 5-8 FC1G Payload PMs on the Client Side*

| FC1G Payload PMs on the Client Port |
|---|
| fcStatsLinkRecoveries<br>fcStatsRxCredits<br>fcStatsTxCredits<br>fcStatsZeroTxCredits<br>gfpStatsRoundTripLatencyUSec<br>gfpStatsRxDistanceExtBuffers<br>gfpStatsTxDistanceExtBuffers |

Table 5-9 lists the Transparent Generic Framing Procedure (GFP-T) payload PMs. The GFP-T payload PMs are available on the GFP port on both the MXP_MR_2.5G and the MXPP_MR_2.5G cards when the ONE_GE or the 1 FC client type is enabled. GFP-T payload PMs are also available on the client port on both the MXP_MR_2.5G and the MXPP_MR_2.5G cards when the 1 FC client type is enabled. For PPM provisioning procedures, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For payload definitions, see the "5.6 Full RMON Statistics PM \ Parameter Definitions" section on page 5-20.

*Table 5-9 GFP-T Payload PMs*

| GFP-T Payload PMs on the GFP Port |
|---|
| gfpStatsCSFRaised<br>gfpStatsLFDRaised<br>gfpStatsRxCRCErrors<br>gfpStatsRxMBitErrors<br>gfpStatsRxSBitErrors<br>gfpStatsRxTypeInvalid |

#### 5.2.2.4 MXP_MR_2.5G/MXPP_MR_2.5G Payload Utilization Window

The Payload PM Utilization window in the card view Performance > Utilization tab shows the percentage of transmit (Tx) and receive (Rx) line bandwidth used by the ports during consecutive time segments. This tab cannot be viewed unless the appropriate PPM port type is provisioned. For PPM provisioning procedures, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*. The Utilization window provides an Interval list that enables you to set time intervals of 15 minutes or 1 day. Line utilization is calculated with the following formulas:

Rx = (inOctets + inPkts * 20) * 8 / 100% interval * maxBaseRate

Tx = (outOctets + outPkts * 20) * 8 / 100% interval * maxBaseRate

The interval is defined in seconds. The maxBaseRate is defined by raw bits per second in one direction for the port (that is, 1 Gbps). The maxBaseRate for MXP_MR_2.5G and MXPP_MR_2.5G cards is shown for the ONS 15454 nodes in Table 5-10.

*Table 5-10 maxBaseRate for STS and VC Circuits*

| STS/VC | maxBaseRate |
|---|---|
| STS-1/VC3 | 51840000 |
| STS-3c/VC4 | 155000000 |
| STS-6c/VC4-2c | 311000000 |
| STS-12c/VC4-4c | 622000000 |

**Note** Line utilization numbers express the average of ingress and egress traffic as a percentage of capacity.

### 5.2.2.5 Payload History Window

The Payload PM History window in the card view Performance > History tab lists past statistics for the previous time intervals. This tab cannot be viewed unless the appropriate PPM port type is provisioned. For PPM provisioning procedures, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*. Depending on the selected time interval, the History window displays the statistics for each port for the number of previous time intervals as shown in Table 5-11.

***Table 5-11 History Statistics per Time Interval***

| Time Interval | Number of Intervals Displayed |
|---|---|
| 15 minutes | 32 (current and previous) |
| 1 day (24 hours) | 2 (current and previous) |

## 5.2.3 OTN PM Window

The OTN tab has a G.709 PM subtab and an FEC subtab. Both subtabs provide buttons to change the statistical values shown in the Performance tab. The Refresh button manually refreshes statistics. Auto-Refresh sets a time interval at which automatic refresh occurs. The Baseline button resets the displayed statistics values to zero. The Statistics window also has a Clear button. The Clear button sets the values on the card to zero. All counters on the card are cleared. The Help button activates context sensitive help. For more information about provisioning optical transport network (OTN) settings, refer to the “Change OTN Settings for TXP_MR_10G and TXP_MR_10E Cards” task or the “Change OTN Settings for MXP_2.5G_10G and MXP_2.5G_10E Cards” task in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Table 5-12 lists the OTN PM provisioning options for all transponder and muxponder cards. The options selected in the Provisioning tab affects the parameters displayed in the Performance > OTN PM tab.

***Table 5-12 Transponder and Muxponder PM Provisioning Options***

| Card | OTN Provisioning[1] |
|---|---|
| MXPP_MR_2.5G | — |
| MXP_2.5G_10E | G.709<br>FEC<br>FEC Thresholds |
| MXP_2.5G_10G | G.709<br>FEC<br>FEC Thresholds |
| MXP_MR_2.5G | — |
| TXPP_MR_2.5G | G.709<br>FEC<br>FEC Thresholds |
| TXP_MR_10E | G.709<br>FEC<br>FEC Thresholds |

*Table 5-12 Transponder and Muxponder PM Provisioning Options (continued)*

| Card | OTN Provisioning[1] |
|---|---|
| TXP_MR_10G | G.709<br>FEC<br>FEC Thresholds |
| TXP_MR_2.5G | G.709<br>FEC<br>FEC Thresholds |

1. OTN provisioning is performed from card view on the Provisioning > OTN > OTN Lines, G.709 Thresholds, and FEC Thresholds tabs.

Table 5-13 lists the OTN trunk-side PM parameters listed on the G.709 tab. OTN PMs are available when ITU G.709 is enabled from the card view Provisioning > OTN > OTN Line tab. OTN PMs are not available on MXP_MR_2.5G and MXPP_MR_2.5G cards. For ITU G.709 section and path monitoring PM definitions, see the "5.5 ITU G.709 and ITU-T G.8021 Trunk-Side PM Parameter Definitions" section on page 5-19.

*Table 5-13 ITU G.709 OTN Trunk-Side PMs*

| OTN Layer (Near End and Far End)[1] | Note |
|---|---|
| BBE-SM<br>BBER-SM<br>ES-SM<br>ESR-SM<br>FC-SM<br>SES-SM<br>SESR-SM<br>UAS-SM | ITU G.709 standard section monitoring<br>ITU-T G.8021 |
| BBE-PM<br>BBER-PM<br>ES-PM<br>ESR-PM<br>FC-PM<br>SES-PM<br>SESR-PM<br>UAS-PM | ITU G.709 standard path monitoring<br>ITU-T G.8021 |

1. Applicable to OCH facility.

Table 5-14 lists the forward error correction (FEC) PM parameters. FEC PMs are available when ITU-T G.709 is enabled and FEC is set to standard or enhanced. These parameters are provisioned from the card view Provisioning > OTN > OTN Line tab. FEC PMs are not available on MXP_MR_2.5G and MXPP_MR_2.5G cards. For PM definitions, see the "5.7 FEC PM Parameter Definitions" section on page 5-23.

*Table 5-14 FEC OTN Trunk-Side PMs*

| FEC Trunk-Side PMs | FEC (Near End)[1] |
|---|---|
| Bit Errors | BIT-EC |
| Uncorrectable Words | UNC-WORDS |

1. Applicable to OCH facility.

Table 5-15 lists ONS 15454 optics and 8b10b PM parameters. For ONS 15454 optics and 8b10b definitions, see the "5.4 Optics and 8b10b PM Parameter Definitions" section on page 5-17.

*Table 5-15 ONS 15454 Optics and 8b10b PMs*

| Optics (Near End)[1, 1] | 8B10B (Near End)[2] |
|---|---|
| LBCL-AVG<br>LBCL-MAX<br>LBCL-MIN<br>OPT-AVG<br>OPT-MAX<br>OPT-MIN<br>OPR-AVG<br>OPT-MAX<br>OPR-MIN | CGV<br>DCG<br>IOS<br>IPC<br>NIOS<br>VPC |

1. The TXP_MR_2.5G and TXPP_MR_2.5G card Enterprise System Connection (ESCON) payload does not support optics PMs on the client port due to Small Form-factor Pluggable (SFP)-imposed restrictions.
2. Applicable to TXP_MR_2.5G and TXPP_MR_2.5G cards only.

# 5.3 DWDM Card Performance Monitoring

The following sections define PM parameters and definitions for the ONS 15454 OPT-PRE, OPT-BST, 32MUX-O, 32DMX-O, 32DMX, 4MD-xx.x, AD-1C-xx.x, AD-2C-xx.x, AD-4C-xx.x, AD-1B-xx.x, AD-4B-xx.x, OSCM, OSC-CSM, and 32WSS DWDM cards.

## 5.3.1 Optical Amplifier Card Performance Monitoring Parameters

The PM parameters for the OPT-PRE and OPT-BST cards are listed Table 5-16. For ONS 15454 optics definitions, see the "5.4 Optics and 8b10b PM Parameter Definitions" section on page 5-17.

*Table 5-16 Optical PM Parameters for OPT-PRE and OPT-BST Cards*

| Optical Line | Optical Amplifier Line |
|---|---|
| OPT | OPR |

## 5.3.2 Multiplexer and Demultiplexer Card Performance Monitoring Parameters

The PM parameters for the 32MUX-O, 32WSS, 32DMX, and 32DMX-O cards are listed in Table 5-17. For ONS 15454 optics definitions, see the "5.4 Optics and 8b10b PM Parameter Definitions" section on page 5-17.

*Table 5-17 Optical PM Parameters for 32MUX-O, 32WSS, 32DMX and 32DMX-O Cards*

| Optical Channel | Optical Line |
|---|---|
| OPR | OPT |

## 5.3.3 4MD-xx.x Card Performance Monitoring Parameters

The PM parameters for the 4MD-xx.x cards are listed in Table 5-18. For ONS 15454 optics definitions, see the "5.4 Optics and 8b10b PM Parameter Definitions" section on page 5-17.

*Table 5-18 Optical PM Parameters for 4MD-xx.x Cards*

| Optical Channel | Optical Band |
|---|---|
| OPR | OPT |

## 5.3.4 OADM Channel Filter Card Performance Monitoring Parameters

The PM parameters for the AD-1C-xx.x, AD-2C-xx.x, and AD-4C-xx.x cards are listed in Table 5-19. For ONS 15454 optics definitions, see the "5.4 Optics and 8b10b PM Parameter Definitions" section on page 5-17.

*Table 5-19 Optical PM Parameters for AD-1C-xx.x, AD-2C-xx.x, and AD-4C-xx.x Cards*

| Optical Channel | Optical Line |
|---|---|
| OPR | OPT |

## 5.3.5 OADM Band Filter Card Performance Monitoring Parameters

The PM parameters for the AD-1B-xx.x and AD-4B-xx.x cards are listed in Table 5-20. For ONS 15454 optics definitions, see the "5.4 Optics and 8b10b PM Parameter Definitions" section on page 5-17.

