Cisco NCS 2000 Series Troubleshooting Guide, Release 11.x.x

First Published: 2019-03-08

Last Modified: 2023-06-16

Americas 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: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

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: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by using one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Modifications to this product not authorized by Cisco 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.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

CONTENTS

Preface

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

This section provides the following information:

Document Objectives

This guide gives troubleshooting information and troubleshooting-related parameters for the Cisco NCS 2002 and Cisco NCS 2006 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, on page xliv section.

Note Cisco ONS 15454 M2 chassis has reached its end-of-life status. For more information, see the Retirement Notification page.

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 telecommunications technician.

Document Organization

This document is organized into the following chapters:

Chapter	Description
General Troubleshooting, on page 1	Provides procedures for troubleshooting the most common problems encountered when operating on Cisco NCS 2000 Seriesplatforms.
Alarm Troubleshooting, on page 85	Gives a description, severity, and troubleshooting procedure for each commonly encountered Cisco DWDM alarm and condition.
Transient Conditions, on page 403	Gives a description, entity, Simple Network Management Protocol (SNMP) number, and trap for each commonly encountered transient condition.
Error Messages, on page 415	Lists the error messages.

Document Conventions

This document uses the following conventions:

Convention	Description
^ or Ctrl	Both the ^ symbol and Ctrl represent the Control (Ctrl) key on a keyboard. For example, the key combination **^D** or **Ctrl-D** means that you hold down the Control key while you press the D key. (Keys are indicated in capital letters but are not case sensitive.)
bold font	Commands and keywords and user-entered text appear in **bold** font.
Italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
`Courier font`	Terminal sessions and information the system displays appear in `courier` font.
`Bold Courier font`	Bold Courier font indicates text that the user must enter.
[x]	Elements in square brackets are optional.
...	An ellipsis (three consecutive nonbolded periods without spaces) after a syntax element indicates that the element can be repeated.

Convention	Description
|	A vertical line, called a pipe, indicates a choice within a set of keywords or arguments.
[x | y]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
{x | y}	Required alternative keywords are grouped in braces and separated by vertical bars.
[x {y | z}]	Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Reader Alert Conventions

This document uses the following conventions for reader alerts:

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

Tip Means *the following information will help you solve a problem.*

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

Timesaver Means *the described action saves time.* You can save time by performing the action described in the paragraph.

Warning **Means *reader be warned.* In this situation, you might perform an action that could result in bodily injury.**

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

Preface

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

Figyelem

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

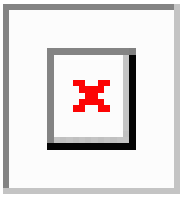
警告

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



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

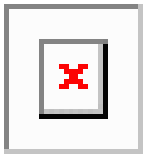
Advarsel

VIGTIGE SIKKERHEDSANVISNINGER

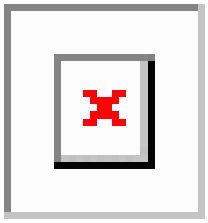
Dette advarselssymbol betyder fare. Du befinder dig i en situation med risiko for legemesbeskadigelse. Før du begynder arbejde på udstyr, skal du være opmærksom på de involverede risici, der er ved elektriske kredsløb, og du skal sætte dig ind i standardprocedurer til undgåelse af ulykker. Brug erklæringsnummeret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

GEM DISSE ANVISNINGER

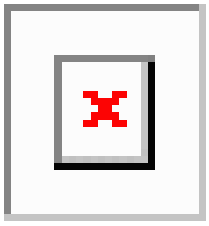
تحذير

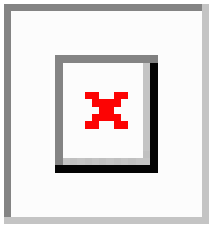


Upozorenje

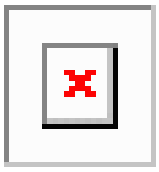


Upozornění

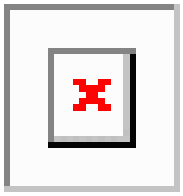




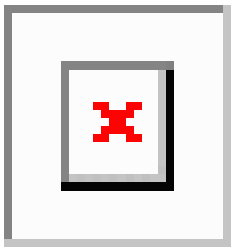
אזהרה



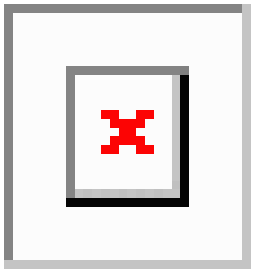
Opomena



Ostrzeżenie



Upozornenie



Related Documentation

Use this guide in conjunction with the following referenced Release 10.x publications:

- Release Notes for Cisco NCS 2000 Series, Release 10.x
- *Cisco NCS 2000 Series Line Card Configuration Guide*
- *Cisco NCS 2000 Series Network Configuration Guide*
- *Cisco NCS 2000 Series Licensing Configuration Guide*
- *Cisco NCS 2000 Series Hardware Installation Guide*
- *Cisco NCS 2000 Series TL1 Command Guide*
- *Cisco Transport Planner DWDM Operations Guide*
- Regulatory Compliance and Safety Information for Cisco NCS Platforms
- Electrostatic Discharge and Grounding Guide for Cisco NCS Platforms
- Installing the GBIC, SFP, SFP+, XFP, CXP, and CFP Optical Modules in Cisco NCS Platforms
- Installing the Cisco NCS 2000 Series Passive Optical Modules

For an update on End-of-Life and End-of-Sale notices, refer to

http://www.cisco.com/en/US/products/hw/optical/ps2006/prod_eol_notices_list.html

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

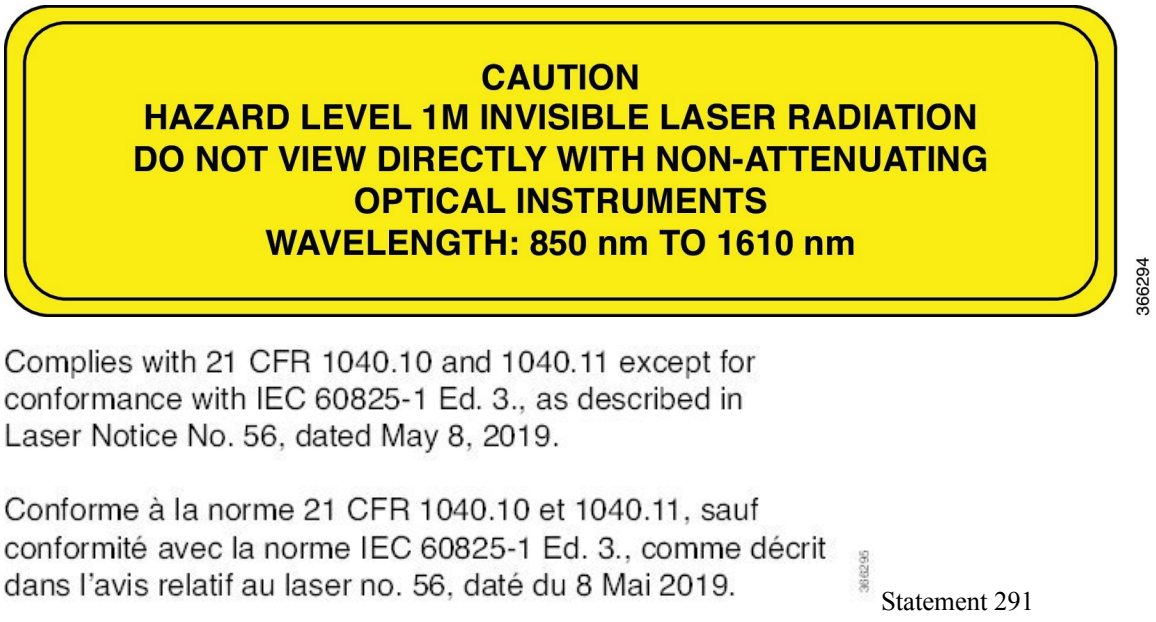
For safety and warning information, refer to the Regulatory Compliance and Safety Information document that accompanied the product. This publication describes the international agency compliance and safety information. It also includes translations of the safety warnings.

Safety Labels

Cisco NCS 2000 Series cards are classified as Laser Class 1 or 1M as per IEC 60825-1 and Hazard Level 1M as per IEC 60825-2.

Figure 1: Class 1M Laser Product Label

Figure 2: Class 1M Laser Product Label



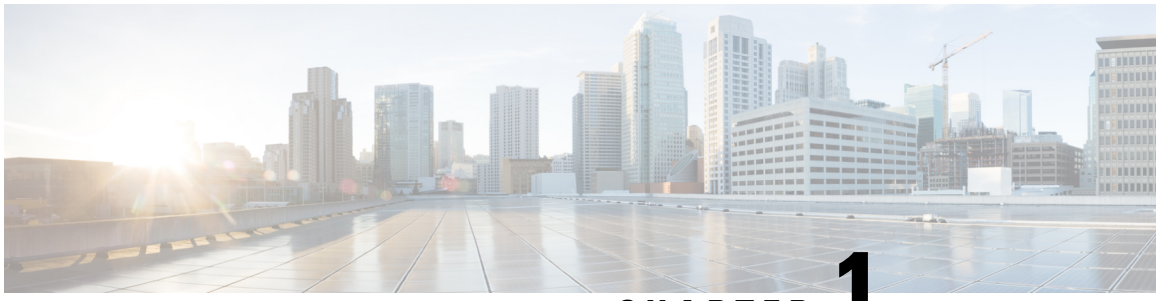
Statement 291

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.



CHAPTER 1

General Troubleshooting

This chapter provides procedures for troubleshooting the most common problems encountered when operating a DWDM shelf in ANSI or ETSI platforms. To troubleshoot specific alarms, see Alarm Troubleshooting, on page 85 If you cannot find what you are looking for, contact Cisco Technical Support (1 800 553-2447).

Alarms can occur even in those cards that are not explicitly mentioned in the Alarm sections. When an alarm is raised, refer to its clearing procedure.

This chapter includes the following sections on network problems:

Loopback Description

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 a 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 Alarm Troubleshooting, on page 85 chapter.

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.

Facility Loopbacks

The following sections give general information about facility loopback operations and specific information about card loopback activity.

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 3: Facility Loopback Path on a Near-End Transponder Card, on page 2 shows a facility loopback at a trunk port and at a client port on a TXP card.

Figure 3: 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.

Card Behavior

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

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 the following table, 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: DWDM Card Facility Loopback Behavior

Card/Port	Facility Loopback Signal
TXP_MR_10E/TXP_MR_10E_C/TXP_MR_10E_L client ports	Bridged
TXP_MR_10E/TXP_MR_10E_C/TXP_MR_10E_L trunk ports	Terminated
TXP_MR_2.5G/TXPP_MR_2.5G client ports	Terminated
TXP_MR_2.5G/TXPP_MR_2.5G trunk ports	Terminated
MXP_2.5G_10E_C/MXP_2.5G_10E_L client ports	Bridged
MXP_2.5G_10E_C/MXP_2.5G_10E_L trunk ports	Terminated
MXP_MR_10DME client ports	Terminated
MXP_MR_10DME trunk ports	Terminated
MXP_MR_2.5G/MXPP_MR_2.5G client ports	Bridged
MXP_MR_2.5G/MXPP_MR_2.5G trunk ports	Terminated
GE_XP/10GE_XP client ports	Terminated
GE_XP/10GE_XP trunk ports	Terminated
ADM-10G client ports	Bridged
ADM-10G trunk ports	Terminated
40G-MXP-C/40E-MXP-C/40ME-MXP-C client ports	Bridged
40G-MXP-C/40E-MXP-C/40ME-MXP-C trunk ports	Bridged
40E-TXP-C/40ME-TXP-C client ports	Bridged
40E-TXP-C/40ME-TXP-C trunk ports	Bridged
AR_XP/AR_MXP client ports	Terminated

Card/Port	Facility Loopback Signal
AR_XP/AR_MXP trunk 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 unless the default is set to alarm for loopback while in AS-MT.)

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 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.

When you apply a facility loopback on the GE_XP, 10GE_XP, GE_XPE, and 10GE_XPE cards, the ifInDiscard counters increment continuously.

Terminal Loopbacks

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

General Behavior

A terminal loopback tests a circuit path as it passes through a TXP, MXP, or ADM-10G card and loops back. For example, as shown in Figure 4: Terminal Loopback on a TXP Card, on page 4, 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 4: Terminal Loopback on a TXP Card

Card Behavior

The SDH terminal port loopbacks can either terminate or bridge the signal. TXP terminal loopbacks are terminated as shown in the following table. 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 the following table.

Note AIS signal is not injected if the signal is bridged. If the signal is terminated, an applicable AIS is injected downstream.

Table 2: DWDM Card Terminal Loopback Behavior

Card/Port	Terminal Loopback Signal
TXP_MR_10E/TXP_MR_10E_C/TXP_MR_10E_L client ports	Bridged
TXP_MR_10E/TXP_MR_10E_C/TXP_MR_10E_L trunk ports	Bridged
TXP_MR_2.5G/TXPP_MR_2.5G client ports	Bridged
TXP_MR_2.5G/TXPP_MR_2.5G trunk ports	Bridged
MXP_2.5G_10E_C/MXP_2.5G_10E_L client ports	Bridged
MXP_2.5G_10E_C/MXP_2.5G_10E_L trunk ports	Bridged
MXP_MR_10DME client ports	Bridged
MXP_MR_10DME trunk ports	Bridged
MXP_MR_2.5G/MXPP_MR_2.5G client ports	Bridged
MXP_MR_2.5G/MXPP_MR_2.5G trunk ports	Bridged
GE_XP/10GE_XP client ports	Bridged
GE_XP/10GE_XP trunk ports	Bridged
ADM-10G client ports	Bridged
ADM-10G trunk ports	Bridged
40G-MXP-C/40E-MXP-C/40ME-MXP-C client ports	Bridged
40G-MXP-C/40E-MXP-C/40ME-MXP-C trunk ports	Bridged
40E-TXP-C/40ME-TXP-C client ports	Bridged
40E-TXP-C/40ME-TXP-C trunk ports	Bridged
AR_XP/AR_MXP client ports	Bridged
AR_XP/AR_MXP trunk ports	Bridged

Important notes about loopback on MXP and TXP trunk and client ports:

- 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.
- For ADM-10G cards with Client Terminal Loopback on a SONET Client port, AIS-P is sent forward on client for the circuits on that port.
- For ADM-10G cards with a Terminal Loopback on a GE Client port, the client port is squelched.
- 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 ADM-10G cards with a Facility Loopback on the Trunk port, AIS-P is sent forward on all the SONET client ports.
- For ADM-10G cards with a Facility Loopback on the Trunk port, all the GE client ports is squelched
- For ADM-10G Terminal Loopback on the Trunk port, the signal is anyway sent downstream (drop and continue).
- 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 unless the default is set to alarm for loopback while in AS-MT.)

Troubleshooting MXP, TXP, XP, or ADM-10G 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, TXP, XP, or ADM-10G card loopback tests differ from other testing in that loopback testing does not require circuit creation. MXP, TXP, and XP 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, ADM-10G), muxponder, or xponder cards (MXP, MXPP, XP, ADM-10G) cards. The example in this section tests an MXP or TXP circuit on a three-node

bidirectional line switched ring (BLSR) or multiplex section-shared protection 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, TXP, XP, or ADM-10G 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.

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, TXP, XP, or ADM-10G port
2. A terminal loopback on the source-node MXP, TXP, XP, or ADM-10G port
3. A facility loopback on the intermediate-node MXP, TXP, XP, or ADM-10G port
4. A terminal loopback on the intermediate-node MXP, TXP, XP, or ADM-10G port
5. A facility loopback on the destination-node MXP, TXP, XP, or ADM-10G port
6. A terminal loopback on the destination-node MXP, TXP, XP, or ADM-10G port

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

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, transponder, xponder, or ADM-10G 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, TXP, XP, or ADM-10G port as a possible failure point. Figure 5: Facility Loopback on a Circuit Source MXP or TXP Port, on page 7 shows the facility loopback examples on source ONS node TXP ports (client and trunk).

Figure 5: 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, TXP, XP or ADM-10G Port, on page 8.