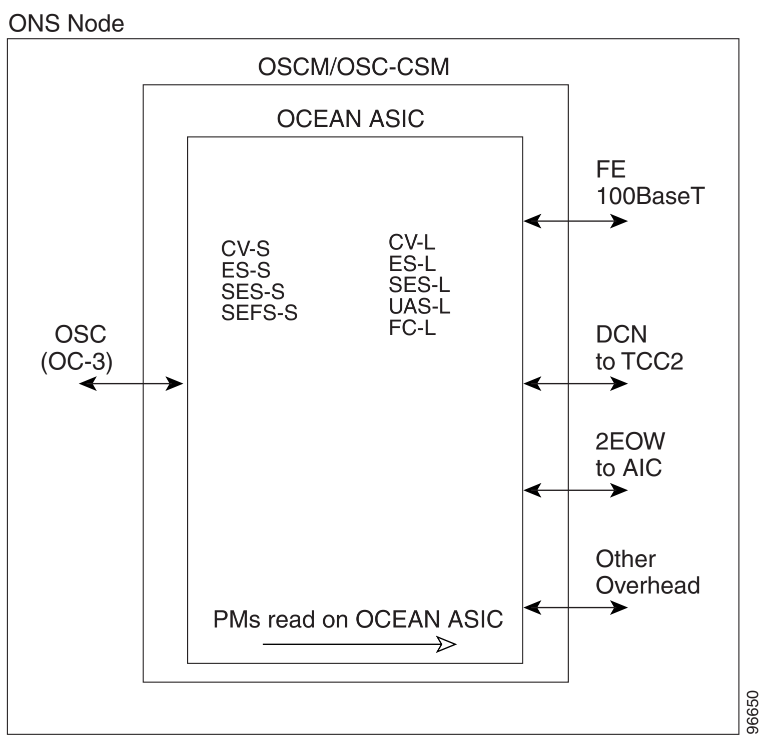
*Table 5-20 Optical PM Parameters for AD-1B-xx.x and AD-4B-xx.x Cards*

| Optical Line | Optical Band |
|---|---|
| OPR | OPT |

## 5.3.6 Optical Service Channel Card Performance Monitoring Parameters

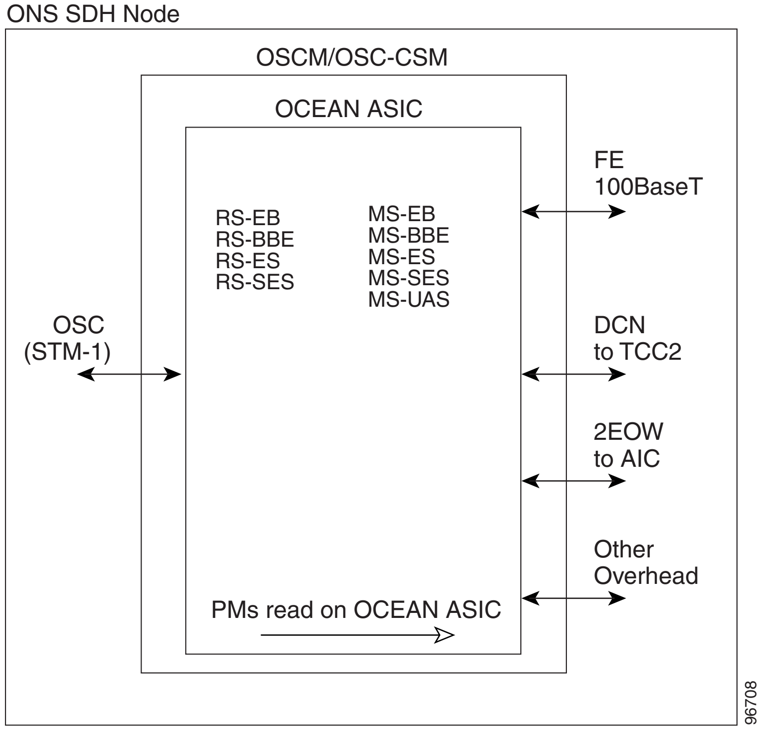
For ONS 15454 ANSI nodes, Figure 5-3 shows where overhead bytes detected on the ASICs produce PM parameters for the OSCM and OSC-CSM cards.

*Figure 5-3 ONS 15454 ANSI Node PM Read Points on OSCM and OSC-CSM Cards*




For ONS 15454 ETSI nodes, Figure 5-4 shows where overhead bytes detected on the ASICs produce PM parameters for the OSCM and OSC-CSM cards.

*Figure 5-4 ONS 15454 ETSI Node PM Read Points on OSCM and OSC-CSM Cards*




The ONS 15454 ANSI node PM parameters for the OSCM and OSC-CSM cards are listed in Table 5-21. For PM definitions, see the "5.8 SONET PM Parameter Definitions" section on page 5-24. For optics PM definitions, see the "5.4 Optics and 8b10b PM Parameter Definitions" section on page 5-17.

*Table 5-21 ANSI OSCM/OSC-CSM (OC3) Card PMs*

| Section (Near End)[1] | Line (Near End/Far End)[1] | Optics (Near End)[2] |
|---|---|---|
| CV-S<br>ES-S<br>SEF-S<br>SES-S | CV-L<br>ES-L<br>FC-L<br>SES-L<br>UAS-L | OPWR |

1. Applicable to OC3
2. Applicable to OTS facilities

*Table 5-22 ETSI OSCM and OSC-CSM Card PMs*

| Regeneration Section (Near End) | Multiplex Section (Near End/Far End) | Optics (Near End) |
|---|---|---|
| RS-BBE<br>RS-EB<br>RS-ES<br>RS-SES | MS-BBE<br>MS-EB<br>MS-ES<br>MS-SES<br>MS-UAS | OPT |

# 5.4 Optics and 8b10b PM Parameter Definitions

Table 5-23 on page 5-17 lists Cisco ONS 15454 a optics and 8b10b PM parameter definitions.

*Table 5-23 ONS 15454 Optics and 8b10b PM Definitions*

| Parameter | Definition |
|---|---|
| 8b10bDataOrderedSets | 8b10b takes 8 bits of data and sends it as 10 bits, which allows control information to be sent along with the data. DataOrderedSets is a count of data ordered sets. |
| 8b10bErrors | 8b10b takes 8 bits of data and sends it as 10 bits, which allows control information to be sent along with the data. Errors is a count of 10b errors received by the serial or deserializer (serdes 8b/10b). |
| 8b10bIdleOrderedSets | 8b10b takes 8 bits of data and sends it as 10 bits, which allows control information to be sent along with the data. IdleOrderedSets is a count of idle ordered sets. |
| 8b10bInvalidOrderedSets | 8b10b takes 8 bits of data and sends it as 10 bits, which allows control information to be sent along with the data. InvalidOrderedSets is a count of the received invalid work errors. |
| 8b10bNonIdleOrderedSets | 8b10b takes 8 bits of data and sends it as 10 bits, which allows control information to be sent along with the data. NonIdleOrderedSets is a count of ordered sets that are not idle. |
| 8b10bStatsEncodingDispErrors | 8b10b takes 8 bits of data and sends it as 10 bits, which allows control information to be sent along with the data. StatsEncodingDispErrors is a count of the received disparity errors. |
| BIE | The number of bit errors (BIE) corrected in the DWDM trunk line during the PM time interval. |
| BIT-EC | The number of Bit Errors Corrected (BIT-EC) in the DWDM trunk line during the PM time interval. |
| CGV | Code Group Violations (CGV) is a count of received code groups that do not contain a start or end delimiter. |
| DCG | Date Code Groups (DCG) is a count of received data code groups that do not contain ordered sets. |
| IOS | Idle Ordered Sets (IOS) is a count of received packets containing idle ordered sets. |
| IPC | Invalid Packets (IPC) is the count of received packets that contain errored data code groups that have start and end delimiters. |
| LBCL-AVG | Laser Bias Current Line-Average (LBCL-AVG) is the average percentage of laser bias current. |
| LBCL-MAX | Laser Bias Current Line-Maximum (LBCL-MAX) is the maximum percentage of laser bias current. |
| LBCL-MIN | Laser Bias Current Line-Minimum (LBCL-MIN) is the minimum percentage of laser bias current. |

*Table 5-23 ONS 15454 Optics and 8b10b PM Definitions (continued)*

| Parameter | Definition |
|---|---|
| LOFC | Loss of Frame Count (LOFC) is a count of the lost frames. |
| NIOS | Non-Idle Ordered Sets (NIOS) is a count of received packets containing non-idle ordered sets. |
| OPR | Optical Power Received (OPR) is the measure of average optical power received as a percentage of the nominal OPR. |
| OPR-AVG | Average Receive Optical Power (OPR-AVG) is the average received optical power measured in dBm. |
| OPR-MAX | Maximum Receive Optical Power (OPR-MAX) is the maximum received optical power measured in dBm. |
| OPR-MIN | Minimum Receive Optical Power (OPR-MIN) is the minimum received optical power measured in dBm. |
| OPT | Optical Power Transmitted (OPT) is the average optical power transmitted as a percentage of the nominal OPT. |
| OPT-AVG | Average Transmit Optical Power (OPT-AVG) is the average transmitted optical power measured in dBm. |
| OPT-MAX | Maximum Transmit Optical Power (OPT-MAX) is the maximum transmitted optical power measured in dBm. |
| OPT-MIN | Minimum Transmit Optical Power (OPT-MIN) is the minimum transmitted optical power measured in dBm. |
| OPWR-AVG | Optical Power - Average (OPWR-AVG) is the measure of average optical power on the unidirectional port. |
| OPWR-MAX | Optical Power - Maximum (OPWR-MAX) is the measure of maximum value of optical power on the unidirectional port. |
| OPWR-MIN | Optical Power - Minimum (OPWR-MIN) is the measure of minimum value of optical power on the unidirectional port. |
| UNC-WORDS | Uncorrectable Words (UNC-WORDS) is the number of uncorrectable words detected in the DWDM trunk line during the PM time interval. |
| VPC | Valid Packets (VPC) is a count of received packets that contain non-errored data code groups that have start and end delimiters. |

# 5.5 ITU G.709 and ITU-T G.8021 Trunk-Side PM Parameter Definitions

Table 5-26 defines the ITU G.709 and ITU-T G.8021 section monitoring trunk-side PM parameters. For more information, see the "5.2 Transponder and Muxponder Card Performance Monitoring" section on page 5-2.

*Table 5-24 ITU G.709 and ITU-T G.8021 Section Monitoring PM Definitions*

| Parameter | Definition |
|---|---|
| BBE-SM | Section Monitoring Background Block Errors (BBE-SM) shows the number of background block errors recorded in the OTN section during the PM time interval. |
| BBER-SM | Section Monitoring Background Block Errors Ratio (BBER-SM) shows the background block errors ratio recorded in the OTN path during the PM time interval. |
| ES-SM | Section Monitoring Errored Seconds (ES-SM) shows the errored seconds recorded in the OTN section during the PM time interval. |
| ESR-SM | Section Monitoring Errored Seconds Ratio (ESR-SM) shows the severely errored seconds ratio recorded in the OTN section during the PM time interval. |
| FC-SM | Section Monitoring Failure Counts (FC-SM) shows the failure counts recorded in the OTN section during the PM time interval. |
| SES-SM | Section Monitoring Severely Errored Seconds (SES-SM) shows the severely errored seconds recorded in the OTN section during the PM time interval. |
| SESR-SM | Section Monitoring Severely Errored Seconds Ratio (SESR-SM) shows the severely errored seconds ratio recorded in the OTN section during the PM time interval. |
| UAS-SM | Section Monitoring Unavailable Seconds (UAS-SM) shows the unavailable seconds recorded in the OTN section during the PM time interval. |

Table 5-25 defines the ITU G.709 path monitoring trunk-side PM parameters. For more information, see the "5.2 Transponder and Muxponder Card Performance Monitoring" section on page 5-2.

*Table 5-25 ITU G.709 Path Monitoring PM Definitions*

| Parameter | Definition |
|---|---|
| BBE-PM | Path Monitoring Background Block Errors (BBE-PM) shows the number of background block errors recorded in the OTN path during the PM time interval. |
| BBER-PM | Path Monitoring Background Block Errors Ratio (BBER-PM) shows the background block errors ratio recorded in the OTN path during the PM time interval. |

*Table 5-25 ITU G.709 Path Monitoring PM Definitions (continued)*

| Parameter | Definition |
|---|---|
| ES-PM | Path Monitoring Errored Seconds (ES-PM) shows the errored seconds recorded in the OTN path during the PM time interval. |
| ESR-PM | Path Monitoring Errored Seconds Ratio (ESR-PM) shows the severely errored seconds ratio recorded in the OTN path during the PM time interval. |
| FC-PM | Path Monitoring Failure Counts (FC-PM) shows the failure counts recorded in the OTN path during the PM time interval. |
| SES-PM | Path Monitoring Severely Errored Seconds (SES-PM) shows the severely errored seconds recorded in the OTN path during the PM time interval. |
| SESR-PM | Path Monitoring Severely Errored Seconds Ratio (SESR-PM) shows the severely errored seconds ratio recorded in the OTN path during the PM time interval. |
| UAS-PM | Path Monitoring Unavailable Seconds (UAS-PM) shows the unavailable seconds recorded in the OTN path during the PM time interval. |

# 5.6 Full RMON Statistics PM \ Parameter Definitions

Table 5-26 defines the MXP_MR_2.5G, MXPP_MR_2.5G, and TXP_MR_10E card full RMON statistics PM parameters. For more information, see the "5.2 Transponder and Muxponder Card Performance Monitoring" section on page 5-2.

*Table 5-26 Full RMON Statistics PM Definitions*

| Parameter | Definition |
|---|---|
| dot3StatsFCSErrors | The number of frames with frame check errors. |
| dot3StatsFrameTooLong | The number of packets at least 64 octets long, without a bad Frame Check Sequence (FCS), where the 802.3 length/type field did not match the computed DATA field length. |
| etherStatsBroadcastPkts | The number of broadcast packets, excluding multicast packets, that are 64–16376 octets in length, and have a valid FCS. |
| etherStatsCRCAlignErrors | The number of packets that are 64–1518 octets in length without an integral number of octets, or with a bad FCS. |
| etherStatsFragments | The number of packets less than 64 octets long that do not have an integral number of octets or that have a bad FCS. |
| etherStatsJabbers | The number of octets of data, including bad packets, that were received on the network. |
| etherStatsMulticastPkts | The number of multicast packets, excluding broadcast packets, that are 64–16376 octets in length, and have a valid FCS. |
| etherStatsOctets | The number in bytes of received packets, including bad packets and excluding framing bits except for FCS bytes. |

*Table 5-26 Full RMON Statistics PM Definitions (continued)*

| Parameter | Definition |
|---|---|
| etherStatsOversizePkts | The number of packets more than 16376 octets long that have a valid FCS. |
| etherStatsPkts64Octets | The number of packet received, including error packets, that are 64 octets in length. |
| etherStatsPkts65to127Octets | The number of packets received, including error packets, that are 65–127 octets in length. |
| etherStatsPkts128to255Octets | The number of packets received, including error packets, that are 128–255 octets in length. |
| etherStatsPkts256to511Octets | The number of packets received, including error packets, that are 256–511 octets in length. |
| etherStatsPkts512to1023Octets | The number of packets received, including error packets, that are 512–1023 octets in length. |
| etherStatsPkts1024to1518Octets | The number of packets received, including error packets, that are 1024–1518 octets in length. |
| etherStatsUndersizePkts | The number of packets less than 64 octets long that have a valid FCS. |
| fcStatsLinkRecoveries | The number of link recoveries. |
| fcStatsRxCredits | The number of current receive buffer to buffer credits. |
| fcStatsTxCredits | The number of current transmit buffer to buffer credits. |
| fcStatsZeroTxCredits | This is a count that increments when the FC/FICON Tx credits go from a nonzero value to zero. |
| gfpStatsLFDRaised | The number of loss of frame delineation (LFD) raised. |
| gfpStatsRoundTripLatencyUSec | Round trip delay for the end-to-end Fibre Channel transport in microseconds. |
| gfpStatsRxCRCErrors | The number of packets received with a payload FCS error. |
| gfpStatsRxCSFRaised | Received GFP loss of client character synchronization (LOCCS). |
| gfpStatsRxDistanceExtBuffers | The number of receive buffer credit for GFP-T (valid only if distance extension is enabled). |
| gfpStatsRxMBitErrors | The received multibit errored core header count (cHEC). |
| gfpStatsRxSBitErrors | The received single-bit errored cHEC. |
| gfpStatsRxSblkCRCErrors | The number of packets received with a payload FCS error. Sblk stands for super block in the GFP payload. |
| gfpStatsRxTypeInvalid | Received invalid type. |
| gfpStatsTxDistanceExtBuffers | The number of transmit buffer credit for GFP-T (valid only if distance extension is enabled). |
| ifInBroadcastPkts | The number of packets delivered to a higher sublayer and addressed to a broadcast address at this sublayer. |

*Table 5-26 Full RMON Statistics PM Definitions (continued)*

| Parameter | Definition |
|---|---|
| ifInDiscards | The number of inbound packets that were chosen to be discarded even though no errors were detected, to prevent them from being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free buffer space. |
| ifInErrors | The number of inbound packets (or transmission units) that contained errors preventing them from being delivered to a higher-layer protocol. |
| ifInErrorBytePkts | The number of received packets with an error symbol detected. |
| ifInFramingErrorPkts | The number of received packets with a control symbol other than an error detected. |
| ifInJunkInterPkts | The number of interpacket gaps between valid start symbols during which a symbol other than idle is detected, including packets of length 1–8 octets. |
| ifInMulticastPkts | The total number of multicast frames received error-free. |
| ifInOctets | The number of bytes received since the last counter reset. |
| ifOutBroadcastPkts | The number of packets requested by higher-level protocols and addressed to a broadcast address at this sublayer, including those not transmitted. |
| ifOutDiscards | The number of outbound packets that were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free buffer space. |
| ifOutMulticastPkts | The number of multicast frames transmitted error-free. |
| ifOutOctets | The number of bytes transmitted since the last counter reset. |
| InvalidCRCError | A count of invalid cyclic redundancy checks (CRCs). |
| mediaIndStatsRxFramesBadCRC | The number of received frames with a CRC error. |
| mediaIndStatsRxFramesTooLong | The number of received frames that are too long. |
| mediaIndStatsRxFramesTruncated | The number of received frames that are too small. |
| mediaIndStatsTxFramesBadCRC | The number of transmitted frames with a CRC error. |
| Running Disparity Count | A count of errors that affect the disparity of the received data stream. |
| rxControlFrames | The number of MAC control packets that are type 0x8808 and contain at least 64 octets in length. |
| rxFrames | A count of the number of frames received without errors. |
| rxLinkReset (Only for FC Mode) | A count of the received link resets. |
| rxPauseFrames | The number of received 802.x paused frames. |
| rxTotalPkts | The number of received packets. |
| rxUnknownOpcodeFrames | Number of packets of at least 64 octets in length and type 0x8808, with opcode not equal to 1. |
| Time Last Cleared | A time stamp indicating the last time statistics were reset. |

*Table 5-26 Full RMON Statistics PM Definitions (continued)*

| Parameter | Definition |
|---|---|
| txBytes | A count of the number of bytes transmitted from the frame since the last counter reset. |
| txFrames | A count of the number of transmitted frames. |
| txTotalPkts | The number of transmitted packets. |

# 5.7 FEC PM Parameter Definitions

Table 5-27 defines the MXP_MR_2.5G, MXPP_MR_2.5G, and TXP_MR_10E card FEC PM parameters. For more information, see the "5.2 Transponder and Muxponder Card Performance Monitoring" section on page 5-2.

*Table 5-27 FEC PM Definitions*

| Parameter | Definition |
|---|---|
| Bit Errors | Bit Errors are the number of bit errors corrected. |
| FEC (NE) | FEC enables correction and detection of errors along the optical links where OTN and FEC are provisioned. FEC uses Reed Solomon code RS (255,239) encoding. The FEC field is found in Rows 1 to 4 and Columns 3835 to 4080. It will contain either the Reed-Solomon RS(255,239) codes, or if FEC is disabled, fixed stuff bytes (zeros).<br>**Note** The FEC PM information can be found in the card view Performance > OTN PM tab. FEC must be enabled on the transponder units in order for FEC PM values to be reported. |
| UNC-Words | Uncorrectable Words (UNC-Words) occur when FEC detects and corrects errors to deliver a 7 to 8 dB improvement in the signal-to-noise ratio (also called margin). For ITU G.709, the FEC code used is Reed-Solomon RS (255, 239). |

# 5.8 SONET PM Parameter Definitions

Table 5-28 gives definitions for each type of SONET PM parameter available on an ONS 15454 ANSI node. These parameters become available when the client type is set to OC-3, OC-12, or OC-48 on a TXP_MR_2.5 or TXPP_MR_2.5 card or to OC-192 on a TXP_MR_10G or TXP_MR_10E card. The OC-48 client PM is available on MXP_2.5_10G and MXP_2.5_10E cards. The OC-48 trunk PM is available on MXP_MR_2.5 and MXPP_MR_2.5 cards.

*Table 5-28 SONET PM Parameters*

| Parameter | Definition |
|---|---|
| CV-L | Line Coding Violation (CV-L) indicates the number of coding violations occurring on the line. This parameter is a count of bipolar violations (BPVs) and excessive zeros (EXZs) occurring over the accumulation period. |
| CV-S | Section Coding Violation (CV-S) is a count of bit interleaved parity (BIP) errors detected at the section layer (that is, using the B1 byte in the incoming SONET signal). Up to eight section BIP errors can be detected per STS-N frame; each error increments the current CV-S second register. |
| ES-L | Line Errored Seconds (ES-L) is a count of the seconds containing one or more anomalies (BPV + EXZ) and/or defects (that is, loss of signal) on the line. |
| ES-S | Section Errored Seconds (ES-S) is a count of the number of seconds when at least one section-layer BIP error was detected or an SEF or loss of signal (LOS) defect was present. |
| FC-L | Line Failure Count (FC-L) is a count of the number of near-end line failure events. A failure event begins when an Alarm Indication Signal Line (AIS-L) failure is declared or when a lower-layer, traffic-related, near-end failure is declared. This failure event ends when the failure is cleared. A failure event that begins in one period and ends in another period is counted only in the period where it begins. |
| SEF-S | Severely Errored Framing Seconds (SEFS-S) is a count of the seconds when an SEF defect was present. An SEF defect is expected to be present during most seconds when an LOS or loss of frame (LOF) defect is present. However, there can be situations when the SEFS-S parameter is only incremented based on the presence of the SEF defect. |
| SES-L | Line Severely Errored Seconds (SES-L) is a count of the seconds containing more than a particular quantity of anomalies (BPV + EXZ $\geq$ 44) and/or defects on the line. |
| SES-S | Section Severely Errored Seconds (SES-S) is a count of the seconds when K (see Telcordia GR-253 for value) or more section-layer BIP errors were detected or an SEF or LOS defect was present. |
| UAS-L | Line Unavailable Seconds (UAS-L) is a count of the seconds when the line is unavailable. A line becomes unavailable when ten consecutive seconds occur that qualify as SES-Ls, and it continues to be unavailable until ten consecutive seconds occur that do not qualify as SES-Ls. |

# 5.9 SDH PM Parameter Definitions

Table 5-29 gives definitions for each type of SDH PM parameter available on an ONS 15454 ETSI node. These parameters become available when the client type is set to STM-1, STM-4, or STM-16 on a TXP_MR_2.5 or TXPP_MR_2.5 card or to STM-64 on a TXP_MR_10G or TXP_MR_10E card. The STM-16 client PM is available on MXP_2.5_10G and MXP_2.5_10E cards. The STM-16 trunk PM is available on MXP_MR_2.5 and MXPP_MR_2.5 cards.