Create the Facility Loopback on the Source-Node MXP, TXP, XP or ADM-10G Port

Procedure

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 node view (single-shelf mode) or shelf view (multishelf mode), 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) , on page 256, LPBKFACILITY (FC) , on page 256, LPBKFACILITY (GE) , on page 257, LPBKFACILITY (ISC) , on page 258, or the LPBKFACILITY (TRUNK) , on page 258 to appear during loopback setup. The condition clears when you remove the loopback.

Step 9 Complete the Test and Clear the MXP, TXP, XP or ADM-10G Facility Loopback Circuit, on page 8.

Test and Clear the MXP, TXP, XP or ADM-10G Facility Loopback Circuit

Procedure

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.
f) Complete the Perform a Terminal Loopback on a Source-Node MXP, TXP, XP, or ADM-10G Port, on page 9.

Step 4 If the test set indicates errors, complete the Test the MXP, TXP, XP or ADM-10G Card, on page 9.

Test the MXP, TXP, XP or ADM-10G Card

Procedure

Step 1 Complete the Physically Replace a Card, on page 394 for the suspected bad card and replace it with a known-good one.

Warning **High-performance devices on this card can get hot during operation. To remove the card, hold it by the faceplate and bottom edge. Allow the card to cool before touching any other part of it or before placing it in an antistatic bag.** Statement 201

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 Protection Switching, Lock Initiation, and Clearing, on page 387. For more information, refer to the Maintain the Node chapter in the *Cisco NCS 2002 and NCS 2006 Network 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 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 5 Complete the Perform a Terminal Loopback on a Source-Node MXP, TXP, XP, or ADM-10G Port, on page 9.

Perform a Terminal Loopback on a Source-Node MXP, TXP, XP, or ADM-10G Port

The terminal loopback test is performed on the node source MXP, TXP, XP, or ADM-10G 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 6: Terminal

Loopback on a Source-Node MXP or TXP Port, on page 10 shows an example of a terminal loopback on a source TXP port and a client TXP port.

Figure 6: 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, TXP, XP, or ADM-10G Port, on page 10.

Create the Terminal Loopback on a Source-Node MXP, TXP, XP, or ADM-10G Port

Procedure

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 Perform a Facility Loopback on a Source-Node MXP or TXP Port, on page 7, leave the optical test set hooked up to the MXP, TXP, XP, or ADM-10G 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 (single-shelf mode) or shelf view (multishelf mode), 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, TXP, XP, or ADM-10G Port Terminal Loopback Circuit, on page 11.

Test and Clear the MXP, TXP, XP, or ADM-10G Port Terminal Loopback Circuit

Procedure

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.
g) Complete the Create a Facility Loopback on an Intermediate-Node MXP or TXP Port, on page 12.

Step 4 If the test set indicates errors, complete the Test the MXP, TXP, XP, or ADM-10G Card, on page 11.

Test the MXP, TXP, XP, or ADM-10G Card

Procedure

Step 1 Complete the Physically Replace a Card, on page 394 for the suspected bad card and replace it with a known-good one.

Warning **High-performance devices on this card can get hot during operation. To remove the card, hold it by the faceplate and bottom edge. Allow the card to cool before touching any other part of it or before placing it in an antistatic bag.** Statement 201

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 Protection Switching, Lock Initiation, and Clearing, on page 387.

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 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 5 Complete the Create a Facility Loopback on an Intermediate-Node MXP or TXP Port, on page 12.

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 7: Facility Loopback on an Intermediate-Node MXP or TXP Port, on page 12, the test is being performed on an intermediate MXP or TXP port.

Figure 7: 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, on page 12.

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

Procedure

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 Perform a Terminal Loopback on a Source-Node MXP, TXP, XP, or ADM-10G Port, on page 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 (single-shelf mode) or shelf view (multishelf mode), 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, on page 13.

Test and Clear the MXP or TXP Port Facility Loopback Circuit

Procedure

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.
f) Complete the Create a Terminal Loopback on Intermediate-Node MXP or TXP Ports, on page 14.

Step 4 If the test set indicates errors, complete the Test the MXP or TXP Card, on page 13.

Test the MXP or TXP Card

Procedure

Step 1 Complete the Physically Replace a Card, on page 394 for the suspected bad card and replace it with a known-good one.

Warning **High-performance devices on this card can get hot during operation. To remove the card, hold it by the faceplate and bottom edge. Allow the card to cool before touching any other part of it or before placing it in an antistatic bag.** Statement 201

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 Protection Switching, Lock Initiation, and Clearing, on page 387.

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 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 5 Complete the Create a Terminal Loopback on Intermediate-Node MXP or TXP Ports, on page 14.

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 8: Terminal Loopback on an Intermediate-Node MXP or TXP Port, on page 14, 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 8: 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, on page 14.

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

Procedure

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 Create a Facility Loopback on an Intermediate-Node MXP or TXP Port, on page 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 node view (single-shelf mode) or shelf view (multishelf mode) of the intermediate node:

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

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

b) In node view (single-shelf mode) or shelf view (multishelf mode), 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, on page 15.

Test and Clear the MXP or TXP Terminal Loopback Circuit

Procedure

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.
g) Complete the Perform a Facility Loopback on a Destination-Node MXP, TXP, XP, or ADM-10G Port, on page 16.
Step 4 If the test set indicates errors, complete the Test the MXP or TXP Card, on page 15.

Test the MXP or TXP Card

Procedure

Step 1 Complete the Physically Replace a Card, on page 394 for the suspected bad card and replace it with a known-good one.

Warning **High-performance devices on this card can get hot during operation. To remove the card, hold it by the faceplate and bottom edge. Allow the card to cool before touching any other part of it or before placing it in an antistatic bag.** Statement 201

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 Protection Switching, Lock Initiation, and Clearing, on page 387.

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 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 5 Complete the Perform a Facility Loopback on a Destination-Node MXP, TXP, XP, or ADM-10G Port, on page 16.

Perform a Facility Loopback on a Destination-Node MXP, TXP, XP, or ADM-10G 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 9: Facility Loopback on a Destination-Node MXP or TXP Port, on page 16 shows a facility loopback being performed on a TXP client or trunk port at a destination node.

Figure 9: 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, TXP, XP, or ADM-10G Port, on page 17.

Create the Facility Loopback on a Destination-Node MXP, TXP, XP, or ADM-10G Port

Procedure

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 Create a Terminal Loopback on Intermediate-Node MXP or TXP Ports, on page 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 (single-shelf mode) or shelf view (multishelf mode) of the destination node:
   - Choose **View > Go To Other Node** from the menu bar.
   - Choose the node (or shelf) from the drop-down list in the Select Node dialog box and click **OK.**
b) In node view (single-shelf mode) or shelf view (multishelf mode), 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, TXP, XP, or ADM-10G Facility Loopback Circuit, on page 17.

Test and Clear the MXP, TXP, XP, or ADM-10G Facility Loopback Circuit

Procedure

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.
f) Complete the Perform a Terminal Loopback on a Destination-Node MXP, TXP, XP, or ADM-10G Port, on page 18.

Step 4 If the test set indicates errors, complete the Test the MXP, TXP, XP, or ADM-10G Card, on page 18.

Test the MXP, TXP, XP, or ADM-10G Card

Procedure

Step 1 Complete the Physically Replace a Card, on page 394 for the suspected bad card and replace it with a known-good one.

Warning **High-performance devices on this card can get hot during operation. To remove the card, hold it by the faceplate and bottom edge. Allow the card to cool before touching any other part of it or before placing it in an antistatic bag.** Statement 201

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 Protection Switching, Lock Initiation, and Clearing, on page 387.

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 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 5 Complete the Perform a Terminal Loopback on a Destination-Node MXP, TXP, XP, or ADM-10G Port, on page 18.

Perform a Terminal Loopback on a Destination-Node MXP, TXP, XP, or ADM-10G 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 10: Terminal Loopback on a Destination-Node MXP or TXP Port, on page 19 shows a terminal loopback on an destination node TXP port.

Figure 10: 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, TXP, XP, or ADM-10G Port, on page 19.

Create the Terminal Loopback on a Destination-Node MXP, TXP, XP, or ADM-10G Port

Procedure

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 Perform a Facility Loopback on a Destination-Node MXP, TXP, XP, or ADM-10G Port, on page 16, 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 LPBKFACILITY (ESCON) , on page 256, LPBKFACILITY (FC) , on page 256, LPBKFACILITY (GE) , on page 257, LPBKFACILITY (ISC) , on page 258, or the LPBKFACILITY (TRUNK) , on page 258 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 (single-shelf mode) or shelf view (multishelf mode) of the destination node:
   - Choose **View** > **Go To Other Node** from the menu bar.
   - Choose the node (or shelf) from the drop-down list in the Select Node dialog box and click **OK**.
b) In node view (single-shelf mode) or shelf view (multishelf mode), 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, TXP, XP, or ADM-10G Terminal Loopback Circuit, on page 20.

Test and Clear the MXP, TXP, XP, or ADM-10G Terminal Loopback Circuit

Procedure

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, TXP, XP, or ADM-10G Card, on page 20.

Test the MXP, TXP, XP, or ADM-10G Card

Procedure

Step 1 Complete the Physically Replace a Card, on page 394 for the suspected bad card and replace it with a known-good one.

Warning **High-performance devices on this card can get hot during operation. To remove the card, hold it by the faceplate and bottom edge. Allow the card to cool before touching any other part of it or before placing it in an antistatic bag.** Statement 201

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 Protection Switching, Lock Initiation, and Clearing, on page 387.

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 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.

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.

ITU-T G.709 Monitoring in Optical Transport Networks

ITU-T Recommendation 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 11: Optical Transport Network Layers, on page 21). This structure enables localized monitoring that helps you isolate and troubleshoot network problems.

Figure 11: Optical Transport Network Layers

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:

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).

A second overhead is added to the OPUk unit to create the optical channel data unit (ODUk).

A third overhead including forward error correction (FEC) is added to the ODUk to create the optical channel transport unit (OTUk).

A fourth overhead is added to the OTUk to create the entire OCH layer.

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.

Optical Transmission Section Layer

The optical transmission section (OTS) layer supports monitoring partial spans of a network 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

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 12: Performance Monitoring Points on ONS DWDM, on page 22 illustrates the PM read points that are useful in identifying DWDM circuit points of failure. The Performance Monitoring chapter in the *Cisco ONS 15454 DWDM Reference Manual*Monitor Performance document 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 might vary according to your configuration.

Note When LOS, LOS-P, or LOF alarms occur on TXP and MXP trunks, G709/SONET/SDH TCAs are suppressed. For details, see the Alarm and TCA Monitoring and Management chapter in the *Cisco ONS 15454 DWDM Procedure Guide* Alarm and TCA Monitoring and Management document.

Figure 12: 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. The Performance Monitoring chapter in the *Cisco ONS 15454 DWDM Reference Manual*Monitor Performance document 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.

Procedure

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **Defaults** tabs.

Step 2 In the Defaults Selector field, click the 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.

Procedure

Step 1 In node view (single-shelf mode) or shelf view (multishelf mode), double-click the applicable card (TXP, MXP, or XP.)

Step 2 Click the **Provisioning** > **OTN** > **G.709 Thresholds** tabs.

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.

Procedure

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

Step 2 In the TL1 command line, enter a command using 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 OCH, 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 that 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 ONS SONET TL1 Command Guide* and *Cisco ONS SDH TL1 Command Guide* .

Provision Optical TCA Thresholds

Complete the following procedure to provision TCA thresholds in CTC.

Procedure

Step 1 In card view, click the **Provisioning > Optics Thresholds** tabs.

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.

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-WORDSThe 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

Procedure

Step 1 In node view (single-shelf mode) or shelf view (multishelf mode), double-click a transponder, muxponder, or xponder card to open the card view.

Step 2 Click the **Provisioning > OTN > FEC Thresholds** tabs.

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**.

Sample Trouble Resolutions

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

Problem There is a BBE TCA on a single transponder pair.

Possible Cause The transponder input power is out of range.

Solution 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.

Solution Check the connector on the trunk port.

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

Solution 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.

Solution 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.

Solution If an optical channel bypass exists along the line, check the connectors.

Problem 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.

Solution 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.

Solution 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.

Solution 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.

Solution 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.

Solution If an optical band bypass exists along the line, check the band connectors.

Problem 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.

Solution The problem is in the intercabinet signal path preceding the transponder.

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

Possible Cause The laser of the transponder is degrading.

Solution The problem is within the laser circuitry. Check the OPT-PRE, OPT-BST, OPT-AMP-C, and OPT-AMP-17C optical amplifier cards.

Using CTC Diagnostics

In Software Release 9.1, CTC provides diagnostics for the following functions:

- Verifying proper card application-specific integrated circuit (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 functionsverifying card LED function, creating bidirectional diagnostic circuits, and also downloading diagnostic files for technical supportare available to the user in the node view (single-shelf mode) or shelf view (multishelf mode) **Maintenance > Diagnostic** tab. The user-operated diagnostic features are described in the following paragraphs.

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 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

Procedure

Step 1 In node view (single-shelf mode) or shelf view (multishelf mode), click the **Maintenance > Diagnostic** tabs.

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

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

Retrieve Tech Support Logs Button

When you click the **Retrieve Tech Support Logs** button in the Diagnostics tab of the Maintenance window, CTC retrieves system data that a Retrieve or higher level user can off-load to a local directory and send 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 procedure to off-load the diagnostics file.

Note In addition to the machine-readable diagnostics file, the system stores an audit trail of all system events such as user log-ins, remote log-ins, configuration, and changes. This audit trail is considered a record-keeping feature rather than a troubleshooting feature.

Off-Load the Diagnostics File

Note The diagnostics operation is performed at a shelf level. Only single-node-related diagnostic information can be downloaded at a time.

The diagnostic files retrieved by CTC depends on the user privilege levels. Table 3: Diagnostic Files Retrieved Based on User Privilege, on page 27 lists the user privilege levels and the diagnostic retrieval operations they can perform.

Table 3: Diagnostic Files Retrieved Based on User Privilege

User Privilege Level	Diagnostic File Retrieval Operation
Retrieve	• Export the unfiltered alarm table contents • Export the unfiltered conditions table contents • Export the unfiltered history table contents • Export the inventory table contents • CTC Dump Diagnostics log

User Privilege Level	Diagnostic File Retrieval Operation
Maintenance	• All Retrieve level access operations • Save the node database
Provisioning	• All Maintenance level access operations • Retrieve and save the node-level diagnostics report. (If secure mode is not set on the node.) • Export the audit table contents. (If the NODE.security.grantPermission.RetrieveAuditLog NE Default is set to Provisioning.)
Superuser	• All Provisioning level access operations • Retrieve and save the node-level diagnostics report • Export the audit table contents

Procedure

Step 1 In the node view, click the **Maintenance > Diagnostic** tabs.

Step 2 Click **Retrieve Tech Support Logs** in the Controller area.

Step 3 In the Select a Filename for the Tech Support Logs Zip Archive dialog box, add the diagnostics file name in the format **TechSupportLogs**_<*node_name*>**.zip** by default. Substitute the last 20 alphanumeric characters of the node name for <*node_name*>. Navigate to the directory (local or network) where you want to save the file.

A message appears asking you if you want to overwrite any existing disgnostics file in the selected directory.

Step 4 Click **Save.**

CTC performs the diagnostic tasks and writes the diagnostic files in a folder named TechSupportLogs_<*node_name*> under the location selected in Step Step 3, on page 28. After all the diagnostic files are written to the TechSupportLogs_<*node_name*> **folder**, CTC archives the retrieved diagnostic files as TechSupportLogs_<*node_name*>.zip. CTC deletes the **TechSupportLogs**_<*node_name*> **folder** after the archiving process is successfully completed. CTC retains this folder if the archiving process fails. The retrieved diagnostic files can be accessed in the **TechSupportLogs_**<*node_name*> **folder.**

A progress bar indicates the percentage of the file that is being saved. The Save Tech Support Logs Completed dialog box appears when the file is saved. CTC logs any error during the retrieval and archiving of diagnostics file to the CTC Alerts Log.

Table 4: List of Diagnostic Files, on page 28 lists the diagnostic files retrieved by CTC.