*Table 5-29 SDH PM Parameters*

| Parameter | Definition |
|---|---|
| MS-BBE | Multiplex Section Background Block Error (MS-BBE) is an errored block not occurring as part of an SES. |
| MS-BBER | Multiplex Section Background Block Error Ratio (MS-BBER) is the ratio of BBE to total blocks in available time during a fixed measurement interval. The count of total blocks excludes all blocks during SESs. |
| MS-EB | Multiplex Section Errored Block (MS-EB) indicates that one or more bits are in error within a block. |
| MS-ES | Multiplex Section Errored Second (MS-ES) is a one-second period with one or more errored blocks or at least one defect. |
| MS-ESR | Multiplex Section Errored Second Ratio (MS-ESR) is the ratio of errored seconds to total seconds in available time during a fixed measurement interval. |
| MS-SES | Multiplex Section Severely Errored Second (MS-SES) is a one-second period that contains 30 percent or more errored blocks or at least one defect. SES is a subset of ES. For more information, refer to ITU-T G.829 Section 5.1.3. |
| MS-SESR | Multiplex Section Severely Errored Second ratio (MS-SESR) is the ratio of SES to total seconds in available time during a fixed measurement interval. |
| MS-UAS | Multiplex Section Unavailable Seconds (MS-UAS) is a count of the seconds when the section was unavailable. A section becomes unavailable when ten consecutive seconds occur that qualify as MS-SESs, and it continues to be unavailable until ten consecutive seconds occur that do not qualify as MS-SESs. When the condition is entered, MS-SESs decrement and then count toward MS-UAS. |
| RS-BBE | Regenerator Section Background Block Error (RS-BBE) is an errored block not occurring as part of an SES. |
| RS-BBER | Regenerator Section Background Block Error Ratio (RS-BBER) is the ratio of BBE to total blocks in available time during a fixed measurement interval. The count of total blocks excludes all blocks during SESs. |
| RS-EB | Regenerator Section Errored Block (RS-EB) indicates that one or more bits are in error within a block. |
| RS-ES | Regenerator Section Errored Second (RS-ES) is a one-second period with one or more errored blocks or at least one defect. |

*Table 5-29 SDH PM Parameters (continued)*

| Parameter | Definition |
|---|---|
| RS-ESR | Regenerator Section Errored Second Ratio (RS-ESR) is the ratio of errored seconds to total seconds in available time during a fixed measurement interval. |
| RS-SES | Regenerator Section Severely Errored Second (RS-SES) is a one-second period which contains 30 percent or more errored blocks or at least one defect. SES is a subset of ES. |
| RS-SESR | Regenerator Section Severely Errored Second Ratio (RS-SESR) is the ratio of SES to total seconds in available time during a fixed measurement interval. |
| RS-UAS | Regenerator Section Unavailable Second (RS-UAS) is a count of the seconds when the regenerator section was unavailable. A section becomes unavailable when ten consecutive seconds occur that qualify as RS-UASs, and it continues to be unavailable until ten consecutive seconds occur that do not qualify as RS-UASs. |

# 5.10 Pointer Justification Count Performance Monitoring

For the MultiService Transport Platform (MSTP), only the MXP_2.5G_10G card uses pointer justification counts. Pointers are used to compensate for frequency and phase variations. Pointer justification counts indicate timing errors on networks. When a network is out of synchronization, jitter and wander occur on the transported signal. Excessive wander can cause terminating equipment to slip.

Slips cause different effects in service. Voice service has intermittent audible clicks. Compressed voice technology has short transmission errors or dropped calls. Fax machines lose scanned lines or experience dropped calls. Digital video transmission has distorted pictures or frozen frames. Encryption service loses the encryption key, causing data to be transmitted again.

For ONS 15454 ANSI nodes, pointers provide a way to align the phase variations in STS and VT payloads. The STS payload pointer is located in the H1 and H2 bytes of the line overhead. Clocking differences are measured by the offset in bytes from the pointer to the first byte of the STS synchronous payload envelope (SPE) called the J1 byte. Clocking differences that exceed the normal range of 0 to 782 can cause data loss.

For ONS 15454 ETSI nodes, pointers provide a way to align the phase variations in VC4 payloads. The VC4 payload pointer is located in the H1 and H2 bytes of the AU pointers section and is a count of the number of bytes the VC4 path overhead (POH) J1 byte is away from the H3 byte, not including the section overhead bytes. Clocking differences are measured by the offset in bytes from the pointer to the first byte of the VC4 POH called the J1 byte. Clocking differences that exceed the normal range of 0 to 782 can cause data loss.

There are positive (PPJC) and negative (NPJC) pointer justification count parameters. PPJC is a count of path-detected (PPJC-PDET-P) or path-generated (PPJC-PGEN-P) positive pointer justifications. NPJC is a count of path-detected (NPJC-PDET-P) or path-generated (NPJC-PGEN-P) negative pointer justifications depending on the specific PM name. PJCDIFF is the absolute value of the difference between the total number of detected pointer justification counts and the total number of generated pointer justification counts. PJCS-PDET-P is a count of the one-second intervals containing one or more PPJC-PDET or NPJC-PDET. PJCS-PGEN-P is a count of the one-second intervals containing one or more PPJC-PGEN or NPJC-PGEN.

A consistent pointer justification count indicates clock synchronization problems between nodes. A difference between the counts means that the node transmitting the original pointer justification has timing variations with the node detecting and transmitting this count. For ONS 15454 SONET nodes, positive pointer adjustments occur when the frame rate of the SPE is too slow in relation to the rate of the STS-1. For ONS 15454 SDH nodes, positive pointer adjustments occur when the frame rate of the path overhead (POH) is too slow in relation to the rate of the VC4.

In CTC, the count fields for PPJC and NPJC PMs appear white and blank unless they are enabled on the card view Provisioning tab.

For detailed information and definitions of specific pointer justification count PM parameters, refer to the *Cisco ONS 15454 Troubleshooting Guide* or the *Cisco ONS 15454 SDH Troubleshooting Guide*.


# SNMP

This chapter explains Simple Network Management Protocol (SNMP) as implemented by the Cisco ONS 15454.

For SNMP setup information, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

**Note** Unless otherwise specified, "ONS 15454" refers to both ANSI and ETSI shelf assemblies.

Chapter topics include:



## 6.1 SNMP Overview

SNMP is an application-layer communication protocol that allows ONS 15454 network devices to exchange management information among these systems and with other devices outside the network. Through SNMP, network administrators can manage network performance, find and solve network problems, and plan network growth.

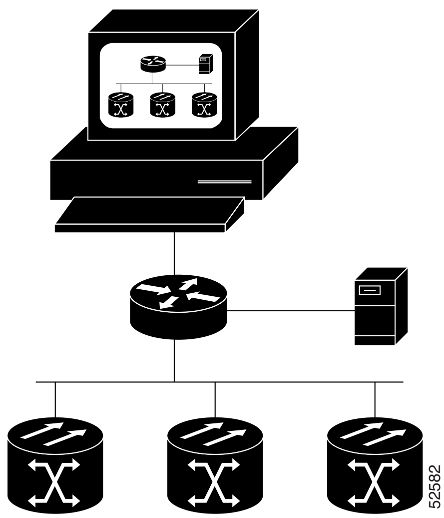
The ONS 15454 uses SNMP for asynchronous event notification to a network management system (NMS). ONS SNMP implementation uses standard Internet Engineering Task Force (IETF) management information bases (MIBs) to convey node-level inventory, fault, and performance management information for generic read-only management of DS-1, DS-3, SONET, and Ethernet technologies. SNMP allows a generic SNMP manager such as HP OpenView Network Node Manager (NNM) or Open Systems Interconnection (OSI) NetExpert to be utilized for limited management functions.

The Cisco ONS 15454 supports SNMP Version 1 (SNMPv1) and SNMP Version 2c (SNMPv2c). These versions share many features, but SNMPv2c includes additional protocol operations and 64-bit performance monitoring support. This chapter describes both versions and gives SNMP configuration parameters for the ONS 15454.

**Note** The CERENT-MSDWDM-MIB.mib, CERENT-FC-MIB.mib, and CERENT-GENERIC-PM-MIB.mib in the CiscoV2 directory support 64-bit performance monitoring counters. The SNMPv1 MIB in the CiscoV1 directory does not contain 64-bit performance monitoring counters, but supports the lower and higher word values of the corresponding 64-bit counter. The other MIB files in the CiscoV1 and CiscoV2 directories are identical in content and differ only in format.

Figure 6-1 illustrates the basic layout idea of an SNMP-managed network.

***Figure 6-1 Basic Network Managed by SNMP***

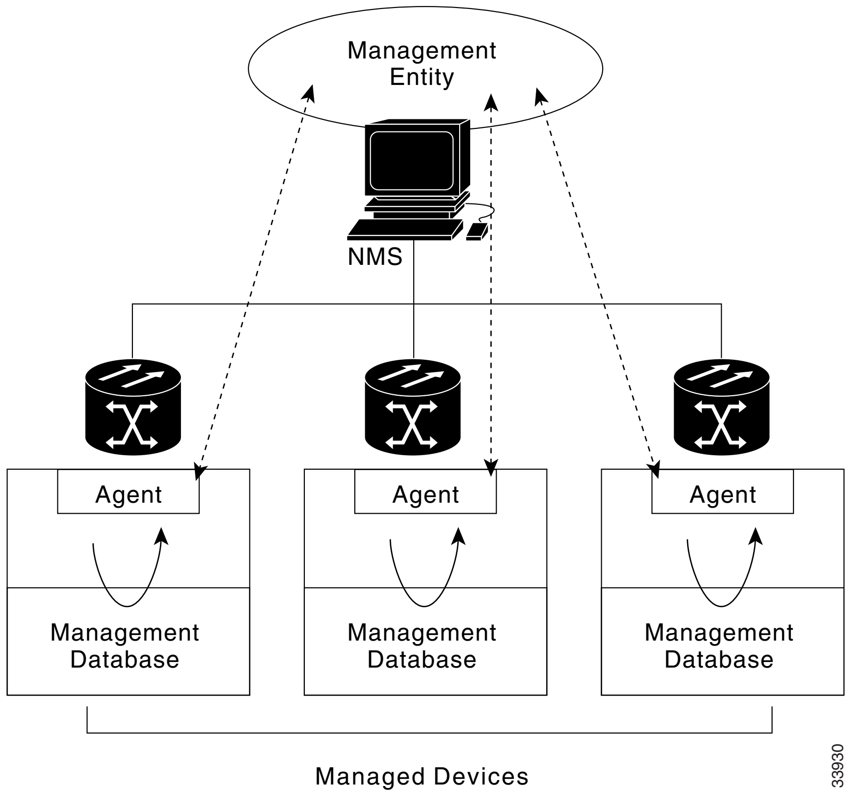



# 6.2 Basic SNMP Components

In general terms, an SNMP-managed network consists of a management system, agents, and managed devices.