Table 4: List of Diagnostic Files

Diagnostic File	Diagnostic File Content
AlarmTableLog.html	Alarm Table export

Diagnostic File	Diagnostic File Content
HistoryTableLog.html	Alarm Table export
ConditionsTableLog.html	Conditions Table export
InventoryTableLog.html	Inventory Table export
AuditTableLog.html	Audit Table export
CTCDumpDiagLog.txt	Audit Table export
NodeDiagnostics.bin	NodeDiagnostics.gz
OBFLDiagnostics.bin	OBFLDiagnostics.bin
NodeDatabaseBackup.bin	Database backup
TechSupportLogs_<*node_name*>.zip	Zip archive of all the diagnostics file

Step 5 Click **OK.**

Data Communications Network Tool

CTC contains a data communications network (DCN) tool that assists with network troubleshooting for Open Shortest Path First (OSPF) networks. It executes an internal dump command to retrieve information about all nodes accessible from the entry point.

The dump, which provides the same information as a dump executed by special networking commands, is available at the network view in the **Maintenance > Diagnostic** tab. You can select the access point node in the Select Node drop-down list. To create the dump, click **Retrieve**. (To clear the dump, click **Clear**.)

The contents of the dump file can be saved or printed and furnished to Cisco Technical Support for use in OSPF network support.

Onboard Failure Logging

Onboard Failure Logging (OBFL) records events that occur during the card operation. In the event of card failure, the stored log can assist in determining root cause of failure. The OBFL data is stored in two different formats:

- Run time log for IO cards
- Snapshot log for IO cards

The OBFL feature is supported on the following cards:

- OPT-BST
- OPT-PRE
- 40-SMR1-C

- 40-SMR2-C
- 40G-MXP-C
- 80-WXC-C

Note To determine if OBFL is supported on the OPT-BST and OPT-PRE cards running in your system, contact the Cisco Technical Assistance Center (TAC).

Note The stored logs can be retrieved only by the Cisco support team to diagnose the root cause of the card failure.

Run Time Log for IO Cards

Run time log traces events and critical information such as alarms raised and cleared, power variations and so on, during the working of the card. The stored logs help identify the cause of failure.

For legacy cards (OPT-BST and OPT-PRE), the run time logs are automatically stored in RAM and are deleted when the card is hard reset. To store the logs in the permanent memory, the user should take the snapshot of logs as explained in the Snapshot Logging in CTC, on page 31 section. For new cards (40-SMR1-C and 40-SMR2-C), the run time logs are automatically written to the flash memory and are not deleted even after reset or hard reboot of the card.

The following table lists a few run time logs captured for a specific event:

Table 5: Run Time Logging—Events and Logs

Event	Log
When the change in Rx and Tx optical power in the active stage is greater than the threshold value, the unit stores the input and output power every second. The difference between the two adjacent input power readings or two adjacent output power readings is greater than 1 db, and this event occurs more than 10 times in 30 seconds	• Input power of all the active stages (1 for the BST, 2 for the PRE) • Output power of all the active stages (1 for the BST, 2 for the PRE)
Target power not reached (0.5 dB or more difference from set point)	• Module status • Laser pump current—set point and value • Laser pump power—set point and value • DCU loss • VOA loss • Optical power values

Event	Log
Fiber Temperature Alarm	• Temperature of the case • Temperature of the laser
Laser Temperature Alarm	• Temperature of the case • Temperature of the fiber
Case Temperature Alarm	• Temperature of the case • Temperature of the fiber
Communication error with TCC	• FPGA dump • E2PROM dump

Snapshot Log for IO Cards

Snapshot log captures the board's information at any given time. In CTC, the user has an option to take a snapshot of the current status of the card. When the snapshot is taken, a log file will be created that contains the information from the card. In addition to the information stored in the run time logs, the snapshot log contains details like card parameters, alarm history, and so on. For legacy and new cards, the snapshot logs are written to the flash memory. When EQPT-FAIL alarm is detected on the card, a snapshot of the log will be automatically taken by the card. In the event of card failure due to other reasons, the users must take the snapshot of logs before swapping the card. Refer to the Snapshot Logging in CTC, on page 31 section.

Snapshot Logging in CTC

The users can take the snapshot of logs in the event of card failure, before replacing the card. This section explains the steps to take snapshot of logs in CTC:

Procedure

Step 1 Login to CTC.

Step 2 In node view (single-shelf mode) or shelf view (multishelf mode), double-click the card to open it in the card view.

Step 3 Click the **Maintenance** > **OBFL** tabs.

Step 4 Click **Start Onboard Failure logging**. The OBFL Info dialog box is displayed.

Step 5 Click **Yes** to continue. The Onboard failure logging feature is launched.

Step 6 Click **OK**. The snapshot log will be written to the flash memory.

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.

Restore the Node Database

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

Possible Cause Incorrect or corrupted node database.

Solution Complete the procedures in the Maintain the Node chapter of the configuration guide.

PC Connectivity Troubleshooting

This section contains information about system minimum requirements, supported platforms, browsers, and Java Runtime Environments (JREs) for Software R9.2.1 and R9.2.29.6.x 9.8, and troubleshooting procedures for PC and network connectivity to the chassis. Table 6: Computer Requirements for CTC lists the requirements for PCs and UNIX workstations. In addition to the JRE, the Java plug-in is also included on the software CD.

Table 6: Computer Requirements for CTC

Area	Requirements	Notes
Processor (PC only)	Pentium Dual-Core processor or equivalent	A faster CPU is recommended if your workstation runs multiple applications or if CTC manages a network with a large number of nodes and circuits.
RAM	2 GB RAM or more	A minimum of 2 GB is recommended if your workstation runs multiple applications or if CTC manages a network with a large number of nodes and circuits.
Hard drive	20 GB hard drive with 250 MB of free space required	CTC application files are downloaded from the TNC/TSC/TNCS/TNCS-O to your computer. These files occupy around 100MB (250MB to be safer) or more space depending on the number of versions in the network.

Area	Requirements	Notes
Operating System	• PC: Windows 2000, Windows XP, Windows Vista, Windows XP, Windows 7, Windows Server 2003 and 2008. • Workstation: Solaris versions 9 or 10 on an UltraSPARC-III or faster processor, with a minimum of 1 GB RAM and a minimum of 250 MB of available hard drive space. • Apple Mac OS X. CTC needs to be installed using the CacheInstaller available on CCO or the ONS CD.	Use the latest patch/Service Pack released by the OS vendor. Check with the vendor for the latest patch/Service Pack.
Java Runtime Environment	• JRE 1.6 • JRE 1.7 (R9.4 and later releases)	JRE 1.6 is installed by the CTC Installation Wizard included on the software CD. JRE 1.6 provides enhancements to CTC performance, especially for large networks with numerous circuits. We recommend that you use JRE 1.6 for networks with Software R9.2 nodes. If CTC must be launched directly from nodes running software R7.0 or R7.2, We recommend JRE 1.4.2 or JRE 5.0. If CTC must be launched directly from nodes running software R5.0 or R6.0, we recommend JRE 1.4.2. If CTC must be launched directly from nodes running software earlier than R5.0, we recommend JRE 1.3.1_02.
Web browser	• PC: Internet Explorer 8.x, 9.x (R9.6 and later releases), 10 (R9.4.0.3, R9.6.0.3 and later releases) 11 (R9.8 and later releases) • UNIX Workstation: Mozilla 1.7 • MacOS-X PC: Safari	For the PC, use JRE 1.6 or JRE 1.7 with any supported web browser. The supported browser can be downloaded from the Web.

Area	Requirements	Notes
Cable	• User-supplied CAT-5 straight-through cable with RJ-45 connectors on each end to connect the computer to the chassis directly or through a LAN. • User-supplied cross-over CAT-5 cable to the DCN port on the patch panel or to the Catalyst 2950 (multishelf mode)	—

Unable to Verify the IP Configuration of Your PC

Problem When connecting your PC to the system, 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.

Solution 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, on page 34.

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

Solution Verify the IP configuration of your PC. Complete the Verify the IP Configuration of Your PC, on page 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

Procedure

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.

Browser Login Does Not Launch Java

Problem 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.

Solution 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, on page 35 and the Reconfigure the Browser, on page 35.

Reconfigure the PC Operating System Java Plug-in Control Panel

Procedure

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 software CD.
b) Open the *CD-drive*:\Windows\JRE folder.
c) Double-click the **j2re-1_6-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 1.6** icon.

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

Step 6 Navigate to **C:\ProgramFiles\JavaSoft\JRE\1.6**.

Step 7 Select **JRE 1.6**.

Step 8 Click **Apply**.

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

Reconfigure the Browser

Procedure

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 2.f, on page 36, 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 Browser Stalls When Downloading CTC JAR Files From Control Card, on page 40.

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 system.

Unable to Verify the NIC Connection on Your PC

Problem When connecting your PC to the system, 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.

Solution 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.

Solution 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.

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

Solution If connecting directly to your laptop, a PC, or a router, use a straight-through CAT-5 cable. When connecting the chassis to a hub or a LAN switch, use a crossover CAT-5 cable. For details on the types of CAT-5 cables, see the Crimp Replacement LAN Cables, on page 49.

Possible Cause The NIC is improperly inserted or installed.

Solution 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.

Solution 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.

Verify PC Connection to the NCS (ping)

Problem The TCP/IP connection was established and then lost.

Possible Cause A lost connection between the PC and the system.

Solution Use a standard ping command to verify the TCP/IP connection between the PC and the card. A ping command should work if the PC connects directly to the control card or uses a LAN to access the control card. Complete the Ping the NCS, on page 37.

Ping the NCS

Procedure

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 *IP-address*

For example:

ping 198.168.10.10

Step 3 If the workstation has connectivity to the NCS, 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 NCS through a LAN, check that the workstation 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 NCS, check that the link light on the workstation NIC is illuminated.

The IP Address of the Node is Unknown

Problem 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.

Solution Leave one control card in the shelf. Connect a PC directly to the remaining control card and perform a hardware reset of the card. The control 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, on page 38.

Retrieve Unknown Node IP Address

Procedure

Step 1 Connect your PC directly to the active control 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 control card.

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

CTC Operation Troubleshooting

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

CTC Colors Do Not Appear Correctly on a UNIX Workstation

Problem 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.

Solution 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, on page 38. If the problem persists after limiting Netscape colors, exit any other color-intensive applications in use.

Limit Netscape Colors

Procedure

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)

Unable to Launch CTC Help After Removing Netscape

Problem 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.

Solution 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 CTCInternet Explorer resetting as default browserresetting Internet Explorer as the default browser, on page 39 to associate the CTC Help files to the correct browser.

Reset Internet Explorer as the Default Browser for CTC

Procedure

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 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.

Unable to Change Node View to Network View

Problem 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 (single-shelf mode) or shelf view (multishelf mode) 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.

Solution 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, on page 40 or the Set the CTC_HEAP and CTC_MAX_PERM_SIZE_HEAP Environment Variables for Solaris, on page 40 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 4 GB of RAM. If your system does not have a minimum of 4 GB of RAM, contact the Cisco Technical Assistance Center (TAC).

Procedure

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 `896` 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 `256` 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