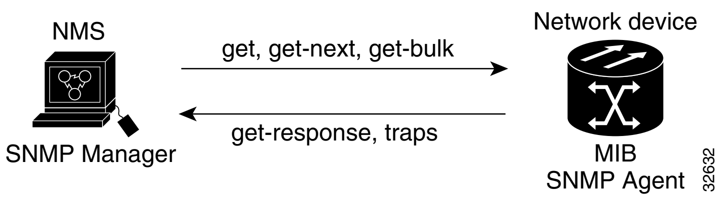
A management system such as HP OpenView executes monitoring applications and controls managed devices. Management systems execute most of the management processes and provide the bulk of memory resources used for network management. A network might be managed by one or more management systems. Figure 6-2 illustrates the relationship between the network manager, the SNMP agent, and the managed devices.

*Figure 6-2 Example of the Primary SNMP Components*




An agent (such as SNMP) residing on each managed device translates local management information data, such as performance information or event and error information caught in software traps, into a readable form for the management system. Figure 6-3 illustrates SNMP agent get-requests that transport data to the network management software.

*Figure 6-3 Agent Gathering Data from a MIB and Sending Traps to the Manager*




The SNMP agent captures data from MIBs, which are device parameter and network data repositories, or from error or change traps.

A managed element—such as a router, access server, switch, bridge, hub, computer host, or network element (such as an ONS 15454)—is accessed through the SNMP agent. Managed devices collect and store management information, making it available through SNMP to other management systems having the same protocol compatibility.

# 6.3 SNMP External Interface Requirement

Since all SNMP requests come from a third-party application, the only external interface requirement is that a third-part SNMP client application can upload RFC 3273 SNMP MIB variables in the etherStatsHighCapacityTable, etherHistoryHighCapacityTable, or mediaIndependentTable.

# 6.4 SNMP Version Support

The ONS 15454 supports SNMPv1 and SNMPv2c traps and get requests. The ONS 15454 SNMP MIBs define alarms, traps, and status. Through SNMP, NMS applications can query a management agent for data from functional entities such as Ethernet switches and SONET multiplexers using a supported MIB.

**Note** ONS 15454 MIB files in the CiscoV1 and CiscoV2 directories are almost identical in content except for the difference in 64-bit performance monitoring features. The CiscoV2 directory contains three MIBs with 64-bit performance monitoring counters:. CERENT-MSDWDM-MIB.mib, CERENT-FC-MIB.mib, and CERENT-GENERIC-PM-MIB.mib The CiscoV1 directory does not contain any 64-bit counters, but it does support the lower and higher word values used in 64-bit counters. The two directories also have somewhat different formats.

# 6.5 SNMP Message Types

The ONS 15454 SNMP agent communicates with an SNMP management application using SNMP messages. Table 6-1 describes these messages.

*Table 6-1 ONS 15454 SNMP Message Types*

| Operation | Description |
|---|---|
| get-request | Retrieves a value from a specific variable. |
| get-next-request | Retrieves the value following the named variable; this operation is often used to retrieve variables from within a table. With this operation, an SNMP manager does not need to know the exact variable name. The SNMP manager searches sequentially to find the needed variable from within the MIB. |
| get-response | Replies to a get-request, get-next-request, get-bulk-request, or set-request sent by an NMS. |
| get-bulk-request | Fills the get-response with up to the max-repetition number of get-next interactions, similar to a get-next-request. |
| set-request | Provides remote network monitoring (RMON) MIB. |
| trap | Indicates that an event has occurred. An unsolicited message is sent by an SNMP agent to an SNMP manager. |

# 6.6 SNMP Management Information Bases

Section 6.6.1 lists IETF-standard MIBs that are implemented in the ONS 15454 and shows their compilation order. Section 6.6.2 lists proprietary MIBs for the ONS 15454 and shows their compilation order. Section 6.6.3 contains information about the generic threshold and performance monitoring MIBs that can be used to monitor any network element (NE) contained in the network.

## 6.6.1 IETF-Standard MIBs for the ONS 15454

Table 6-2 lists the IETF-standard MIBs implemented in the ONS 15454 SNMP agents.

First compile the MIBs in Table 6-2. Compile the Table 6-3 MIBs next.

**Caution** If you do not compile MIBs in the correct order, one or more might not compile correctly.

*Table 6-2 IETF Standard MIBs Implemented in the ONS 15454 System*

| RFC[1] Number | Module Name | Title/Comments |
|---|---|---|
| — | IANAifType-MIB.mib | Internet Assigned Numbers Authority (IANA) ifType |
| 1213 | RFC1213-MIB-rfc1213.mib | Management Information Base for Network |
| 1907 | SNMPV2-MIB-rfc1907.mib | Management of TCP/IP-based Internets: MIB-II Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2) |
| 1253 | RFC1253-MIB-rfc1253.mib | OSPF Version 2 Management Information Base |
| 1493 | BRIDGE-MIB-rfc1493.mib | Definitions of Managed Objects for Bridges (This defines MIB objects for managing MAC bridges based on the IEEE 802.1D-1990 standard between Local Area Network [LAN] segments.) |
| 2819 | RMON-MIB-rfc2819.mib | Remote Network Monitoring Management Information Base |
| 2737 | ENTITY-MIB-rfc2737.mib | Entity MIB (Version 2) |
| 2233 | IF-MIB-rfc2233.mib | Interfaces Group MIB using SNMPv2 |
| 2358 | EtherLike-MIB-rfc2358.mib | Definitions of Managed Objects for the Ethernet-like Interface Types |
| 2493 | PerfHist-TC-MIB-rfc2493.mib | Textual Conventions for MIB Modules Using Performance History Based on 15 Minute Intervals |
| 2495 | DS1-MIB-rfc2495.mib | Definitions of Managed Objects for the DS1, E1, DS2 and E2 Interface Types |
| 2496 | DS3-MIB-rfc2496.mib | Definitions of Managed Object for the DS3/E3 Interface Type |
| 2558 | SONET-MIB-rfc2558.mib | Definitions of Managed Objects for the SONET/SDH Interface Type |

*Table 6-2 IETF Standard MIBs Implemented in the ONS 15454 System (continued)*

| RFC[1] Number | Module Name | Title/Comments |
|---|---|---|
| 2674 | P-BRIDGE-MIB-rfc2674.mib<br>Q-BRIDGE-MIB-rfc2674.mib | Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions |
| 3273 | HC-RMON-MIB | The MIB module for managing remote monitoring device implementations, augmenting the original RMON MIB as specified in RFC 2819 and RFC 1513 and RMON-2 MIB as specified in RFC 2021 |

1. RFC = Request for Comment

## 6.6.2 Proprietary ONS 15454 MIBs

Each ONS 15454 is shipped with a software CD containing applicable proprietary MIBs. Table 6-3 lists the proprietary MIBs for the ONS 15454.

*Table 6-3 ONS 15454 Proprietary MIBs*

| MIB Number | Module Name |
|---|---|
| 1 | CERENT-GLOBAL-REGISTRY.mib |
| 2 | CERENT-TC.mib |
| 3 | CERENT-454.mib |
| 4 | CERENT-GENERIC.mib (not applicable to ONS 15454) |
| 5 | CISCO-SMI.mib |
| 6 | CISCO-VOA-MIB.mib |
| 7 | CERENT-MSDWDM-MIB.mib |
| 8 | CISCO-OPTICAL-MONITOR-MIB.mib |
| 9 | CERENT-HC-RMON-MIB.mib |
| 10 | CERENT-ENVMON-MIB.mib |
| 11 | CERENT-GENERIC-PM-MIB.mib |

**Note** If you cannot compile the proprietary MIBs correctly, log into the Technical Support Website at http://www.cisco.com/techsupport or call Cisco TAC (1 800 553-2447).

**Note** When SNMP indicates that the wavelength is unknown, it means that the corresponding card (MXP_2.5G_10E, TXP_MR_10E, MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G) works with the first tunable wavelength. For more information about MXP and TXP cards, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

## 6.6.3 Generic Threshold and Performance Monitoring MIBs

In Release 6.0, a new MIB called CERENT-GENERIC-PM-MIB allows network management stations (NMS) to use a single, generic MIB for accessing threshold and performance monitoring data of different interface types. The MIB is generic in the sense that it is not tied to any particular kind of interface. The MIB objects can be used to obtain threshold values, current performance monitoring (PM) counts, and historic PM statistics for each kind of monitor and any supported interval at the near end and far end.

Previously existing MIBs in the ONS 15454 system provide some of these counts. For example, SONET interface 15-minute current PM counts and historic PM statistics are available using the SONET-MIB. DS-1 and DS-3 counts and statistics are available through the DS1-MIB and DS-3 MIB respectively. The generic MIB provides these types of information and also fetches threshold values and single-day statistics. In addition, the MIB supports optics and dense wavelength division multiplexing (DWDM) threshold and performance monitoring information.

The CERENT-GENERIC-PM-MIB is organized into three different tables:

- cerentGenericPmThresholdTable
- cerentGenericPmStatsCurrentTable
- cerentGenericPmStatsIntervalTable

The cerentGenericPmThresholdTable is used to obtain the threshold values for the monitor types. It is indexed based on the interface index (cerentGenericPmThresholdIndex), monitor type (cerentGenericPmThresholdMonType), location (cerentGenericPmThresholdLocation), and time period (cerentGenericPmThresholdPeriod). The syntax of cerentGenericPmThresholdMonType is type cerentMonitorType, defined in CERENT-TC.mib. The syntax of cerentGenericPmThresholdLocation is type cerentLocation, defined in CERENT-TC.mib. The syntax of cerentGenericPmThresholdPeriod is type cerentPeriod, defined in CERENT-TC.mib.

Threshold values can be provided in 64-bit and 32-bit formats. (For more information about 64-bit counters, see the "6.10.2 HC-RMON-MIB Support" section on page 6-18.) The 64-bit values in cerentGenericPmThresholdHCValue can be used with agents that support SNMPv2. The two 32-bit values (cerentGenericPmThresholdValue and cerentGenericPmThresholdOverFlowValue) can be used by NMSs that only support SNMPv1. The objects compiled in the cerentGenericPmThresholdTable are shown in Table 6-4.

*Table 6-4 cerentGenericPmThresholdTable*

| Index Objects | Information Objects |
|---|---|
| cerentGenericPmThresholdIndex | cerentGenericPmThresholdValue |
| cerentGenericPmThresholdMonType | cerentGenericPmThresholdOverFlowValue |
| cerentGenericPmThresholdLocation | cerentGenericPmThresholdHCValue |
| cerentGenericPmThresholdPeriod | — |

The second table within the MIB, cerentGenericPmStatsCurrentTable, compiles the current performance monitoring (PM) values for the monitor types. The table is indexed based on interface index (cerentGenericPmStatsCurrentIndex), monitor type (cerentGenericPmStatsCurrentMonType), location (cerentGenericPmStatsCurrentLocation) and time period (cerentGenericPmStatsCurrentPeriod). The syntax of cerentGenericPmStatsCurrentIndex is type cerentLocation, defined in CERENT-TC.mib. The syntax of cerentGenericPmStatsCurrentMonType is type cerentMonitor, defined in CERENT-TC.mib. The syntax of cerentGenericPmStatsCurrentPeriod is type cerentPeriod, defined in CERENT-TC.mib.