Procedure

Step 1 From the user shell window, kill any CTC sessions and browser 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 896
% setenv CTC_MAX_PERM_SIZE_HEAP 256
```

Browser Stalls When Downloading CTC JAR Files From Control Card

Problem The browser stalls or hangs when downloading a CTC Java archive (JAR) file from the control 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.

Solution Disable the VirusScan Download Scan feature. Complete the Disable the VirusScan Download Scan, on page 41.

Disable the VirusScan Download Scan

Procedure

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.

CTC Does Not Launch

Problem 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.

Solution Redirect the Netscape cache to a valid directory. Complete the Redirect the Netscape Cache to a Valid Directory, on page 41.

Redirect the Netscape Cache to a Valid Directory

Procedure

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.

Slow CTC Operation or Login Problems

Problem You experience slow CTC operation or have problems logging into CTC.

Problem Table 7: Slow CTC Operation or Login Problems, on page 42 describes the potential cause of the symptom and the solution.

Table 7: 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 NCS to download a new set of Java archive (JAR) files to your computer hard drive. Complete the Delete the CTC Cache File Automatically, on page 42 or the Delete the CTC Cache File Manually, on page 43.
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, on page 40 or the Set the CTC_HEAP and CTC_MAX_PERM_SIZE_HEAP Environment Variables for Solaris, on page 40. **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

Before you begin

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.

Procedure

Step 1 Enter an NCS 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.

Delete the CTC Cache File Manually

Before you begin

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.

Procedure

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 control card.

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

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

Node Icon is Gray on CTC Network View

Problem 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.

Solution Correct the core version build as described in the Different CTC Releases Do Not Recognize Each Other, on page 44.

Possible Cause Username and password do not match.

Solution Correct the username and password as described in the Username or Password Do Not Match, on page 45.

Possible Cause A lost DCC connection.

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

Java Runtime Environment Incompatible

Problem The CTC application does not run properly.

Possible Cause The compatible Java JRE is not installed.

Solution 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 NCS 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 NCS software CD. Complete the Launch CTC to Correct the Core Version Build, on page 45. 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. The following table shows JRE compatibility with NCS software releases.

Table 8: JRE Compatibility for NCS

Software Release	JRE 1.2.2	JRE 1.3	JRE 1.4	JRE 5.0	JRE 1.6	JRE 1.7
NCS R10.0	No	No	No	No	Yes	Yes

Note Software Release 4.0 notifies you if an earlier JRE version is running on your PC or UNIX workstation.

Launch CTC to Correct the Core Version Build

Procedure

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

Step 2 Start the browser.

Step 3 Enter the NCS 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.

Different CTC Releases Do Not Recognize Each Other

Problem 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 control card are incompatible.

Solution This occurs when the control card 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, on page 45.

Note **Solution** 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

Procedure

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

Step 2 Start the browser.

Step 3 Enter the 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.

Username or Password Do Not Match

Problem 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 control card.

Solution 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 NCS, enter the CISCO15 user name in capital letters, click **Login**, and use the password **otbu+1**, which is case-sensitive.

Solution Complete the Verify Correct Username and Password, on page 45. If the node has been configured for Remote Authentication Dial In User Service (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 Security Reference document.

Verify Correct Username and Password

Procedure

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.

DCC Connection Lost

Problem 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.

Solution Usually accompanied by an EOC alarm. Clear the EOC alarm and verify the DCC connection as described in the Alarm Troubleshooting, on page 85.

Path in Use Error When Creating a Circuit

Problem 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.

Solution 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.

Calculate and Design IP Subnets

Problem You cannot calculate or design IP subnets on the NCS.

Possible Cause The IP capabilities of the NCS require specific calculations to properly design IP subnets.

Solution Cisco provides a free online tool to calculate and design IP subnets. Go to http://www.cisco.com/techtools/ip_addr.html.

Timing

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

NCS Switches Timing Reference

Problem 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.

Solution The NCS internal clock operates at a Stratum 3E level of accuracy. This gives the NCS 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. NCS 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.

Holdover Synchronization Alarm

Problem The clock is running at a different frequency than normal and the HLDOVRSYNC , on page 198 appears.

Possible Cause The last reference input has failed.

Solution 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 , on page 198 for a detailed description.

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

Free-Running Synchronization Mode

Problem The clock is running at a different frequency than normal and the FRNGSYNC , on page 182 appears.

Possible Cause No reliable reference input is available.

,

Solution 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 , on page 182 for a detailed description.

Daisy-Chained BITS Not Functioning

Problem You are unable to daisy chain the BITS sources.

Possible Cause Daisy-chained BITS sources are not supported on the NCS.

Solution 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 NCS.

Blinking STAT LED after Installing a Card

Problem 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.

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 Alarm Troubleshooting, on page 85 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 Alarm Troubleshooting, on page 85.

Solution

Warning **Solution High-performance devices on this card can get hot during operation. To remove the card, hold it by the faceplate and bottom edge. Allow the card to cool before touching any other part of it or before placing it in an antistatic bag.** Statement 201

Caution **Solution** 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 Alarm Troubleshooting, on page 85.

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.

Bit Errors Appear for a Traffic Card

Problem A traffic card has multiple bit errors.

Possible Cause Faulty cabling or low optical-line levels.

Solution 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 NCS. Troubleshoot low optical levels using the Faulty Fiber-Optic Connections, on page 48.

Faulty Fiber-Optic Connections

Problem A card has multiple alarms and/or signal errors.

Possible Cause Faulty fiber-optic connections. Fiber connection problems usually occur in conjunction with alarms.

Solution Refer to the appropriate trouble-clearing procedure in Alarm Troubleshooting, on page 85

Possible Cause Faulty CAT-5 cables.

Solution Faulty CAT-5 cables can be the source of alarms and signal errors. Complete the Crimp Replacement LAN Cables, on page 49.

Possible Cause Faulty Gigabit Interface Converters (GBICs).

Solution Faulty GBICs can be the source of alarms and signal errors. See the Replace Faulty SFP, SFP+, or XFP Connectors, on page 50.

Warning **Invisible laser radiation may be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments.** Statement 1051.

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

Crimp Replacement LAN Cables

You can crimp your own LAN cables for use with the NCS. Use a cross-over cable when connecting an NCS to a hub, LAN modem, or switch, and use a LAN cable when connecting an NCS to a router or workstation. Use CAT-5 cable RJ-45 T-568B, Color Code (100 Mbps), and a crimping tool. Figure 13: RJ-45 Pin Numbers, on page 49 shows the wiring of an RJ-45 connector. Table 9: LAN Cable Pinout, on page 49Figure 15: Cross-Over Cable Layout, on page 50 shows a LAN cable layout, and Table 9: LAN Cable Pinout, on page 49 shows the cable pinouts. Figure 15: Cross-Over Cable Layout, on page 50 shows a cross-over cable layout, and Table 10: Cross-Over Cable Pinout, on page 50 shows the cross-over pinouts.

Figure 13: RJ-45 Pin Numbers

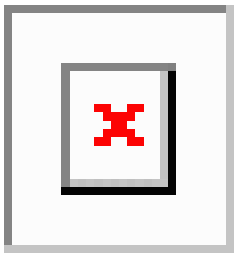


Figure 14: LAN Cable Layout

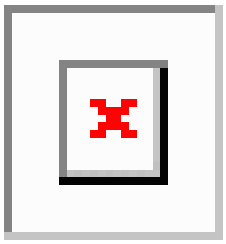


Table 9: LAN Cable Pinout

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

Pin	Color	Pair	Name	Pin
7	white/brown	4	—	7
8	brown	4	—	8

Figure 15: Cross-Over Cable Layout

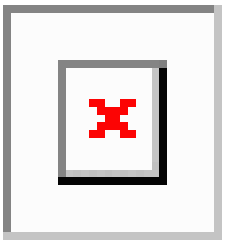


Table 10: Cross-Over Cable Pinout

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.

Replace Faulty SFP, SFP+, or XFP Connectors

Small Form-factor Pluggable (SFP), Enhanced Small Form-factor Pluggable (SFP+), and 10-Gbps SFP (called XFP) modules are input/output devices that plug into some DWDM cards to link the port with the fiber-optic network. The type of SFP, SFP+, or XFP determines the maximum distance that traffic can travel from the card to the next network device. For a description of SFP, SFP+, and XFP modules and their capabilities, refer to the Installing the GBIC, SFP, SFP+, and XFP Optical Modules in Cisco ONS Platforms. SFP, SFP+, and XFP modules are hot-swappable and can be installed or removed while the card or shelf assembly is powered and running.

Warning **Invisible laser radiation may be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments.** Statement 1051.

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

Note SFP, SFP+, and XFP modules must be matched on both ends by type: SX to SX, LX to LX, or ZX to ZX.

Remove SFP or XFP Connectors

Before you begin

Warning **Invisible laser radiation may be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments.** Statement 1051.

Procedure

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, SFP+, or XFP Connector

Before you begin

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 **Class 1 laser product.** Statement 1008

Procedure

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

Step 2 Check the label to verify that you are using a compatible SFP, SFP+, or XFP for the card where you want to install the connector. For a list of the SFP, SFP+, and XFP modules that are compatible with each card, refer to the Installing the GBIC, SFP, SFP+, and XFP Optical Modules in Cisco ONS Platforms document.

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

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

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

To change the payload type of an SFP, SFP+, or XFP (called pluggable port modules [PPMs] in CTC), refer to the Provision Transponder and Muxponder Cards chapter in the Configuration guide.

Power Supply Problems

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

Problem 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.

Solution The NCS 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 NCS that is not properly connected to its power supply does not operate. Power problems can be confined to a specific NCS 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 NCS to default to January 1, 1970, 00:04:15. To reset the clock, in node view (single-shelf mode) or shelf view (multishelf mode) click the **Provisioning > General > General** tab and change the Date and Time fields. Complete the Isolate the Cause of Power Supply Problems, on page 53.

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 NCS are service-affecting.

Isolate the Cause of Power Supply Problems

Procedure

Step 1 If a single NCS 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 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 NCS 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.

Power Up Problems for Node and Cards

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

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

Possible Cause Improper power supply.

Solution Refer to the power information in the Hardware Specifications appendix of the *Cisco ONS 15454 DWDM Reference Manual*Hardware Specifications document.

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

System Restart after a Fiber Cut

When the network ALS setting is Auto Restart, the system automatically restarts after a fiber cut occurs. 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:

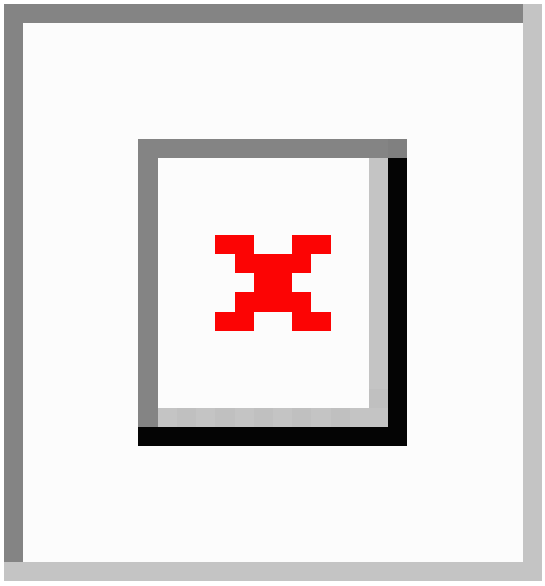
1. Span loss increased:
   - Span loss change > 5 dBm
   - OSC power value on the receiver < –42 dBm
2. Span loss increased:
   - Span loss change > 5 dBm
   - OSC power value on the receiver > –42 dBm
3. Span loss increased: 3 dBm < span loss change < 5 dBm
4. Span loss increased: span loss change < 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-RXPOWER section in the chapter).

The symptoms of the possible span loss scenarios (except for span loss decrease) are described in the following paragraphs. Refer to the linear network given below during the discussion of the scenarios.

Figure 16: Linear Network, With No Fiber Cut



The basic assumption is that the network ALS feature (for feature details, refer to the Network Optical Safety—Automatic Laser Shutdown section in the Network Reference chapter of the Configuration guide) is active (ALS Mode = Auto Restart on the OPT-BST, OPT-AMP-C, OPT-AMP-17-C, [+ OSCM] and OSC-CSM). Given this assumption, the starting condition is as shown in Figure 1.

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.

Scenario 1: Span Loss Change > 5 dBm and OSC Power Value on the Receiver less than –42 dBm

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 in Partial state.

In node view (single-shelf mode) or shelf view (multishelf mode), 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, OPT-AMP-C, OPT-AMP-17-C, 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.

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

Procedure

Step 1 Follow these steps to verify the alarms for both DWDM nodes that are connected to the repaired span:

a) Double-click the card directly connected to the span (either the OPT-BST, OPT-AMP-C, OPT-AMP-17-C, or 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.

If the "gray condition" of the span persists, log into Technical Support Website at http://www.cisco.com/c/en/us/support/index.html 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, OPT-AMP-C, or OPT-AMP-17-C + 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 (single-shelf mode) or shelf view (multishelf mode), 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 TransportPlanner 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 that was 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.

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

Note Before disconnecting any optical amplifier card fiber for troubleshooting, ensure that the optical amplifier card is unplugged.

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.

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 17: Network View for Span Loss Change > 5 dBm and OSC Power Value at Receiver > –42 dBm, on page 57.

Figure 17: Network View for Span Loss Change > 5 dBm and OSC Power Value at Receiver > –42 dBm

In node view (single-shelf mode) or shelf view (multishelf mode), 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, OPT-AMP-C, OPT-AMP-17-C, 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 TransportPlanner.

Corrective Action for Scenario 2

Procedure

Step 1 Verify the validity of the alarm.

Step 2 For both DWDM nodes connected to the repaired span:

a) Double-click the card directly connected with the span (either the OPT-BST, OPT-AMP-C, OPT-AMP-17-C, or 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 Step 1.

If the "gray condition" of the span persists, log into Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

Step 3 Measure the new Span Loss value after fixing the fiber.

a) In the node view (single-shelf mode) or shelf view (multishelf mode) of both nodes for 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 4 Compare the span measurements of Step 3 with the span losses values used during the network design with Cisco TransportPlanner.

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.

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

Note Before disconnecting any optical amplifier card fiber for troubleshooting, ensure that the optical amplifier card is unplugged.

Step 8 Follow the signal flow into the network starting from the repaired fiber:

a) In the downstream node, identify the OPT-BST, OPT-AMP-C, OPT-AMP-17-C, 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, OPT-AMP-C, or OPT-AMP-17-C 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 significantly different span loss value is now present, we highly recommended that you complete the following steps:

a) Go back to the Cisco TransportPlanner 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 insertion loss that was measured in Step 3.
d) Run the Cisco TransportPlanner 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) and 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 optic thresholds (see Step 8b) to the lowest value allowed.

If an OPT-BST, OPT-AMP-C, or OPT-AMP-17-C 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 repeat the steps described in Step 11.

Scenario 3: 3 dBm less than Span Loss Change less than 5 dBm

In network view, both of 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 Network Reference chapter of the Configuration 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-CORRECTIO N-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.

Corrective Action for Scenario 3

Procedure

Step 1 Verify the alarm validity.

Step 2 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 3, on page 60. If not, close the CTC application, delete the CTC cache, and open the CTC connection again. Then, go to Step 1, on page 60.

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 3 Measure the new Span Loss value after the fiber has been repaired.

a) In the node view (single-shelf mode) or shelf view (multishelf mode) 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 4, on page 60, the appropriate values must be taken into account.

Step 4 Compare the Span Measurements of the previous step with the Span Losses values used during the network design with Cisco TransportPlanner.

Step 5 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 6, on page 60. If not, go to Step 9, on page 62.

Step 6 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 7. Otherwise, you are finished with the corrective action.

Step 7 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 8 to fix the system faulty condition.

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

Note Before disconnecting any optical amplifier card fiber for troubleshooting, ensure that the optical amplifier card is unplugged.

Step 8 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, on page 60 for how to do this).

b) If the answer is yes, retrieve the following values according to the card type.

- For pre- or booster amplifier cards, click the **Provisioning > Optical Ampli. Line > Gain Setpoint** tabs.
- Go to 8.d, on page 61.