The cerentGenericPmStatsCurrentTable validates the current PM value using the cerentGenericPmStatsCurrentValid object and registers the number of valid intervals with historical PM statistics in the cerentGenericPmStatsCurrentValidIntervals object.

PM values are provided in 64-bit and 32-bit formats. The 64-bit values in cerentGenericPmStatsCurrentHCValue can be used with agents that support SNMPv2. The two 32-bit values (cerentGenericPmStatsCurrentValue and cerentGenericPmStatsCurrentOverFlowValue) can be used by NMS that only support SNMPv1. The cerentGenericPmStatsCurrentTable is shown in Table 6-5.

***Table 6-5 cerentGenericPmStatsCurrentTable***

| Index Objects | Informational Objects |
|---|---|
| cerentGenericPmStatsCurrentIndex | cerentGenericPmStatsCurrentValue |
| cerentGenericPmStatsCurrentMonType | cerentGenericPmStatsCurrentOverFlowValue |
| cerentGenericPmStatsCurrentLocation | cerentGenericPmStatsCurrentHCValue |
| cerentGenericPmStatsCurrentPeriod | cerentGenericPmStatsCurrentValidData |
| — | cerentGenericPmStatsCurrentValidIntervals |

The third table in the MIB, cerentGenericPmStatsIntervalTable, obtains historic PM values for the monitor types. This table is indexed based on the interface index, monitor type, location, time period, and interval number. It validates the current PM value in the cerentGenericPmStatsIntervalValid object.

This table is indexed based on interface index (cerentGenericPmStatsIntervalIndex), monitor type (cerentGenericPMStatsIntervalMonType), location (cerentGenericPmStatsIntervalLocation), and period (cerentGenericPmStatsIntervalPeriod). The syntax of cerentGenericPmStatsIntervalIndex is type cerentLocation, defined in CERENT-TC.mib. The syntax of cerentGenericPmStatsIntervalMonType is type cerentMonitor, defined in CERENT-TC.mib. The syntax of cerentGernicPmStatsIntervalPeriod is type cerentPeriod, defined in CERENT-TC.mib.

The table provides historic PM values in 64-bit and 32-bit formats. The 64-bit values contained in the cerentGenericPmStatsIntervalHCValue table can be used with SNMPv2 agents. The two 32-bit values (cerentGenericPmStatsIntervalValue and cerentGenericPmStatsIntervalOverFlowValue) can be used by SNMPv1 NMS. The cerentGenericPmStatsIntervalTable is shown in Table 6-6.

***Table 6-6 cerentGenericPmStatsIntervalTable***

| Index Objects | Informational Objects |
|---|---|
| cerentGenericPmStatsIntervalIndex | cerentGenericPmStatsIntervalValue |
| cerentGenericPmStatsIntervalMonType | cerentGenericPmStatsIntervalOverFlowValue |
| cerentGenericPmStatsIntervalLocation | cerentGenericPmStatsIntervalHCValue |
| cerentGenericPmStatsIntervalPeriod | cerentGenericPmStatsIntervalValidData |
| cerentGenericPmStatsIntervalNumber | — |

# 6.7 SNMP Trap Content

The ONS 15454 generates all alarms and events, such as raises and clears, as SNMP traps. These contain the following information:

- Object IDs that uniquely identify each event with information about the generating entity (the slot or port; synchronous transport signal [STS] and Virtual Tributary [VT]; bidirectional line switched ring [BLSR], Spanning Tree Protocol [STP], etc.).
- Severity and service effect of the alarm (critical, major, minor, or event; service-affecting or non-service-affecting).
- Date and time stamp showing when the alarm occurred.

## 6.7.1 Generic and IETF Traps

The ONS 15454 supports the generic IETF traps listed in Table 6-7.

*Table 6-7 Generic IETF Traps*

| Trap | From RFC No. MIB | Description |
|---|---|---|
| coldStart | RFC1907-MIB | Agent up, cold start. |
| warmStart | RFC1907-MIB | Agent up, warm start. |
| authenticationFailure | RFC1907-MIB | Community string does not match. |
| newRoot | RFC1493/ BRIDGE-MIB | Sending agent is the new root of the spanning tree. |
| topologyChange | RFC1493/ BRIDGE-MIB | A port in a bridge has changed from Learning to Forwarding or Forwarding to Blocking. |
| entConfigChange | RFC2737/ ENTITY-MIB | The entLastChangeTime value has changed. |
| dsx1LineStatusChange | RFC2495/ DS1-MIB | The value of an instance of dsx1LineStatus has changed. The trap can be used by an NMS to trigger polls. When the line status change results from a higher-level line status change (for example, a DS-3), no traps for the DS-1 are sent. |
| dsx3LineStatusChange | RFC2496/ DS3-MIB | The value of an instance of dsx3LineStatus has changed. This trap can be used by an NMS to trigger polls. When the line status change results in a lower-level line status change (for example, a DS-1), no traps for the lower-level are sent. |
| risingAlarm | RFC2819/ RMON-MIB | The SNMP trap that is generated when an alarm entry crosses the rising threshold and the entry generates an event that is configured for sending SNMP traps. |
| fallingAlarm | RFC2819/ RMON-MIB | The SNMP trap that is generated when an alarm entry crosses the falling threshold and the entry generates an event that is configured for sending SNMP traps. |

## 6.7.2 Variable Trap Bindings

Each SNMP trap contains variable bindings that are used to create the MIB tables. ONS 15454 traps and variable bindings are listed in Table 6-8. For each group (such as Group A), all traps within the group are associated with all of its variable bindings.

*Table 6-8 ONS 15454 SNMPv2 Trap Variable Bindings*

| Group | Trap Name(s) Associated with | Variable Binding Number | SNMPv2 Variable Bindings | Description |
|---|---|---|---|---|
| A | dsx1LineStatusChange (from RFC 2495) | (1) | dsx1LineStatus | This variable indicates the line status of the interface. It contains loopback, failure, received alarm and transmitted alarm information. |
| | | (2) | dsx1LineStatusLastChange | The value of MIB II's sysUpTime object at the time this DS1 entered its current line status state. If the current state was entered prior to the last proxy-agent reinitialization, the value of this object is zero. |
| | | (3) | cerent454NodeTime | The time that an event occurred. |
| | | (4) | cerent454AlarmState | The alarm severity and service-affecting status. Severities are Minor, Major, and Critical. Service-affecting statuses are Service-Affecting and Non-Service Affecting. |
| | | (5) | snmpTrapAddress | The address of the SNMP trap. |
| B | dsx3LineStatusChange (from RFC 2496) | (1) | dsx3LineStatus | This variable indicates the line status of the interface. It contains loopback state information and failure state information. |
| | | (2) | dsx3LineStatusLastChange | The value of MIB II's sysUpTime object at the time this DS3/E3 entered its current line status state. If the current state was entered prior to the last reinitialization of the proxy-agent, then the value is zero. |
| | | (3) | cerent454NodeTime | The time that an event occurred. |

*Table 6-8 ONS 15454 SNMPv2 Trap Variable Bindings (continued)*

| Group | Trap Name(s) Associated with | Variable Binding Number | SNMPv2 Variable Bindings | Description |
|---|---|---|---|---|
| B (cont.) | | (4) | cerent454AlarmState | The alarm severity and service-affecting status. Severities are Minor, Major, and Critical. Service-affecting statuses are Service-Affecting and Non-Service Affecting. |
| | | (5) | snmpTrapAddress | The address of the SNMP trap. |
| C | coldStart (from RFC 1907) | (1) | cerent454NodeTime | The time that the event occurred. |
| | warmStart (from RFC 1907) | (2) | cerent454AlarmState | The alarm severity and service-affecting status. Severities are Minor, Major, and Critical. Service-affecting statuses are Service-Affecting and Non-Service Affecting. |
| | newRoot (from RFC) | (3) | snmpTrapAddress | The address of the SNMP trap. |
| | topologyChange (from RFC) | | — | — |
| | entConfigChange (from RFC 2737) | | — | — |
| | authenticationFailure (from RFC 1907) | | — | — |
| D1 | risingAlarm (from RFC 2819) | (1) | alarmIndex | This variable uniquely identifies each entry in the alarm table. When an alarm in the table clears, the alarm indexes change for each alarm listed. |
| | | (2) | alarmVariable | The object identifier of the variable being sampled. |
| | | (3) | alarmSampleType | The method of sampling the selected variable and calculating the value to be compared against the thresholds. |
| | | (4) | alarmValue | The value of the statistic during the last sampling period. |

*Table 6-8 ONS 15454 SNMPv2 Trap Variable Bindings (continued)*

| Group | Trap Name(s) Associated with | Variable Binding Number | SNMPv2 Variable Bindings | Description |
|---|---|---|---|---|
| D1 (cont.) | | (5) | alarmRisingThreshold | When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single event is generated. A single event is also generated if the first sample after this entry is greater than or equal to this threshold. |
| | | (6) | cerent454NodeTime | The time that an event occurred. |
| | | (7) | cerent454AlarmState | The alarm severity and service-affecting status. Severities are Minor, Major, and Critical. Service-affecting statuses are Service-Affecting and Non-Service Affecting. |
| | | (8) | snmpTrapAddress | The address of the SNMP trap. |
| D2 | fallingAlarm (from RFC 2819) | (1) | alarmIndex | This variable uniquely identifies each entry in the alarm table. When an alarm in the table clears, the alarm indexes change for each alarm listed. |
| | | (2) | alarmVariable | The object identifier of the variable being sampled. |
| | | (3) | alarmSampleType | The method of sampling the selected variable and calculating the value to be compared against the thresholds. |
| | | (4) | alarmValue | The value of the statistic during the last sampling period. |
| | | (5) | alarmFallingThreshold | When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, a single event is generated. A single is also generated if the first sample after this entry is less than or equal to this threshold. |
| | | (6) | cerent454NodeTime | The time that an event occurred. |

*Table 6-8 ONS 15454 SNMPv2 Trap Variable Bindings (continued)*

| Group | Trap Name(s) Associated with | Variable Binding Number | SNMPv2 Variable Bindings | Description |
|---|---|---|---|---|
| D2 (cont.) | | (7) | cerent454AlarmState | The alarm severity and service-affecting status. Severities are Minor, Major, and Critical. Service-affecting statuses are Service-Affecting and Non-Service Affecting. |
| | | (8) | snmpTrapAddress | The address of the SNMP trap. |
| E | failureDetectedExternal ToTheNE (from CERENT-454-mib) | (1) | cerent454NodeTime | The time that an event occurred. |
| | | (2) | cerent454AlarmState | The alarm severity and service-affecting status. Severities are Minor, Major, and Critical. Service-affecting statuses are Service-Affecting and Non-Service Affecting. |
| | | (3) | cerent454AlarmObjectType | The entity that raised the alarm. The NMS should use this value to decide which table to poll for further information about the alarm. |
| | | (4) | cerent454AlarmObjectIndex | Every alarm is raised by an object entry in a specific table. This variable is the index of objects in each table; if the alarm is interface-related, this is the index of the interface in the interface table. |
| | | (5) | cerent454AlarmSlotNumber | The slot of the object that raised the alarm. If a slot is not relevant to the alarm, the slot number is zero. |
| | | (6) | cerent454AlarmPortNumber | The port of the object that raised the alarm. If a port is not relevant to the alarm, the port number is zero. |
| | | (7) | cerent454AlarmLineNumber | The object line that raised the alarm. If a line is not relevant to the alarm, the line number is zero. |
| | | (8) | cerent454AlarmObjectName | The TL1-style user-visible name that uniquely identifies an object in the system. |