c) If the answer is no, go to 8.d, on page 61.

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 8.b, on page 61.

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 8.a, on page 61:

- 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 8.b, on page 61 or 8.e, on page 61) 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) state 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 and 8.a, on page 61 and 8.i, on page 61back 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 8.a, on page 61) has been provisioned.

Note The total variation of the above parameter setpoint must be within approximately +/– 1 dBm of the Span Loss Change measured in Step 3, on page 60.

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 TransportPlanner 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 Insertion Loss measured in Step 3, on page 60.
- Run the Cisco TransportPlanner 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 9 For the two fibers belonging to the repaired span, identify the fiber for to the east to west (E–W) line direction.

Step 10 Repeat the procedures from Step 6, on page 60 to Step 8, on page 61 for the E–W direction.

Scenario 4: Span Loss Change less than 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 Network Reference chapter of the Configuration 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 Transport Planner 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.

Corrective Action for Scenario 4

Procedure

Step 1 Verify the alarm validity.

Step 2 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 3, on page 63. If not, close the CTC application, delete the CTC cache, and open the CTC connection again. Then, go to Step 1, on page 62.

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 3 Measure the new Span Loss value after the fiber is repaired.

a) In the node view (single-shelf mode) or shelf view (multishelf mode) 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 4, on page 63, the appropriate values must be taken into account.

Step 4 Compare the Span Measurements done in Step 3, on page 63 with the Span Losses values used during the network design with Cisco TransportPlanner.

Step 5 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 6, on page 63.
- If the Span Loss Change is 1 dBm or less, move to Step 9, on page 63.

Step 6 Clean the LINE-RX and LINE-TX connectors of the DWDM cards that manage the fiber of the repaired span.

Step 7 If the problem persists, continue with the next step. If not, you have finished the corrective action.

Step 8 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.

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

Note Before disconnecting any optical amplifier card fiber for troubleshooting, ensure that the optical amplifier card is unplugged.

Note If this is not possible 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

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 6, on page 63 to Step 8, on page 63for the E–W direction.

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 (OOS or Locked) state to the final (IS or Unlocked) state.

Prerequisites for Successful OCHNC Circuit Creation

The prerequisite conditions for successfully completed circuit creation are:

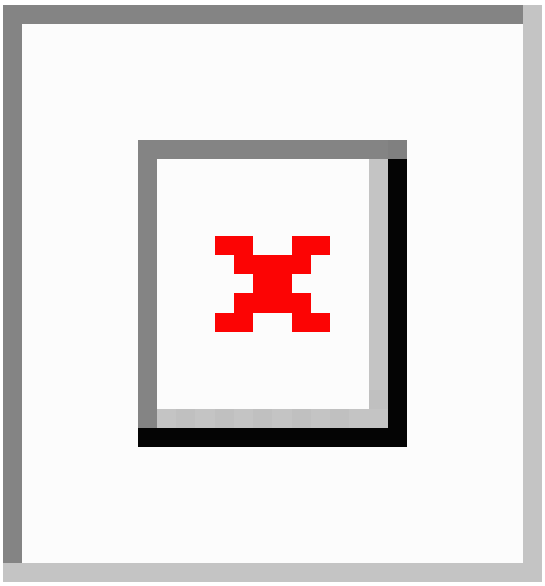
1. Internode: OSC link active among all DWDM nodes involved
2. Internode: APC enabled (or alternatively manually disabled by the user)
3. Intranode: Logical connections among cards created and provisioned on every node of the network (ANS completed)

Note For more information about these operations, refer to the NTP-G183 Diagnose and Fix OCHNC and OCH Trail Circuits section in Configuration guide.

OCHNC circuit creation is successfully completed when the CTC circuit table reports the situation shown in Figure 18: OCHNC Circuit Successfully Completed, on page 64.

- The 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 (or unlocked).

Figure 18: OCHNC Circuit Successfully Completed



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 19: Partial Circuits, on page 65. In the message, click Details to see the partial connections

that WPP can set up. Start troubleshooting the problem in the first node that is unreachable along the path.

Figure 19: Partial Circuits

- 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 20: Circuit Discovered, State OSS, on page 65 .

Figure 20: 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 a. or b (OSC link fail or APC disabled), described below.

The root cause identification for the preceding conditions are found in the prerequisite conditions described in Prerequisites for Successful OCHNC Circuit Creation, on page 64.

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 of Prerequisites for Successful OCHNC Circuit Creation, on page 64 has not been met.
   a. 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 1 of Prerequisites for Successful OCHNC Circuit Creation, on page 64 has not been met.
   b. One (or more) of the intranode connections between two DWDM cards associated with the circuit have not been properly created. Prerequisite condition of 2 Prerequisites for Successful OCHNC Circuit Creation, on page 64 has not been met.
   c. One (or more) of the intranode connections between two DWDM cards associated with the circuit have 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 Prerequisites for Successful OCHNC Circuit Creation, on page 64 has not been met.

To troubleshoot and eventually fix issues related to the faulty OCHNC circuit creation shown in Figure 19: Partial Circuits, on page 65, the following procedure must be performed.

Corrective Action

Procedure

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 System Restart after a Fiber Cut, on page 54).

  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 Corrective Action, on page 65.

Step 2 Verify APC status:

a) Go to node view (single-shelf mode) or shelf view (multishelf mode) 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, complete the appropriate troubleshooting procedure from Alarm Troubleshooting, on page 85.

  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 (single-shelf mode) or multishelf view (multishelf mode) on the MSTP node that is the source node for the circuit.

b) Click the **Provisioning** > **WDM-ANS** > **Connections** tabs.

Step 4 Verify that 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 Turn Up a Node in the Configuration guide.

Step 5 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.

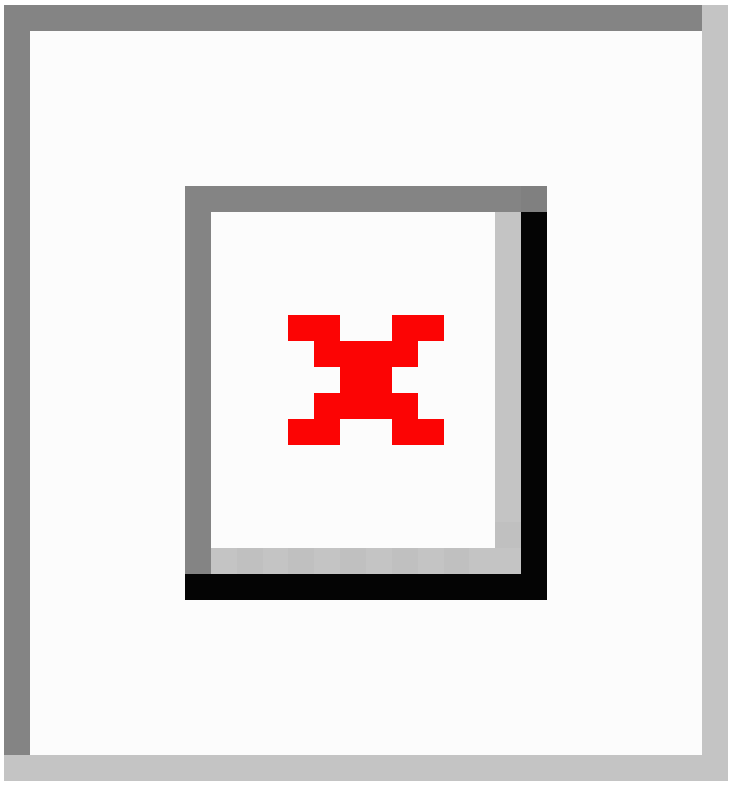
Node Level (Intranode) Problems

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.

VOA Startup Phases

The final VOA condition is achieved through a startup procedure divided into the four sequential phases shown in Figure 21: VOA Startup Procedure, on page 67.

Figure 21: VOA Startup Procedure



Until the VOA has completed all the phases shown in Figure 21: VOA Startup Procedure, on page 67, the power control mode is not fully activated.

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 TransportPlanner 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 Reference chapter of the Configuration guide.)

If the interface that is connected has a power value outside the allowed range, the Phase 1 check prevents OCHNC turn-up.

Phase 2: 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 TransportPlanner on a case-by-case basis. During the ANS run, the power target is provisioned on the VOA.

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.

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.

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.

Scenario A: Optical Power Level of the Incoming Signal Lower Than Minimum Allowed by MSTP Supported Optical Interfaces

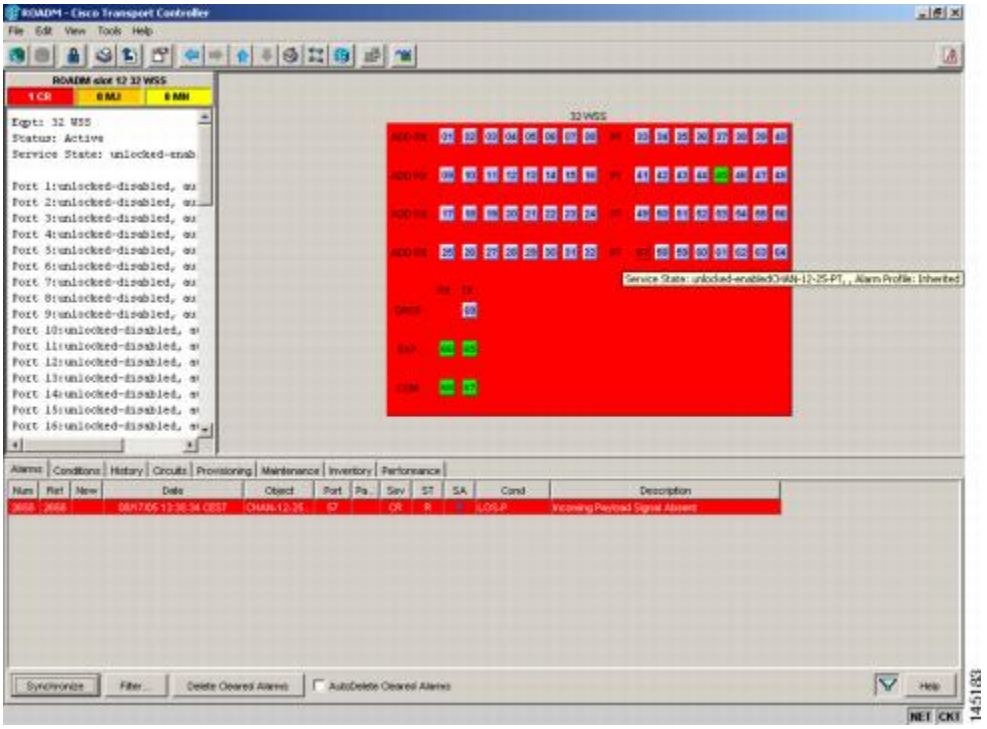
This scenario is for a condition where a TXP or MXP card is directly connected to a 32MUX-O, 40MUX, 32WSS, or 40WSS-C card where power in is expressed as Pin < –4.5 dBm.

If the incoming power level is lower than the minimum allowed, the startup procedure always stops at Phase 1 (see Figure 22: LOS-P Indication on the VOA Port, on page 69). 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 22: LOS-P Indication on the VOA Port, on page 69)
- A valid optical power value (different from the end of scale value of – 50 dBm) 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 22: 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.

Corrective Action for Scenario A

Procedure

Step 1 Verify the alarm validity:

a) Identify the DWDM nodes where the alarmed card is seated.
b) Double-click the 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 If the alarmed card is a 32WSS or 40WSS-C, verify the incoming power level from the connected TXP, MXP, or line card. If the alarmed card is a 32MUX-O or 40MUX, go to Step 5.

a) Double-click the WSS card.

b) Click the **Provisioning > Optical Chn: Optical Connector** *X* **> Parameters** tabs to display the optical power physically coming into the WSS ADD-RX port.

Note *X* is the number (1 to 45) of the appropriate multifiber 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 Upgrade, Add, and Remove Cards and Nodes chapter of the Configuration 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.

Warning **High-performance devices on this card can get hot during operation. To remove the card, hold it by the faceplate and bottom edge. Allow the card to cool before touching any other part of it or before placing it in an antistatic bag.** Statement 201

Step 3 Because the actual power received by the WSS card is lower than expected, verify the correct behavior of the TXP, MXP, or line card connected to the WSS:

- The TX laser must be active (trunk port is in IS [or Unlocked] state).
- The wavelength provisioned must be the proper one.
- The output power value must be within the expected range (refer to the Configuration guide). If the trunk port PM is not available through CTC, perform a manual measurement using a standard power meter.

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 Upgrade, Add, and Remove Cards and Nodes chapter of the Configuration guide. Replacing the card should correct the problem.)

Warning **High-performance devices on this card can get hot during operation. To remove the card, hold it by the faceplate and bottom edge. Allow the card to cool before touching any other part of it or before placing it in an antistatic bag.** Statement 201

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 WSS 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 Configuration 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 Configuration 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 or 40MUX, 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 or 40MUX:

- The TX laser must be active (trunk port is in IS [or Unlocked] state).
- The wavelength provisioned must be the proper one.
- The output power value must be within the expected range (refer to the Configuration guide). If the trunk port PM is not available through CTC, perform a manual measurement using a standard power meter.

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 Upgrade, Add, and Remove Cards and Nodes chapter of the Configuration 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 or 40MUX 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 Configuration 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 Configuration 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 or 40MUX card:

a) Double-click the 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 > Parameters** tabs and identify the proper channel (wavelength).
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 or 40MUX card (refer to the Upgrade, Add, and Remove Cards and Nodes chapter of the Configuration 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).

Warning **High-performance devices on this card can get hot during operation. To remove the card, hold it by the faceplate and bottom edge. Allow the card to cool before touching any other part of it or before placing it in an antistatic bag.** Statement 201

Scenario B: Optical Power Level of the Incoming Signal Lower Than Expected

In some cases, the pass-through channels on the WSS card or the optical bypass channels on the 32MUX-O or 40MUX 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 . 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.

Condition B1—Delta Power > 6 dB (LOS-P Alarm)

When the optical power is more 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 optical power value (different from the end of scale value of – 50 dBm) can be read in the Power field, but the value for Power is less than –33 dBm. (To access this value, in card view, click the **Provisioning > Parameters** tabs.)

Condition B2—Delta Power less than 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 optical power value (different from the end of scale value of –50 dBm) can be read in the Power field, but the value is (VOA Power Ref – 6 dBm) < Power < VOA Power Ref. To access this value, in card view, click the **Provisioning > Parameters** tabs.

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 WSS or the optical bypass channels on the 32MUX-O or 40MUX card, use the following procedures 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. These procedures are given in the following sections.

Condition B1 - LOS-P Alarm

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, 40MUX, or WSS 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, on page 74. 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/cisco/web/support/index.html for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

Step 2

Step 3 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 45) 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 Reference manual. 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, on page 74 and Step 4, on page 74 are operating properly, go to Step 6, on page 74. If not, take the appropriate corrective actions according to the alarm raised on the card.

Step 6 If the alarmed card is a 32MUX-O or 40MUX, go to Step 9, on page 75.

Step 7 If the alarmed card is a 32WSS or 40MUX, 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 45) 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, on page 75. 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 or 4-WSS-C card:

a) The EXP_RX port of the alarmed 32WSS card must be connected to the EXP_TX port of the coupled WSS card on the opposite side of the node.
b) Pull out the LC connector from the EXP_RX port of the WSS card and clean the fiber according to site practice.
c) Pull out the LC connector from the EXP_TX port of the coupled WSS card 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 Before disconnecting any optical amplifier card fiber for troubleshooting, ensure that the optical amplifier card is unplugged.

Note If no site practice exists for cleaning fibers, complete the procedure in the Maintain the Node chapter of the Configuration Guide.

f) If the alarm condition persists even after the checking and fixing the fibers, replace the 32WSS card (refer to the Upgrade, Add, and Remove Cards and Nodes chapter of the Configuration 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).

Warning **High-performance devices on this card can get hot during operation. To remove the card, hold it by the faceplate and bottom edge. Allow the card to cool before touching any other part of it or before placing it in an antistatic bag.** Statement 201

Step 9 Verify the correct behavior of the VOA inside the 32MUX-O or 40MUX card:

a) Double-click the 32MUX-O or 40MUX 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 > Parameters** tabs and identify the proper 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 8, on page 75. 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 or 40MUX card:

a) The ADD_RX port of the alarmed 32MUX-O or 40MUX must be connected to the DROP_TX port of the coupled 32DMX-O or 40DMX 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 Configuration Guide).

b) Verify that the power value coming out of DROP_TX port of the coupled 32DMX-O or 40DMX card is correct:

- In card view, click the **Provisioning > Optical Chn: > Parameters** tabs.
- 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 Alarm Troubleshooting, on page 85

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 10.e, on page 76 for the MPO-LC multifiber cable coming out of the DROP_TX port of the coupled 32DMX-O or 40DMX 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 Configuration Guide.

Warning **High-performance devices on this card can get hot during operation. To remove the card, hold it by the faceplate and bottom edge. Allow the card to cool before touching any other part of it or before placing it in an antistatic bag.** Statement 201

g) If the alarm condition persists even after the cabling is checked or fixed, replace the 32MUX-O or 40MUX card (refer to the Upgrade, Add, and Remove Cards and Nodes chapter of the Configuration 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).

Condition B2 - OPWR-LowDEGrade Alarm

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, 32WSS, 40MUX, or 40WSS-C 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, go 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

Step 3 a) In card view, click the **Provisioning** > **Optical Chn: Optical Connector** *X* > **Parameters** tabs.

Note *X* is number (1 to 45) of the proper multi-fibers MPO connector that manages the alarmed channel (wavelength).

b) The Power field value must be the same as the VOA Power Ref field. If it is not, take the appropriate corrective action for the alarm according to Alarm Troubleshooting, on page 85

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 Configuration 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 Alarm Troubleshooting, on page 85).

Step 6 If the alarmed card is a 32MUX-O or 40MUX card, go to Step 8.

Step 7 If the alarmed card is a 32WSS or 40WSS-C card, verify the proper cabling of the EXP_RX port (common input port for all pass-through channels) on the WSS card:

a) Verify that the EXP_RX port of the alarmed WSS card is connected to the EXP_TX port of the coupled WSS card on the opposite side of the node.
b) Pull out the LC connector from the EXP_RX port of the WSS card and clean the fiber according to site practice.
c) Pull out the LC connector from the EXP_TX port of the coupled WSS 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 Before disconnecting any optical amplifier card fiber for troubleshooting, ensure that the optical amplifier card is unplugged.

Note If no site practice exists for cleaning fibers, complete the procedure in the Maintain the Node chapter of the Configuration 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 or 40MUX card:

a) Verify that the ADD_RX port of the alarmed 32MUX-O or 40MUX is connected to the DROP_TX port of the coupled 32DMX-O or 40DMX 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 Configuration 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> Parameters** tabs.
   - 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 Alarm Troubleshooting, on page 85

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 Condition B2 - OPWR-LowDEGrade Alarm, on page 76 for the MPO-LC multifiber cable coming out of the DROP_TX port of the coupled 32DMX-O or 40DMX 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 Configuration 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.

Scenario C: Optical Drop Power Level Lower Than Expected

This scenario describes the condition in which the optical power at the 32DMX-O or 40DMX 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 Scenario B: Optical Power Level of the Incoming Signal Lower Than Expected, on page 72. The only difference is the type of alarm that is raised when the condition exists in which Delta Power is greater than 6 dB.

Condition C1—Delta Power > 6 dB Lower than Expected

When the optical power on the dropped channel is more 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.
- A valid optical power value (different from the end of scale value of –50 dBm) 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.)

Condition C2—Delta Power less than 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 Condition B2 (see the Condition B2—Delta Power less than 6 dB (OPWR-LowDEGrade Alarm), on page 73):

- An OPWR-LowDEGrade (OCH layer) alarm is present on the port associated with the VOA.
- A valid optical power value (different from the end of scale value of –50 dBm) can be read in the CTC Power field, but the value is (VOA Power Ref – 6 dBm) < Power < VOA Power Ref. 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.

Corrective Action for Scenario C (Optical Power Level of Incoming Signal Lower than Expected)

Scenario C1 - LOS-P Alarm

Procedure

Step 1 Verify the alarm validity:

a) Identify the DWDM nodes where the alarmed card is located.
b) Double-click the 32DMX-O or 40DMX 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 Scenario C1 - LOS-P Alarm, on page 79. 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/cisco/web/support/index.html for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

Step 2

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 45) 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 Alarm Troubleshooting, on page 85

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 Configuration 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 Scenario C1 - LOS-P Alarm, on page 79 is correct, go to Scenario C1 - LOS-P Alarm, on page 79. If not, take the appropriate corrective actions according to Alarm Troubleshooting, on page 85

Step 3 Verify the correct behavior of the VOA inside the 32DMX-O or 40DMX card:

a) Double-click the 32DMX-O or 40DMX 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 > Parameters** tabs and identify the proper 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 Scenario C1 - LOS-P Alarm, on page 79. 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 or 40DMX card:

a) Verify that the COM_RX port of the alarmed 32DMX-O or 40DMX is connected either to the DROP_TX port of a 32WSS or 40WSS-C card or to the COM_TX port of an OPT-PRE, OPT-BST/OPT-AMP-C/OPT-AMP-17-C, 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 or 40DMX 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.

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

Note Before disconnecting any optical amplifier card fiber for troubleshooting, ensure that the optical amplifier card is unplugged.

Note If no site practice exists for cleaning fibers, complete the procedure in the Maintain the Node chapter of the Configuration guide.

f) If the alarm condition persists even after the cabling has been checked and fixed, replace the 32DMX-O card (refer to the Upgrade, Add, and Remove Cards and Nodes chapter of the Configuration 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).

Warning **High-performance devices on this card can get hot during operation. To remove the card, hold it by the faceplate and bottom edge. Allow the card to cool before touching any other part of it or before placing it in an antistatic bag.** Statement 201

Scenario C2 - OPWR-LowDEGrade Alarm

Procedure

Step 1 Verify the alarm validity:

a) Identify the DWDM nodes where the alarmed card is seated.
b) Double-click the 32DMX-O or 40DMX 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 Scenario C2 - OPWR-LowDEGrade Alarm, on page 81. 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/cisco/web/support/index.html for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

Step 2

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 45) 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 Alarm Troubleshooting, on page 85

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 Configuration guide). If the trunk port PM is not available through CTC, perform a manual measurement using a standard power meter.

e) If everything in Scenario C2 - OPWR-LowDEGrade Alarm, on page 81 is correct, move to Scenario C2 - OPWR-LowDEGrade Alarm, on page 81. If not, take the appropriate corrective actions according to Alarm Troubleshooting, on page 85.

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 or 40DMX:

a) Verify that the COM_RX port of the alarmed 32DMX-O or 40DMX is connected either to the DROP_TX port of a 32WSS or 40WSS-C card or to the COM_TX port of an OPT-PRE, OPT-BST/OPT-AMP-C/OPT-AMP-17-C, or OSC-CSM, depending on the actual node layout.

b) Pull out the LC connector from the COM_RX port of the 32DMX-O or 40DMX 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.

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

Note Before disconnecting any optical amplifier card fiber for troubleshooting, ensure that the optical amplifier card is unplugged.

Note If no site practice exists for cleaning fibers, complete the procedure in the Maintain the Node chapter in the Configuration 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.

Counter-Propagating Light Affecting Operation of 32DMX-C and 32DMX-L Cards

Problem The in-service operation of the 32DMX-C and 32DMX-L cards (with vendor ID 2049 and 2050) can be seriously affected by the counter-propagating light travelling from the drop ports of the card towards the COM RX port. This counter-propagating light affects the internal VOA control loop of the vendor-specific optical module of the 32DMX-C and 32DMX-L cards, leading to an increased optical path attenuation. This is traffic affecting for all in-service channels.

Possible Cause The counter-propagating light can be inserted into the 32DMX-C or 32DMX-L card as a result of incorrect cabling of transponder or line cards to the fiber patch-panel (in particular, swapping RX with TX patchcords).

Solution For software releases higher than or equal to 9.0, the vendor-specific optical module on all the cards is automatically upgraded to a newer version. The vendor ID of the new version of the card is 2051 and can be viewed at **CTC > Card View > Inventory** tab. This new version of the optical module makes the VOA

control robust to counter-propagating light, thus, minimizing the effects of incorrect cabling during installation and/or maintenance.

Solution For software releases lower than 9.0, for new 32DMX-C and 32DMX-L cards that are not already installed, the vendor-specific optical module on all these new cards is automatically upgraded to a newer version at the Cisco Spare depots. Once the new card is installed in field, a downgrade of the optical module will be prevented and the latest optical module version is preserved on the software package. If the 32DMX-C or 32DMX-L card is already installed, complete the Corrective Action for Software Releases Lower than 9.0, on page 83 to manually fix the problem.

Corrective Action for Software Releases Lower than 9.0

Procedure

Step 1 If the TXP card is preprovisioned in CTC, but not installed:

a) Log into CTC.
b) Display card view for the TXP card.
c) Click the **Provisioning > Line** tab and choose **OOS,DSBLD** (ANSI) or **Locked,disabled** (ETSI) from the Admin State drop-down list for the Trunk-TX port.
d) Continue with Step 2.

Step 2 Install the TXP card into the receptacle at the back of the designated slot.

Step 3 Wait for the TXP card to boot completely.

Step 4 Verify that the Trunk-TX port of the TXP card is in OOS,DSBLD (ANSI) or Locked,disabled (ETSI) state.

Step 5 Wire the Trunk-TX/RX port of the TXP card to the fiber patch-panel.

Step 6 Turn up the TXP card and display card view for the TXP card in CTC.

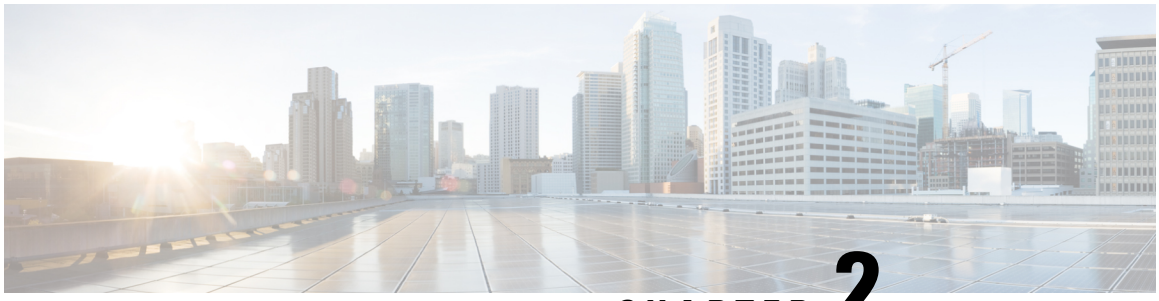
Step 7 Click the **Provisioning > Line** tab and choose **IS,AINS** (ANSI) or **Unlocked,automaticInService** (ETSI) from the Admin State drop-down list for the Trunk-TX port.

Step 8 Display card view for the 32WSS card.

Step 9 Click the **Performance > Optical Chn** tab and verify the Power ADD field on the CHAN-RX port of the 32WSS card connected to the TXP card.

a) If a valid power level exists, the cabling of the TXP card is correct. Change the admin state of the Trunk-TX port of the TXP card back to the original state.
b) If no power level exists, the cabling of the TXP card is incorrect. Change the admin state of the Trunk-TX port of the TXP card to OOS,DSBLD (ANSI) or Locked,disabled (ETSI) state and reverse the cabling.

Note It is important that you perform Steps Step 7, on page 83 to Step 9, on page 83 in the shortest time possible. That is, you must check the presence of a valid RX power on WSS card (Step 9, on page 83) immediately after you turn up the TXP Trunk-TX port (Step 7, on page 83), and in case of a bad connection, you must shut off the TXP Trunk-TX port (Step 9) as soon as possible. This is to minimize possible impairments on other channels that are already in service.



CHAPTER 2

Alarm Troubleshooting

This chapter gives a description, severity, and troubleshooting procedure for each commonly encountered Cisco DWDM alarm and condition. Table 11: Alarm Logical Object Type Definitions, on page 96 gives definitions of all DWDM alarm logical objects. For a comprehensive list of all conditions and instructions for using TL1 commands, refer to the TL1 Command Guide. An alarm troubleshooting procedure applies to both the Cisco Transport Controller (CTC) and TL1 version of that alarm.

Alarms can occur even in those cards that are not explicitly mentioned in the Alarm sections. When an alarm is raised, refer to its clearing procedure.

For more information about alarm profiles, see the Manage Alarms chapter in the *Cisco ONS 15454 DWDM Procedure Guide*see the Alarm and TCA Monitoring and Management document.

Alarm Indexes

The following tables group alarms and conditions by their default severities. These severities are the same whether they are reported in the CTC Alarms window severity (SEV) column or in SNMP 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 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.

Logical Objects

The CTC alarm profile list organizes all alarms and conditions according to the logical objects they are raised against. These logical objects represent physical objects such as cards, logical objects such as circuits, or transport and signal monitoring entities such as the SONET or ITU-T G.709 optical overhead bits. One alarm can appear in multiple entries. It can be raised against multiple objects. For example, the loss of signal (LOS) alarm can be raised against the optical signal (OC-N) or the optical transport layer overhead (OTN) as well as other objects. Therefore, both OCN: LOS and OTN: LOS appear in the list (as well as the other objects).

Alarm profile list objects are defined in Table 11: Alarm Logical Object Type Definitions, on page 96.

Note Alarm logical object names can appear as abbreviated versions of standard terms used in the system and the documentation. For example, the OCN logical object refers to the OC-N signal. Logical object names or industry-standard terms are used within the entries as appropriate.

Alarm Logical Objects

The table below lists all logical alarm objects used in this chapter.

Table 11: Alarm Logical Object Type Definitions

Logical Object	Definition
2R	Reshape and retransmit (used for transponder [TXP] cards).
AICI-AEP	Alarm Interface ControllerInternational/alarm expansion panel. A combination term that refers to this platform 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).
ESCON	Enterprise System Connection fiber optic technology, referring to the following TXP cards: TXP_MR_2.5G, TXPP_MR_2.5G, MXP_MR_2.5G, MXPP_MR_2.5G, AR-XP, AR-MXP, AR-XPE.

Logical Object	Definition
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, MXP_MR_10DME_C, MXP_MR_10DME_L, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, TXP_MR_10E_C, TXP_MR_10E_L, GE_XP, 10GE_XP, ADM-10G, and OTU2_XP, 40G-MXP-C, 40E-MXP, 10x10G-LC, WSE, 400G-XP-LC.
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_10G, TXP_MR_10E,TXP_MR_10E_C, TXP_MR_10E_L, MXP_MR_10DME_C, MXP_MR_10DME_L, GE-XP, 10GE-XP, ADM-10G, and OTU2_XP, 40G-MXP, 40E-MXP, 40G-TXP-C, 40G-TXP-E, 40E-TAR-XP, AR-MXP, AR-XPE, 10x10G, WSE, 100G-LC-C, 100G-CK-C, CFP-LC, MR-MXP, 100GS-CK-LC-C, 200G-CK-C, 400G-XP-LC.
ISC	Inter-service channel, referring to TXPP_MR_2.5G or TXP_MR_2.5G cards.
NE	The entire network element.
NE-SREF	The timing status of the NE.
OCH	The optical channel, referring to dense wavelength division multiplexing (DWDM) cards.
OCH-TERM	The optical channel termination node, referring to DWDM cards.
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 SFP), referring to MXP and TXP cards.
PWR	Power equipment.
SHELF	The shelf assembly.
TRUNK	The card carrying the high-speed signal; referring to MXP or TXP cards.

Trouble Characterizations

The NCS DWDM 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 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.

Note For a description of CTC-view terminology, refer to the Cisco Transport Controller Operation chapter in the *Cisco ONS 15454 DWDM Reference Manual*CTC Enhancements, Operations, and Shortcuts.

Alarm Characteristics

The DWDM system 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.)

Condition Characteristics

Conditions include any problem detected on a 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 TL1 Command Guide. For information about transients, see Transient Conditions, on page 403.

Note When an entity is put in the OOS,MT administrative state, the NCS suppresses all standing alarms on that entity. You can retrieve alarms and events on the Conditions tab. You can change this behavior for the LPBKFACILITY and LPBKTERMINAL alarms. To display these alarms on the Alarms tab, set the NODE.general.ReportLoopbackConditionsOnPortsInOOS-MT to TRUE on the NE Defaults tab.

Severity

The system uses Telcordia-devised standard severities for alarms and conditions: Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA), and Not Reported (NR). These are described below:

- A Critical (CR) alarm generally indicates severe, Service-Affecting trouble that needs immediate correction.
- A Major (MJ) alarm is a serious alarm, but the trouble has less impact on the network.
- 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. Procedures for customizing alarm severities are located in the Manage Alarms chapter in the *Cisco ONS 15454 DWDM Procedure Guide*Alarm and TCA Monitoring and Management document.

Service Effect

Service-Affecting (SA) alarmsthose that interrupt servicecould 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.

State

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/shelf view, etc. Transient events do not require user action. These are listed in the chapter, Transient Conditions, on page 403.

Safety Summary

This section covers safety considerations designed to ensure safe operation of the NCS 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 cards; in these instances users should pay close attention to the following warnings.

Warning **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

Trouble-Clearing 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.

Note When checking alarms, ensure that alarm suppression is not enabled on the card or port.

Note When an entity is put in the OOS,MT administrative state, the system suppresses all standing alarms on that entity. All alarms and events appear on the Conditions tab. You can change this behavior for the LPBKFACILITY and LPBKTERMINAL alarms. To display these alarms on the Alarms tab, set the NODE.general.ReportLoopbackConditionsOnPortsInOOS-MT to TRUE on the NE Defaults tab.

ACT-SOFT-VERIF-FAIL

On the Active Controller card, the Alarm severity is Critical (CR) and Service Affecting (SA).

On the Standby Controller card, the Alarm severity is Minor (MN) and Non-Service affecting (NSA).

Logical Object: EQPT

The Active Volume Software Signature Verification Failed (ACT-SOFT-VERIF-FAIL) alarm occurs under the following conditions:

- The working software running on the control card in the NCS system is tampered with or the working software running on the system did not originate from Cisco.
- Problem present in the software stored in the protect or standby card.

Clear the ACT-SOFT-VERIF-FAIL Alarm

Procedure

Step 1 To clear the ACT-SOFT-VERIF-FAIL alarm, download the software on the protect (standby) flash.

Step 2 Activate the protect (standby) flash.

Step 3 After the control card is activated, download the software on the standby partition or the standby code volume on the protect flash.

If the troubleshooting procedure does not clear the alarm, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html or call the Cisco Technical Assistance Center (1 800 553-2447) to report the problem.

AIS

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

Logical Objects: BITS, FUDC, MSUDC

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 resolve the problem on the upstream node.

Clear the AIS Condition

Procedure

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 (or Locked,disabled) ports.

Step 2 Clear the upstream alarms using the applicable procedures in this chapter.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

AIS-L

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA),

logical Objects: OCN, TRUNK

The AIS Line condition indicates that this node is detecting line-level AIS in the incoming signal. This alarm is secondary to another alarm occurring simultaneously in an upstream node.

This condition can also be raised in conjunction with the TIM-S alarm if AIS-L is enabled.

Clear the AIS-L Condition

Procedure

Complete the Clear the AIS Condition, on page 102 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

AIS-P

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

Logical Object: STSMON, STSTRM

The AIS Path condition means that this node is detecting AIS in the incoming path. This alarm is secondary to another alarm occurring simultaneously in an upstream node.

Clear the AIS-P Condition

Procedure

Complete the Clear the AIS Condition, on page 102 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

ALS

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Objects: 2R, AOTS, ESCON, FC, GE, ISC, OCN, TRUNK

The Automatic Laser Shutdown (ALS) condition on the amplifier cards indicate that the ALS safety feature on the card port is switched ON. This condition is accompanied by a corresponding LOS alarm in the reverse direction of the same port.

Note ALS is an informational condition and does not require troubleshooting.

ALS-DISABLED

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: EQPT

The Automatic Laser Shutdown (ALS) condition occurs when Amplifier card ALS is changed to Disabled from any other state (such as Enabled) by user command.

Clear the ALS-DISABLED Condition

Procedure

Step 1 In node view (single-shelf mode) or shelf view (multishelf mode), double-click the OPT-BST, or OPT-PRE, OPT-AMP-C, or OMP-AMP-17-C card to display the card view.

Step 2 Click the **Maintenance** > **ALS** tabs.

Step 3 In the ALS Mode column, change the entry from Disabled to your required state.

AMPLI-INIT

Default Severity:Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: AOTS

The Amplifier Initialized condition occurs when an amplifier card is not able to calculate gain. This condition typically accompanies the APC-DISABLED , on page 104 alarm.

Clear the AMPLI-INIT Condition

Procedure

Step 1 Complete the Delete a Circuit, on page 395 procedure on the most recently created circuit.

Step 2 Recreate this circuit using the procedures in the Configuration guide.

APC-CORR-SKIPPED

Default Severity: Minor (MN), 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 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-CORR-SKIPPED condition is raised.

The APC Correction Skipped alarm strongly limits network management (for example, a new circuit cannot be turned into IS). The Force APC Correction button helps to restore normal conditions by clearing the APC Correction Skipped alarm.

APC-DISABLED

Default Severity:Minor (MN), Non-Service-Affecting (NSA)

Logical Objects: NE, SHELF, AOTS, OTS, OMS, OCH, EQPT

The APC Disabled alarm occurs when the information related to the number of channels is not reliable. The condition can occur when any of the following related alarms also occur: the EQPT alarm, the IMPROPRMVL alarm, or the MEA (EQPT)alarm. If the condition occurs with the creation of the first circuit, delete and recreate the circuit.