*Table 6-8 ONS 15454 SNMPv2 Trap Variable Bindings (continued)*

| Group | Trap Name(s) Associated with | Variable Binding Number | SNMPv2 Variable Bindings | Description |
|---|---|---|---|---|
| E (cont.) | | (9) | cerent454AlarmAdditionalInfo | Additional information for the alarm object. In the current version of the MIB, this object contains provisioned description for alarms that are external to the NE. If there is no additional information, the value is zero. |
| | | (10) | snmpTrapAddress | The address of the SNMP trap. |
| F | performanceMonitor ThresholdCrossingAlert (from CERENT-454-mib) | (1) | cerent454NodeTime | The time that an event occurred. |
| | | (2) | cerent454AlarmState | The alarm severity and service-affecting status. Severities are Minor, Major, and Critical. Service-affecting statuses are Service-Affecting and Non-Service Affecting. |
| | | (3) | cerent454AlarmObjectType | The entity that raised the alarm. The NMS should use this value to decide which table to poll for further information about the alarm. |
| | | (4) | cerent454AlarmObjectIndex | Every alarm is raised by an object entry in a specific table. This variable is the index of objects in each table; if the alarm is interface-related, this is the index of the interface in the interface table. |
| | | (5) | cerent454AlarmSlotNumber | The slot of the object that raised the alarm. If a slot is not relevant to the alarm, the slot number is zero. |
| | | (6) | cerent454AlarmPortNumber | The port of the object that raised the alarm. If a port is not relevant to the alarm, the port number is zero. |
| | | (7) | cerent454AlarmLineNumber | The object line that raised the alarm. If a line is not relevant to the alarm, the line number is zero. |
| | | (8) | cerent454AlarmObjectName | The TL1-style user-visible name that uniquely identifies an object in the system. |
| | | (9) | cerent454ThresholdMonitorType | This object indicates the type of metric being monitored. |

*Table 6-8 ONS 15454 SNMPv2 Trap Variable Bindings (continued)*

| Group | Trap Name(s) Associated with | Variable Binding Number | SNMPv2 Variable Bindings | Description |
|---|---|---|---|---|
| F (cont.) | | (10) | cerent454ThresholdLocation | Indicates whether the event occurred at the near or far end. |
| | | (11) | cerent454ThresholdPeriod | Indicates the sampling interval period. |
| | | (12) | cerent454ThresholdSetValue | The value of this object is the threshold provisioned by the NMS. |
| | | (13) | cerent454ThresholdCurrentValue | — |
| | | (14) | cerent454ThresholdDetectType | — |
| | | (15) | snmpTrapAddress | The address of the SNMP trap. |
| G | All other traps (from CERENT-454-MIB) not listed above | (1) | cerent454NodeTime | The time that an event occurred. |
| | | (2) | cerent454AlarmState | The alarm severity and service-affecting status. Severities are Minor, Major, and Critical. Service-affecting statuses are Service-Affecting and Non-Service Affecting. |
| | | (3) | cerent454AlarmObjectType | The entity that raised the alarm. The NMS should use this value to decide which table to poll for further information about the alarm. |
| | | (4) | cerent454AlarmObjectIndex | Every alarm is raised by an object entry in a specific table. This variable is the index of objects in each table; if the alarm is interface-related, this is the index of the interface in the interface table. |
| | | (5) | cerent454AlarmSlotNumber | The slot of the object that raised the alarm. If a slot is not relevant to the alarm, the slot number is zero. |
| | | (6) | cerent454AlarmPortNumber | The port of the object that raised the alarm. If a port is not relevant to the alarm, the port number is zero. |
| | | (7) | cerent454AlarmLineNumber | The object line that raised the alarm. If a line is not relevant to the alarm, the line number is zero. |

*Table 6-8 ONS 15454 SNMPv2 Trap Variable Bindings (continued)*

| Group | Trap Name(s) Associated with | Variable Binding Number | SNMPv2 Variable Bindings | Description |
|---|---|---|---|---|
| G (cont.) | | (8) | cerent454AlarmObjectName | The TL1-style user-visible name that uniquely identifies an object in the system. |
| | | (9) | snmpTrapAddress | The address of the SNMP trap. |

# 6.8 SNMP Community Names

Community names are used to group SNMP trap destinations. All ONS 15454 trap destinations can be provisioned as part of SNMP communities in Cisco Transport Controller (CTC). When community names are assigned to traps, the ONS 15454 treats the request as valid if the community name matches one that is provisioned in CTC. In this case, all agent-managed MIB variables are accessible to that request. If the community name does not match the provisioned list, SNMP drops the request.

# 6.9 Proxy Over Firewalls

SNMP and NMS applications have traditionally been unable to cross firewalls used for isolating security risks inside or from outside networks. Release 6.0 CTC enables network operations centers (NOCs) to access performance monitoring data such as RMON statistics or autonomous messages across firewalls by using an SMP proxy element installed on a firewall.

The application-level proxy transports SNMP protocol data units (PDU) between the NMS and NEs, allowing requests and responses between the NMS and NEs and forwarding NE autonomous messages to the NMS. The proxy agent requires little provisioning at the NOC and no additional provisioning at the NEs.

The firewall proxy is intended for use in a gateway network element-end network element (GNE-ENE) topology with many NEs through a single NE gateway. Up to 64 SNMP requests (such as get, getnext, or getbulk) are supported at any time behind single or multiple firewalls. The proxy interoperates with common NMS such as HP OpenView.

For security reasons, the SNMP proxy feature must be enabled at all receiving and transmitting NEs to function. For instructions to do this, refer to the *Cisco ONS 15454 Procedure Guide*.

# 6.10 Remote Monitoring

The ONS 15454 incorporates RMON to allow network operators to monitor Ethernet card performance and events. The RMON thresholds are user-provisionable in CTC. Refer to the *Cisco ONS 15454 Procedure Guide* for instructions. Note that otherwise, RMON operation is invisible to the typical CTC user.

ONS 15454 system RMON is based on the IETF-standard MIB RFC 2819 and includes the following five groups from the standard MIB: Ethernet Statistics, History Control, Ethernet History, Alarm, and Event.

## 6.10.1 64-Bit RMON Monitoring over DCC

The ONS 15454 DCC is implemented over the IP protocol, which is not compatible with Ethernet. The system builds Ethernet equipment History and Statistics tables using HDLC statistics that are gathered over the DCC (running point-topoint protocol, or PPP). This release adds RMON DCC monitoring (for both IP and Ethernet) to monitor the health of remote DCC connections.

In R6.0, the implementation contains two MIBS for DCC interfaces. They are:

- cMediaIndependentTable—standard, rfc3273; the proprietary extension of the HC-RMON MIB used for reporting statistics
- cMediaIndependentHistoryTable—proprietary MIB used to support history

### 6.10.1.1 Row Creation in MediaIndependentTable

The SetRequest PDU for creating a row in the mediaIndependentTable should contain all the values required to activate a row in a single set operation along with an assignment of the status variable to createRequest (2). The SetRequest PDU for entry creation must have all the object IDs (OIDs) carrying an instance value of 0. That is, all the OIDs should be of the type OID.0.

In order to create a row, the SetRequest PDU should contain the following:

- mediaIndependentDataSource and its desired value
- mediaIndependentOwner and its desired value (The size of mediaIndependentOwner is limited to 32 characters.)
- mediaIndependentStatus with a value of createRequest (2)

The mediaIndependentTable creates a row if the SetRequest PDU is valid according to the above rules. When the row is created, the SNMP agent decides the value of mediaIndependentIndex. This value is not sequentially allotted or contiguously numbered. It changes when an Ethernet interface is added or deleted. The newly created row will have mediaIndependentTable value of valid (1).

If the row already exists, or if the SetRequest PDU values are insufficient or do not make sense, the SNMP agent returns an error code.

**Note** mediaIndependentTable entries are not preserved if the SNMP agent is restarted.

The mediaIndependentTable deletes a row if the SetRequest PDU contains a mediaIndependentStatus with a value of invalid (4). The varbind's OID instance value identifies the row for deletion. You can recreate a deleted row in the table if desired.

### 6.10.1.2 Row Creation in cMediaIndependentHistoryControlTable

SNMP row creation and deletion for the cMediaIndependentHistoryControlTable follows the same processes as for the MediaIndependentTable; only the variables differ.

In order to create a row, the SetRequest PDU should contain the following:

- cMediaIndependentHistoryControlDataSource and its desired value
- cMediaIndependentHistoryControlOwner and its desired value
- cMediaIndependentHistoryControlStatus with a value of createRequest (2)

## 6.10.2 HC-RMON-MIB Support

For the ONS 15454, the implementation of the high-capacity remote monitoring information base (HC-RMON-MIB, or RFC 3273) enables 64-bit support of existing RMON tables. This support is provided with the etherStatsHighCapacityTable and the etherHistoryHighCapacityTable. An additional table, the mediaIndependentTable, and an additional object, hcRMONCapabilities, are also added for this support. All of these elements are accessible by any third-party SNMP client having RFC 3273 support.

## 6.10.3 Ethernet Statistics RMON Group

The Ethernet Statistics group contains the basic statistics monitored for each subnetwork in a single table called the etherStatsTable.

### 6.10.3.1 Row Creation in etherStatsTable

The SetRequest PDU for creating a row in this table should contain all the values needed to activate a row in a single set operation, and an assigned status variable to createRequest. The SetRequest PDU object ID (OID) entries must all carry an instance value, or type OID, of 0.

In order to create a row, the SetRequest PDU should contain the following:

- The etherStatsDataSource and its desired value
- The etherStatsOwner and its desired value (size of this value is limited to 32 characters)
- The etherStatsStatus with a value of createRequest (2)

The etherStatsTable creates a row if the SetRequest PDU is valid according to the above rules. When the row is created, the SNMP agent decides the value of etherStatsIndex. This value is not sequentially allotted or contiguously numbered. It changes when an Ethernet interface is added or deleted. The newly created row will have etherStatsStatus value of valid (1).

If the etherStatsTable row already exists, or if the SetRequest PDU values are insufficient or do not make sense, the SNMP agent returns an error code.

**Note** EtherStatsTable entries are not preserved if the SNMP agent is restarted.

### 6.10.3.2 Get Requests and GetNext Requests

Get requests and getNext requests for the etherStatsMulticastPkts and etherStatsBroadcastPkts columns return a value of zero because the variables are not supported by ONS 15454 Ethernet cards.