APC Disabled alarm is raised under the following conditions:

- When APC is manually disabled in a domain to prevent unexpected power regulations during maintenance or troubleshooting.
- When an abnormal event impacting optical regulation occurs.
- When an EQPT, MEA or IMPROPRMVL alarm is raised by any unit in a network.
- When gain or power degrade occurs or when the Power Fail alarm is raised by the output port of any amplifier in the network.
- When a VOA degrade or a VOA Fail alarm is raised by any unit in a network.
- When signalling protocol detects that one of the APC instances in a network is no longer reachable.
- When all nodes in a network do not belong to metro core.

Note The MEA and IMPROPRMVL alarms does not disable APC when raised on MXP/TXP cards.

Clear the APC-DISABLED Alarm

Procedure

Step 1 Complete the appropriate procedure to clear the main alarm:

- Clear the EQPT Alarm
- Clear the IMPROPRMVL Alarm
- Clear the MEA (EQPT) Alarm

Step 2 If the condition does not clear, .

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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. APC-END is an informational condition that is raised and cleared spontaneously by the system. It is visible only by retrieving it in the Conditions or History tabs.

Note APC-END is an informational condition and does not require troubleshooting.

APC-OUT-OF-RANGE

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Objects: AOTS, OCH, OMS, OTS

The APC-OUT-OF-RANGE condition is raised on amplifier cards 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 maximum setpoint) or to set the attenuation on the express VOA lower than 0 dBm (its minimum setpoint).

Note A common cause of an amplifier trying to attain a value higher than the maximum setpoint or an attenuator trying to attain a value lower than the minimum setpoint is the low input power.

Clear the APC-OUT-OF-RANGE Alarm

Procedure

There are various root causes for the APC-OUT-OF-RANGE condition. To determine the correct root cause, complete the network-level troubleshooting procedures and node level problems.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

APC-WRONG-GAIN

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: AOTS

The APC-WRONG-GAIN condition is raised on the amplifier card, when the actual gain of the card (17dB) does not match the expected gain calculated by APC. There is a margin of +1 or -1 dB before the condition is raised.

Note The APC-WRONG-GAIN condition indicates a system issue and not the card problem.

Clear the APC-WRONG-GAIN Alarm

The condition can be cleared by recovering the power at the input port:

Procedure

Step 1 Check the incoming fiber connection and clean them.

Step 2 Check the regulation points (VOA and amplifiers) along the optical path upstream of the card.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

APSB

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: OCN, STMN

The APS Channel Byte Failure alarm occurs when LTE detects protection switching byte failure or an invalid switching code in the incoming APS signal. Some older SONET not manufactured by Cisco send invalid APS codes if they are configured in a 1+1 protection group with newer SONET nodes.

Clear the APSB Alarm

Procedure

Step 1 Use an optical test set to examine the incoming SONET overhead to confirm inconsistent or invalid K bytes. For specific procedures to use the test set equipment, consult the manufacturer. If corrupted K bytes are confirmed and the upstream equipment is functioning properly, the upstream equipment might not interoperate effectively with the NCS.

Step 2 If the alarm does not clear and the overhead shows inconsistent or invalid K bytes, you could need to replace the upstream cards for protection switching to operate properly. Complete the Physically Replace a Card, on page 394 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

APSCM

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: OCN, STMN

The APS Channel Mismatch alarm occurs when the NCS expects a working channel but receives a protect channel. In many cases, the working and protect channels are crossed and the protect channel is active. If the fibers are crossed and the working line is active, the alarm does not occur. The APSCM alarm occurs only on the NCS when bidirectional protection is used on OC-N cards in a 1+1 protection group configuration. The APSCM alarm does not occur in an optimized 1+1 protection configuration.

Warning **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

Clear the APSCM Alarm

Before you begin

Caution Always use the supplied electrostatic discharge wristband when working with a powered system. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Procedure

Step 1 Verify that the working-card channel fibers are physically connected directly to the adjoining node working-card channel fibers.

Step 2 If the fibers are correctly connected, verify that the protection-card channel fibers are physically connected directly to the adjoining node protection-card channel fibers.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

APSIMP

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: OCN, STMN

The APS Invalid Code alarm occurs if a 1+1 protection group is not properly configured at both nodes to send or receive the correct APS byte. A node that is either configured for no protection or is configured for path protection or BLSR protection does not send the right K2 APS byte anticipated by a system configured for 1+1 protection. The 1+1 protect port monitors the incoming K2 APS byte and raises this alarm if it does not receive the byte.

The alarm is superseded by an APSCM or APSMM alarm, but not by an AIS condition. It clears when the port receives a valid code for 10 ms.

Clear the APSIMP Alarm

Procedure

Step 1 Check the configuration of the other node in the 1+1 protection group. If the far end is not configured for 1+1 protection, create the group.

Step 2 If the other end of the group is properly configured or the alarm does not clear after you have provisioned the group correctly, verify that the working ports and protect ports are cabled correctly.

Step 3 Ensure that both protect ports are configured for SONET.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

APSMM

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: STMN

An APS Mode Mismatch failure alarm occurs on OC-N cards when there is a mismatch of the protection switching schemes at the two ends of the span, such as being bidirectional at one end and unidirectional at the other. Each end of a span must be provisioned the same way: bidirectional and bidirectional, or unidirectional and unidirectional. APSMM can also occur if third-party equipment is provisioned as 1:N and the NCS is provisioned as 1+1.

If one end is provisioned for 1+1 protection switching and the other is provisioned for path protection protection switching, an APSMM alarm occurs in the NCS that is provisioned for 1+1 protection switching.

Clear the APSMM Alarm

Procedure

Step 1 For the reporting NCS, display node view and verify the protection scheme provisioning:

a) Click the **Provisioning** > **Protection** tabs.

b) Click the 1+1 protection group configured for the OC-N cards.

The chosen protection group is the protection group optically connected (with data communications channel, or DCC, connectivity) to the far end.

c) Click **Edit**.

d) Record whether the Bidirectional Switching check box is checked.

Step 2 Click **OK** in the Edit Protection Group dialog box.

Step 3 Log into the far-end node and verify that the OC-N 1+1 protection group is provisioned.

Step 4 Verify that the Bidirectional Switching check box matches the checked or unchecked condition of the box recorded in Step 1, on page 110. If not, change it to match.

Step 5 Click **Apply.**

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

APS-NO-RESPONSE

Default Severity: Minor (MN), Service Affecting (SA)

Logical Object: ODU

The APS-NO-RESPONSE alarm is raised when the requested or bridge signals of a SNC protection do not match.

Clear the APS-NO-RESPONSE Alarm

Procedure

Verify that the requested and bridge signals of SNC protection match.

If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

APS-PROV-MISM

Default Severity: Minor (MN), Non-Service Affecting (NSA)

Logical Object: ODU

The APS-PROV-MISM alarm is raised when the SNC protection types on the near end and far end near are incompatible.

Clear the APS-PROV-MISM Alarm

Procedure

Verify that the near end and far end SNC protection types match.

If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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, SHELF, 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 Procedure Guide*.

Note For more information about suppressing alarms, refer to the Alarm and TCA Monitoring and Management document.

Note This condition is not raised for multiservice transport platform (MSTP) cards such as amplifiers, multiplexers, or demultiplexers.

Clear the AS-CMD Condition

Procedure

Step 1 For all nodes, in node view (single-shelf mode) or shelf view (multishelf mode),,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, on page 112.
- If the condition is reported against the backplane, go to Step 7, on page 112.
- If the condition is reported against the NE object, go to Step 8, on page 112.

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 (single-shelf mode) or shelf view (multishelf mode), 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 that are not in the optical or electrical slots. To clear the alarm, complete the following steps:

a) 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 (single-shelf mode) or shelf view (multishelf mode), 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.**

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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, SHELF, 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.

While provisioning traffic between two MXP-MR-10DME, MXP-MR-2.5G, or MXPP-MR-2.5G cards, putting the trunk port (09) of the card OOS-MT (initially IS) results in the AS-MT alarm being reported on both trunk and client port. This is because all the GFP interfaces derive their state from the trunk state if the trunk is not IS-NR. If the Trunk port state is IS-NR, then all the GFP interfaces derive their state from the corresponding client port. When the trunk is moved to AS-MT, which is not IS, the GFP of the client port also moves to the AS-MT state. The FAC of the client does not change state.

Clear the AS-MT Condition

Procedure

Complete the Clear an MXP, TXP, GE-XP, 10GE-XP, and ADM-10G Card Loopback Circuit, on page 396 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

AU-AIS

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

Logical Object: VCMON-HP, VCTRM-HP

An AU AIS condition applies to the administration unit, which consists of the virtual container (VC) capacity and pointer bytes (H1, H2, and H3) in the SDH frame.

Generally, any AIS is a special SDH 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 AU-AIS Condition

Procedure

Step 1 Complete the Clear the AIS Condition, on page 102 procedure.

Step 2 If the condition does not clear, complete the Clear the APSB Alarm, on page 107 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

AU-LOP

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Objects: VCMON-HP, VCTRM-HP

An AU-LOP alarm indicates that the SDH high order path overhead section of the administration unit has detected a loss of path. AU-LOP occurs when there is a mismatch between the expected and provisioned circuit size. For the TXP card, an AU-LOP is raised if a port is configured for an SDH signal but receives a SDH signal instead. (This information is contained in the H1 byte bits 5 and 6.)

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

Clear the AU-LOP Alarm

Procedure

Step 1 In node view, click the **Circuits** tab and view the alarmed circuit.

Step 2 Verify that the correct circuit size is listed in the Size column. If the size is different from what is expected, such as a VC4-4c instead of a VC4, this causes the alarm.

Step 3 If you have been monitoring the circuit with optical test equipment, a mismatch between the provisioned circuit size and the size expected by the test set can cause this alarm. Ensure that the test set monitoring is set up for the same size as the circuit provisioning. For specific procedures to use the test set equipment, consult the manufacturer.

Step 4 If you have not been using a test set, or if the test set is correctly set up, the error is in the provisioned CTC circuit size. Complete the Delete a Circuit, on page 395 procedure.

Step 5 Recreate the circuit for the correct size.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

AUTH-EC

Default Severity: Major (MJ), Non-Service-Affecting (NSA)

Logical Objects: OTU

The Authentication Error Count (AUTH-EC) alarm is raised when the authentication error count crosses the authentication threshold.

Clear the AUTH-EC Alarm

Procedure

This alarm is cleared automatically when the authentication error count becomes less then authentication error threshold.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

AUTO-SENSE

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: PPM

The AUTO-SENSE alarm is raised when the port detects an incoming signal on the port. The alarm clears automatically after detecting the signal.

AUTO-SENSE-DSBLD

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: PPM

The AUTO-SENSE-DSBLD alarm is raised when the port is configured as an AUTO port, but auto-sensing is disabled.

Clear the AUTO-SENSE-DSBLD Alarm

Procedure

Clear the AUTO-SENSE-DSBLD alarm with either of these procedures:

a) Enable auto-sensing.

1. Login to CTC.
2. In node view (single-shelf mode) or shelf view (multishelf view), double-click the AR_MXP or AR_XP card where you want to enable auto-sensing.
3. Click the **Provisioning** > **Line** > **Auto Ports** tabs.
4. Check the **Auto Sensing** check box.

b) Delete the auto port.

1. Login to CTC.
2. In node view (single-shelf mode) or shelf view (multishelf view), double-click the AR_MXP or AR_XP card where you want to delete the auto port.
3. Click the **Provisioning** > **Pluggable Port Modules** tabs.
4. In the Pluggable Port Modules area, select the auto PPM that you want to delete and click **Delete**.
5. Click **Yes**. The auto port is deleted.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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).

Resets performed during a software upgrade also prompt the condition. This condition clears automatically when the card finishes resetting. If the alarm does not clear, complete the following procedure.

Clear the AUTORESET Alarm

Procedure

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, on page 394 procedure.

Warning **High-performance devices on this card can get hot during operation. To remove the card, hold it by the faceplate and bottom edge. Allow the card to cool before touching any other part of it or before placing it in an antistatic bag.** Statement 201

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

AUTOSW-AIS

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

Logical Object: STSMON, VT-MON

The Automatic Path Protection Switch Caused by an AIS condition indicates that automatic path protection switching occurred because of an AIS condition. If the path protection is configured for revertive switching, it reverts to the working path after the fault clears. The AIS also clears when the upstream trouble is cleared.

Note This condition is only reported if the path protection is set up for revertive switching.

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 AUTOSW-AIS Condition

Procedure

Complete the Clear the AIS Condition, on page 102 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

AUTOSW-AIS-SNCP

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

Logical Object: VCMON-HP, VCMON-LP

The Automatic UPSR Switch Caused by an AIS condition indicates that automatic UPSR protection switching occurred because of the TU-AIS condition. If the UPSR ring is configured for revertive switching, it switches back to the working path after the fault clears. The AUTOSW-AIS-UPSR clears when you clear the primary alarm on the upstream node.

Note This condition is only reported if the SNCP is set up for revertive switching.

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 AUTOSW-AIS-UPSR Condition

Procedure

Complete the Clear the AIS Condition, on page 102 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

AUTOSW-LOP (STSMON)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: STSMON

The Automatic Path Protection Switch Caused by LOP condition for the STS monitor (STSMON) indicates that automatic path protection switching occurred because of the LOP-P , on page 237 alarm. If the path protection is configured for revertive switching, it reverts to the working path after the fault clears.

Note This condition is only reported if the path protection is set up for revertive switching.

Clear the AUTOSW-LOP (STSMON) Condition

Procedure

Complete the Clear the LOP-P Alarm, on page 238 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

AUTOSW-LOP-SNCP

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: VCMON-HP, VCMON-LP

An Automatic UPSR Switch Caused by LOP alarm indicates that an automatic UPSR protection switching occurred because of the AU-LOP , on page 114. If the UPSR ring is configured for revertive switching, it switches back to the working path after the fault clears.

Note This condition is only reported if the SNCP is set up for revertive switching.

Clear the AUTOSW-LOP-SNCP Alarm

Procedure

Complete the Clear the AU-LOP Alarm , on page 114 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

AUTOSW-PDI

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: STSMON, VT-MON

The Automatic Path Protection Switch Caused by Payload Defect Indication (PDI) condition indicates that automatic path protection switching occurred because of a PDI-P , on page 311 alarm. If the path protection is configured for revertive switching, it reverts to the working path after the fault clears.

Note This condition is only reported if the path protection is set up for revertive switching.

Clear the AUTOSW-PDI Condition

Procedure

Complete the Clear the PDI-P Condition, on page 312 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

AUTOSW-PDI-SNCP

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: VCMON-HP, VCMON-LP

The Automatic UPSR Switch Caused by Payload Defect Indication (PDI) condition indicates that automatic UPSR protection switching occurred because of a PDI alarm. If the UPSR is configured for revertive switching, it reverts to the working path after the fault clears.

Note This condition is only reported if the SNCP is set up for revertive switching.

Clear the AUTOSW-PDI-SNCP Condition

Procedure

Complete the Clear the PDI-P Condition, on page 312 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

AUTOSW-SDBER

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: STSMON, VT-MON

The Automatic Path Protection Switch Caused by Signal Degrade Bit Error Rate (SDBER) condition indicates that a SD-P , on page 340 condition caused automatic path protection switching to occur. If the path protection is configured for revertive switching, the path protection reverts to the working path when the SD-P is resolved.

Note This condition is only reported if the path protection is set up for revertive switching.

Clear the AUTOSW-SDBER Condition

Procedure

Complete the Clear the SD-P Condition, on page 340 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

AUTOSW-SDBER-SNCP

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: VCMON-HP, VCMON-LP

The Automatic UPSR Switch Caused by Signal Degrade Bit Error Rate (SDBER) condition indicates that a signal degrade caused automatic UPSR protection switching to occur. If the UPSR ring is configured for revertive switching, it reverts to the working path when the SD is resolved.

Note This condition is only reported if the SNCP is set up for revertive switching.

Clear the AUTOSW-SDBER-SNCP Condition

Procedure