### 6.10.3.3 Row Deletion in etherStatsTable

To delete a row in the etherStatsTable, the SetRequest PDU should contain an etherStatsStatus “invalid” value (4). The OID marks the row for deletion. If required, a deleted row can be recreated.

### 6.10.3.4 64-Bit etherStatsHighCapacity Table

The Ethernet statistics group contains 64-bit statistics in the etherStatsHighCapacityTable, which provides 64-bit RMON support for the HC-RMON-MIB. The etherStatsHighCapacityTable is an extension of the etherStatsTable that adds 16 new columns for performance monitoring data in 64-bit format. There is a one-to-one relationship between the etherStatsTable and etherStatsHighCapacityTable when rows are created or deleted in either table.

## 6.10.4 History Control RMON Group

The History Control group defines sampling functions for one or more monitor interfaces in the historyControlTable. The values in this table, as specified in RFC 2819, are derived from the historyControlTable and etherHistoryTable.

### 6.10.4.1 History Control Table

The RMON is sampled at one of four possible intervals. Each interval, or period, contains specific history values (also called buckets). Table 6-9 lists the four sampling periods and corresponding buckets.

The historyControlTable maximum row size is determined by multiplying the number of ports on a card by the number of sampling periods. For example, an ONS 15454 E100 card contains 24 ports, which multiplied by periods allows 96 rows in the table. An E1000 card contains 14 ports, which multiplied by four periods allows 56 table rows.

*Table 6-9 RMON History Control Periods and History Categories*

| Sampling Periods (historyControlValue Variable) | Total Values, or Buckets (historyControl Variable) |
|---|---|
| 15 minutes | 32 |
| 24 hours | 7 |
| 1 minute | 60 |
| 60 minutes | 24 |

### 6.10.4.2 Row Creation in historyControlTable

The SetRequest PDU must be able to activate a historyControlTable row in one single-set operation. In order to do this, the PDU must contain all needed values and have a status variable value of 2 (createRequest). All OIDs in the SetRequest PDU should be type OID.0 type for entry creation.

To create a SetRequest PDU for the historyControlTable, the following values are required:

- The historyControlDataSource and its desired value
- The historyControlBucketsRequested and it desired value
- The historyControlInterval and its desired value
- The historyControlOwner and its desired value
- The historyControlStatus with a value of createRequest (2)

The historyControlBucketsRequested OID value is ignored because the number of buckets allowed for each sampling period, based upon the historyControlInterval value, is already fixed as listed in Table 6-9.

The historyControlInterval value cannot be changed from the four allowed choices. If you use another value, the SNMP agent selects the closest smaller time period from the set buckets. For example, if the set request specifies a 25-minute interval, this falls between the 15-minute (32 bucket) variable and the 60-minute (24 bucket) variable. The SNMP agent automatically selects the lower, closer value, which is 15 minutes, so it allows 32 buckets.

If the SetRequest PDU is valid, a historyControlTable row is created. If the row already exists, or if the SetRequest PDU values do not make sense or are insufficient, the SNMP agent does not create the row and returns an error code.

### 6.10.4.3 Get Requests and GetNext Requests

These PDUs are not restricted.

### 6.10.4.4 Row Deletion in historyControl Table

To delete a row from the table, the SetRequest PDU should contain a historyControlStatus value of 4 (invalid). A deleted row can be recreated.

## 6.10.5 Ethernet History RMON Group

The ONS 15454 implements the etherHistoryTable as defined in RFC 2819. The group is created within the bounds of the historyControlTable and does not deviate from the RFC in its design.

### 6.10.5.1 64-Bit etherHistoryHighCapacityTable

64-bit Ethernet history for the HC-RMON-MIB is implemented in the etherHistoryHighCapacityTable, which is an extension of the etherHistoryTable. The etherHistoryHighCapacityTable adds four columns for 64-bit performance monitoring data. These two tables have a one-to-one relationship. Adding or deleting a row in one table will effect the same change in the other.

## 6.10.6 Alarm RMON Group

The Alarm group consists of the alarmTable, which periodically compares sampled values with configured thresholds and raises an event if a threshold is crossed. This group requires the implementation of the event group, which follows this section.

### 6.10.6.1 Alarm Table

The NMS uses the alarmTable to determine and provision network performance alarmable thresholds.

### 6.10.6.2 Row Creation in alarmTable

To create a row in the alarmTable, the SetRequest PDU must be able to create the row in one single-set operation. All OIDs in the SetRequest PDU should be type OID.0 type for entry creation. The table has a maximum number of 256 rows.

To create a SetRequest PDU for the alarmTable, the following values are required:

- The alarmInterval and its desired value
- The alarmVariable and its desired value
- The alarmSampleType and its desired value
- The alarmStartupAlarm and its desired value
- The alarmOwner and its desired value
- The alarmStatus with a value of createRequest (2)

If the SetRequest PDU is valid, a historyControlTable row is created. If the row already exists, or if the SetRequest PDU values do not make sense or are insufficient, the SNMP agent does not create the row and returns an error code.

In addition to the required values, the following restrictions must be met in the SetRequest PDU:

- The alarmOwner is a string of length 32 characters.
- The alarmRisingEventIndex always takes value 1.
- The alarmFallingEventIndex always takes value 2.
- The alarmStatus has only two values supported in SETs: createRequest (2) and invalid (4).
- The AlarmVariable is of the type OID.ifIndex, where ifIndex gives the interface this alarm is created on and OID is one of the OIDs supported in Table 6-10.

*Table 6-10 OIDs Supported in the AlarmTable*

| No. | Column Name | OID | Status |
|---|---|---|---|
| 1 | ifInOctets | {1.3.6.1.2.1.2.2.1.10} | — |
| 2 | IfInUcastPkts | {1.3.6.1.2.1.2.2.1.11} | — |
| 3 | ifInMulticastPkts | {1.3.6.1.2.1.31.1.1.1.2} | Unsupported in E100/E1000 |
| 4 | ifInBroadcastPkts | {1.3.6.1.2.1.31.1.1.1.3} | Unsupported in E100/E1000 |
| 5 | ifInDiscards | {1.3.6.1.2.1.2.2.1.13} | Unsupported in E100/E1000 |
| 6 | ifInErrors | {1.3.6.1.2.1.2.2.1.14} | — |
| 7 | ifOutOctets | {1.3.6.1.2.1.2.2.1.16} | — |
| 8 | ifOutUcastPkts | {1.3.6.1.2.1.2.2.1.17} | — |
| 9 | ifOutMulticastPkts | {1.3.6.1.2.1.31.1.1.1.4} | Unsupported in E100/E1000 |
| 10 | ifOutBroadcastPkts | {1.3.6.1.2.1.31.1.1.1.5} | Unsupported in E100/E1000 |
| 11 | ifOutDiscards | {1.3.6.1.2.1.2.2.1.19} | Unsupported in E100/E1000 |
| 12 | Dot3StatsAlignmentErrors | {1.3.6.1.2.1.10.7.2.1.2} | — |
| 13 | Dot3StatsFCSErrors | {1.3.6.1.2.1.10.7.2.1.3} | — |
| 14 | Dot3StatsSingleCollisionFrames | {1.3.6.1.2.1.10.7.2.1.4} | — |
| 15 | Dot3StatsMultipleCollisionFrames | {1.3.6.1.2.1.10.7.2.1.5} | — |
| 16 | Dot3StatsDeferredTransmissions | {1.3.6.1.2.1.10.7.2.1.7} | — |
| 17 | Dot3StatsLateCollisions | {1.3.6.1.2.1.10.7.2.1.8} | — |
| 18 | Dot3StatsExcessiveCollisions | {13.6.1.2.1.10.7.2.1.9} | — |
| 19 | Dot3StatsFrameTooLong | {1.3.6.1.2.1.10.7.2.1.13} | — |
| 20 | Dot3StatsCarrierSenseErrors | {1.3.6.1.2.1.10.7.2.1.11} | Unsupported in E100/E1000 |

*Table 6-10 OIDs Supported in the AlarmTable (continued)*

| No. | Column Name | OID | Status |
|---|---|---|---|
| 21 | Dot3StatsSQETestErrors | {1.3.6.1.2.1.10.7.2.1.6} | Unsupported in E100/E1000 |
| 22 | etherStatsUndersizePkts | {1.3.6.1.2.1.16.1.1.1.9} | — |
| 23 | etherStatsFragments | {1.3.6.1.2.1.16.1.1.1.11} | — |
| 24 | etherStatsPkts64Octets | {1.3.6.1.2.1.16.1.1.1.14} | — |
| 25 | etherStatsPkts65to127Octets | {1.3.6.1.2.1.16.1.1.1.15} | — |
| 26 | etherStatsPkts128to255Octets | {1.3.6.1.2.1.16.1.1.1.16} | — |
| 27 | etherStatsPkts256to511Octets | {1.3.6.1.2.1.16.1.1.1.17} | — |
| 28 | etherStatsPkts512to1023Octets | {1.3.6.1.2.1.16.1.1.1.18} | — |
| 29 | etherStatsPkts1024to1518Octets | {1.3.6.1.2.1.16.1.1.1.19} | — |
| 30 | EtherStatsBroadcastPkts | {1.3.6.1.2.1.16.1.1.1.6} | — |
| 31 | EtherStatsMulticastPkts | {1.3.6.1.2.1.16.1.1.1.7} | — |
| 32 | EtherStatsOversizePkts | {1.3.6.1.2.1.16.1.1.1.10} | — |
| 33 | EtherStatsJabbers | {1.3.6.1.2.1.16.1.1.1.12} | — |
| 34 | EtherStatsOctets | {1.3.6.1.2.1.16.1.1.1.4} | — |
| 35 | EtherStatsCollisions | {1.3.6.1.2.1.16.1.1.1.13} | — |
| 36 | EtherStatsCollisions | {1.3.6.1.2.1.16.1.1.1.8} | — |
| 37 | EtherStatsDropEvents | {1.3.6.1.2.1.16.1.1.1.3} | Unsupported in E100/E1000 and G1000 |

#### 6.10.6.3 Get Requests and GetNext Requests

These PDUs are not restricted.

#### 6.10.6.4 Row Deletion in alarmTable

To delete a row from the table, the SetRequest PDU should contain an alarmStatus value of 4 (invalid). A deleted row can be recreated. Entries in this table are preserved if the SNMP agent is restarted.

## 6.10.7 Event RMON Group

The Event group controls event generation and notification. It consists of two tables: the eventTable, which is a read-only list of events to be generated, and the logTable, which is a writable set of data describing a logged event. The ONS 15454 implements the logTable as specified in RFC 2819.

### 6.10.7.1 Event Table

The eventTable is read-only and unprovisionable. The table contains one row for rising alarms and another for falling ones. This table has the following restrictions:

- The eventType is always log-and-trap (4).

- The eventCommunity value is always a zero-length string, indicating that this event causes the trap to be despatched to all provisioned destinations.
- The eventOwner column value is always "monitor."
- The eventStatus column value is always valid(1).

#### 6.10.7.2 Log Table

The logTable is implemented exactly as specified in RFC 2819. The logTable is based upon data that is locally cached in a controller card. If there is a controller card protection switch, the existing logTable is cleared and a new one is started on the newly active controller card. The table contains as many rows as provided by the alarm controller.

# INDEX

## Numerics



## A

## F

## G



## H



## I

## J



## L

## M

## N



## O

## P

## S

## U



## V



## W



## X