Complete the Clear the SD (TRUNK) Condition, on page 338 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

AUTOSW-SFBER

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: STSMON, VT-MON

The Automatic USPR Switch Caused by Signal Fail Bit Error Rate (SFBER) condition indicates that a SF-P , on page 344 condition caused automatic path protection switching to occur. If the path protection is configured for revertive switching, the path protection reverts to the working path when the SF-P is resolved.

Note This condition is only reported if the path protection is set up for revertive switching.

Clear the AUTOSW-SFBER Condition

Procedure

Complete the Clear the SF-P Condition, on page 344 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

AUTOSW-SFBER-SNCP

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: VCMON-HP, VCMON-LP

The Automatic UPSR Switch Caused by Signal Fail Bit Error Rate (SFBER) condition indicates that a signal fail caused automatic UPSR protection switching to occur. If the UPSR ring is configured for revertive switching, it reverts to the working path when the SF is resolved.

Note This condition is only reported if the SNCP is set up for revertive switching.

Clear the AUTOSW-SFBER-SNCP Condition

Procedure

Complete the Clear the SF (TRUNK) Condition, on page 342 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

AUTOSW-UNEQ (STSMON)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: STSMON

The Automatic Path Protection Switch Caused by Unequipped condition indicates that an UNEQ-P , on page 370, caused automatic path protection switching to occur. If the path protection is configured for revertive switching, it reverts to the working path after the fault clears.

Note This condition is only reported if the path protection is set up for revertive switching.

Clear the AUTOSW-UNEQ (STSMON) Condition

Procedure

Complete the Clear the UNEQ-P Alarm, on page 371 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

AUTOSW-UNEQ-SNCP (VCMON-HP)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: VCMON-HP

The Automatic UPSR Switch Caused by an Unequipped condition indicates that an HP-UNEQ alarm caused automatic UPSR protection switching to occur (see the HP-UNEQ , on page 203). If the UPSR ring is configured for revertive switching, it reverts to the working path after the fault clears.

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

Warning **Class 1M laser radiation when open. Do not view directly with optical instruments.** Statement 1053

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 This condition is only reported if the SNCP is set up for revertive switching.

Clear the AUTOSW-UNEQ-SNCP (VCMON-HP) Condition

Procedure

Complete the Clear the HP-UNEQ Alarm, on page 203 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

AWG-DEG

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: OTS

The Arrayed Waveguide Gratings (AWG) Degrade alarm occurs when a card heater-control circuit degrades. The heat variance can cause slight wavelength drift.

Clear the AWG-DEG Alarm

Procedure

For the alarmed card, complete the Physically Replace a Card, on page 394 procedure during the next maintenance period.

Warning **High-performance devices on this card can get hot during operation. To remove the card, hold it by the faceplate and bottom edge. Allow the card to cool before touching any other part of it or before placing it in an antistatic bag.** Statement 201

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

AWG-FAIL

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: OTS

The AWG Failure alarm occurs when a card heater-control circuit completely fails. The circuit failure disables wavelength transmission. The card must be replaced to restore traffic.

Clear the AWG-FAIL Alarm

Procedure

For the alarmed card, complete the Physically Replace a Card, on page 394 procedure during the next maintenance period.

Warning **High-performance devices on this card can get hot during operation. To remove the card, hold it by the faceplate and bottom edge. Allow the card to cool before touching any other part of it or before placing it in an antistatic bag.** Statement 201

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

AWG-OVERTEMP

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: OTS

The AWG Over Temperature alarm is raised if a 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.

Clear the AWG-OVERTEMP Alarm

Procedure

Complete the Clear the AWG-FAIL Alarm, on page 125 procedure.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

AWG-WARM-UP

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: OTS

The AWG Warm-Up condition occurs when a 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.

BAD-DB-DETECTED

Default Severity: Critical (CR)

Logical Object: NE

The Bad Database Detected alarm is raised when the database load fails due to the following:

- Soft-reset of Active Controller
- Software Upgrade
- Database Restore

A pop-up error message might appear while navigating to card view and shelf view.

Note Do not use the reboot command in the console when the BAD-DB-DETECTED alarm is raised.

Clear the BAD-DB-DETECTED Alarm

Procedure

Restore any known good database.

(or)

Reset NE to the factory default settings.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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.

Note FAN-FAIL alarm is not raised if BAT-FAIL alarm appears on the power module.

Clear the BAT-FAIL Alarm

Procedure

Step 1 At the site, determine which battery is not present or operational.

Step 2 Remove the power cable from the faulty supply. Reverse the power cable installation procedure.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

BP-LPBKFACILITY

Default Severity: Not alarmed (NA)

Logical Object: EQPT

The BP-LPBKFACILITY alarm is raised when the backplane facility loopback is configured on the 100G-LC-C or 10x10G-LC card.

Clear the BP-LPBKFACILTIY Alarm

Remove the backplane facility loopback on the 100G-LC-C or 10x10G-LC card.

Procedure

Step 1 Log in to a node on the network.

Step 2 In node view (single-shelf mode) or shelf view (multishelf mode), double-click the 100G-LC-C or 10x10G-LC card in CTC to open the card view.

Step 3 Click the **Maintenance** > **Card** tabs.

Step 4 Click on the card port that is in IS (or Unlocked) state in the Admin State column, and change the state to OOS,MT.

Step 5 Click **Apply**.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

BP-LPBKTERMINAL

Default Severity: Not alarmed (NA)

Logical Object: EQPT

The BP-LPBKTERMINAL alarm is raised when the backplane terminal loopback is configured on the 100G-LC-C or 10x10G-LC card.

Clear the BP-LPBKTERMINAL Alarm

Remove the backplane terminal loopback on the 100G-LC-C or 10x10G-LC card.

Procedure

Step 1 Log in to a node on the network.

Step 2 In node view (single-shelf mode) or shelf view (multishelf mode), double-click the 100G-LC-C or 10x10G-LC card in CTC to open the card view.

Step 3 Click the **Maintenance** > **Card** tabs.

Step 4 Click on the card port that is in IS (or Unlocked) state in the Admin State column, and change the state to OOS,MT.

Step 5 Click **Apply**.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

CARLOSS (EQPT)

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: EQPT

A Carrier Loss on the LAN Equipment alarm generally occurs on MXP, TXP cards when the system and the workstation hosting do not have a TCP/IP connection. The problem involves the LAN or data circuit used by the RJ-45 (LAN) connector on the control card 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 or the node.

On MXP_2.5G_10G cards, CARLOSS is also raised against trunk ports when ITU-T G.709 encapsulation is turned off.

Note The multishelf management (MSM) port is turning Yellow even when Carloss alarm is not present on external connection unit (ECU) of M6 Chassis, this is a known behaviour.

The CARLOSS alarm is also raised against multishelf management (MSM) ports of the external connection unit (ECU) when the connection to the shelf subtending the node is improper.

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 CARLOSS alarms are not reported on M15-ECU for ONS-SI-100-LX10 and ONS-SE-100-LX1 pluggables under the following conditions.

- When the pluggables are plugged-in for the first time and there is no fiber connection on their ports.
- When the controller switch-over happens or when the cable connects or disconnects.

Clear the CARLOSS (EQPT) Alarm

Procedure

Step 1 If the reporting card is an MXP or TXP card in an NCS node, verify the data rate configured on the PPM (also called SFP):

a) In node view (single-shelf mode) or shelf view (multishelf mode), 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) and their specifications, refer to the Installing the GBIC, SFP, SFP+, and XFP Optical Modules in Cisco ONS Platforms document.

Step 2 If the reporting card is an OC-N/STM-N card, verify connectivity by pinging the system that is reporting the alarm.

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.

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.

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.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

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 MXP_MR_2.5G, MXPP_MR_2.5G, MXP_MR_10DME_C, MXP_MR_10DME_L, 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.

Clear the CARLOSS (FC) Alarm

Procedure

Complete the Clear the CARLOSS (GE) Alarm, on page 132 procedure.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

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 MXP_MR_2.5G, MXPP_MR_2.5G, MXP_MR_10DME_C, MXP_MR_10DME_L, GE-XP, 10GE-XP, or ADM-10G cards supporting 1-Gbps or 10-Gbps traffic. The loss can be due to a misconfiguration, fiber cut, or client equipment problem.

Clear the CARLOSS (GE) Alarm

Procedure

Step 1 Ensure that the GE client is correctly configured:

a) Click the **Provisioning** > **Pluggable Port Modules** tabs.

b) 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. PPM (SFP) specifications are listed in the Installing the GBIC, SFP, SFP+, and XFP Optical Modules in Cisco ONS Platforms document.

c) 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 and provisioning PPMs (SFPs), refer to the Installing the GBIC, SFP, SFP+, and XFP Optical Modules in Cisco ONS Platforms document.

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 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.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

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 MXP_MR_2.5G, or MXPP_MR_2.5G card supporting ISC traffic.
- MSM ports of an NCS NC shelf.
- MSM ports of an NCS SS shelf.

The loss can be due to a misconfiguration, fiber cut, or client equipment problem.

Clear the CARLOSS (ISC) Alarm

Procedure

Perform the following to clear the CARLOSS (ISC) alarm:

- For TXP/MXP cards—Complete the Clear the CARLOSS (GE) Alarm, on page 132 procedure.
- For MS-ISC cards—Suppress the alarm.
  - Check the **Suppress Alarms** check box and click **Apply** in the **Provisioning > Alarm Profiles > Alarm Behavior** tab in the card view of CTC.
- For NCS NC shelf or NCS SS shelf—Suppress the alarm.
  - Check the **Suppress Alarms** check box and click **Apply** in the **Provisioning > Alarm Profiles > ECU MS Ports Alarm Suppression** tab in the shelf view of CTC.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

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 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.

Clear the CARLOSS (TRUNK) Alarm

Procedure

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.

Step 2 If there is no cause upstream, verify cabling continuity from the transmitting port of the DWDM card ( ) 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 Procedure Guide*Manage the Node document.

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.

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, on page 394 procedure for the reporting card.

Warning **High-performance devices on this card can get hot during operation. To remove the card, hold it by the faceplate and bottom edge. Allow the card to cool before touching any other part of it or before placing it in an antistatic bag.** Statement 201

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

CASETEMP-DEG

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: AOTS

Note For specific temperature and environmental information about each DWDM card, refer to the Hardware Specifications appendix in the *Cisco ONS 15454 DWDM Reference Manual*Hardware Specifications document.

Clear the CASETEMP-DEG Alarm

Procedure

Step 1 Determine whether the air filter needs replacement. Complete the Inspect, Clean, and Replace the Air Filter, on page 397 procedure.

Step 2 If the filter is clean, complete the Remove and Reinsert a Fan-Tray Assembly, on page 398 procedure.

Step 3 If the fan does not run or the alarm persists, complete the Replace the Fan-Tray Assembly, on page 399 procedure. The fan should run immediately when correctly inserted.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

CD

Default Severity: Critical (CR) , Service-Affecting (SA)

Logical Object: Trunk port (dir RX)

The Chromatic Dispersion value alarm is raised when the device experiences CD in excess.

Clear the CD Alarm

Procedure

Switch the traffic on a lower CD link.

If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of toll-free Technical Support numbers for your country in order to report a Service-Affecting (SA) problem.

CFM-CONFIG-ERROR

Default Severity: MInor (MN), Non-Service-Affecting (NSA)

Logical Objects: ETH

The Connectivity Fault Management Configuration Error (CFM-CONFIG-ERROR) alarm is raised on GE_XP or 10GE_XP cards under the following scenarios:

- A mismatch is present in the continuity check (CC) timer between two maintenance end points.
- A mismatch exists between the maintenance association and domain name.
- A similar maintenance point (MP) ID exists on both the maintenance end points.

Clear the CFM-CONFIG-ERROR Condition

Procedure

Step 1 In node view, double-click the GE_XP or 10GE_XP card to open the card view.

Step 2 Verify if the CC Timer settings on both the maintenance end points of the card are the same. To set or view the CC timer values do the following:

a) In card view, click the Provisioning > CFM > Configuration > Global Settings tabs.
b) Select or note down the CC Timer value.
c) Repeat step a and b on the other end of the maintenance end point.
d) Set the CC Timer value that is same as the value set at the other maintenance end point.

Step 3 Verify the maintenance association and the domain name are the same. Do the following:

a) In card view, click the **Provisioning** > **CFM** > **Configuration** > **MA Profiles** tabs.
b) Enter or note down the maintenance profile name.
c) In card view, click the **Provisioning** > **CFM** > **Configuration** > **Domain Profiles** tabs.
d) Enter or note down the domain profile name.
e) Repeat step a and d on the other end of the maintenance end point.
f) The maintenance profile name and the domain profile name should be the same on both the maintenance end points.

Step 4 Verify the maintenance point (MP) ID on both the sides are the same. Do the following:

a) In card view, click the **Provisioning** > **CFM** > **Configuration** > **MEP** tabs.
b) Note down the MPID value.
c) MPID should not be the same.
d) Repeat step a and d on the other end of the maintenance end point.
e) The MPID values must not be the same on both the maintenance end points.

CFM-LOOP

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Objects: ETH

The Connectivity Fault Management Loop (CFM-LOOP) alarm occurs on GE_XP or 10GE_XP cards when a continuity check (CC) packet is reused in a loop and consequently the same packet is returned to the source.

Clear the CFM-LOOP Condition

Procedure

Ensure that there are no loops in the L2-over-DWDM mode for VLANs in the network.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

CFM-MEP-DOWN

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Objects: ETH

The Connectivity Fault Management Maintenance End-Point Down (CFM-MEP-DOWN) alarm occurs in GE_XP, 10GE_XP, GE_XPE or 10GE_XPE cards when two maintenance end points cannot communicate with each other.

Clear the CFM-MEP-DOWN Condition

Procedure

Step 1 Make sure that there are no fiber cuts or other CFM alarms present.

Step 2 In card view, click the **Provisioning** > **CFM** > **CCDB** > **Counters** tabs.

Step 3 Ensure that the counter values in the CCM Received field is equivalent to the counter values in the CCM Transmitted field and that the counter is incrementing appropriately.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

CFM-XCON-SERVICE

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Objects: ETH

The Connectivity Fault Management Cross-Connect Service (CFM-XCON-SERVICE) occurs in GE_XP, 10GE_XP, GE_XPE and 10GE_XPE cards when the domain are configured incorrectly, and a packet meant for a one domain goes to the other.

Clear the CFM-XCON-SERVICE Condition

Procedure

Step 1 In card view, click the **Provisioning** > **CFM** > **Configuration** > **MEP** tabs.

Step 2 Do the following to ensure that the maintenance association and the domain names are the same.

a) In card view, click the **Provisioning** > **CFM** > **Configuration** > **MA Profiles** tabs.

b) Enter or note down the maintenance profile name.

c) In card view, click the **Provisioning** > **CFM** > **Configuration** > **Domain Profiles** tabs.

d) Enter or note down the domain profile name.

e) Repeat steps a to d on the other end of the maintenance end point.

The maintenance profile name and the domain profile name must be the same on both the maintenance end points.

Step 3 Verify that the MA-Domain Mapping is correct. Click **Provisioning** > **CFM** > **Configuration** > **MA-Domain Mapping**

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

CHANLOSS

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: OCN

The SONET Section Layer DCC Termination Failure condition occurs when the NCS receives unrecognized data in the section layer DCC bytes.

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

Clear the CHANLOSS Condition

Procedure

Step 1 In the absence of other alarms, determine whether the alarmed port is connected to another vendor equipment. If so, you can mask the alarm on this path using a custom alarm profile. For more information about custom profiles, refer to the Manage Alarms chapter.

Step 2 If alternate vendor equipment is not the cause of the alarm, complete the Reset a Card in CTC, on page 391 procedure for the traffic card.

Caution Always use the supplied electrostatic discharge wristband when working with a powered NCS. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 3 If the alarm does not clear, complete the Physically Replace a Card, on page 394 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

CHAN-PWR-THRESHOLD-CHECK

Default Severity: Minor (MN), Non-Service Affecting (NSA)

Logical Objects: OTS

The Channel Power Threshold Check (CHAN-PWR-THRESHOLD-CHECK) alarm is raised againstd OPT-EDFA cards. This alarm is raised when deleting or restoring a channel results in channel power drop below the fail thresholds. The alarm is raised even if the power of one channel drops below the fail threshold. The check for channel power is run every hour.

Clear the CHAN-PWR-THRESHOLD-CHECK Alarm

Procedure

CHAN-PWR-THRESHOLD-CHECK alarm is cleared in one of the these scenarios:

a) The alarm clears automatically when the periodic check determines that the total channel power does not cross failure thresholds. This scenario occurs when channels are deleted or restored. This increases the total channel power.
b) The alarm must be cleared manually by changing the failure threshold limits.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

CLDRESTART

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: EQPT

The Cold Restart condition occurs when a card is physically removed and inserted, replaced, or when the NCS power is initialized.

Clear the CLDRESTART Condition

Procedure

Step 1 Remove and reinsert (reseat) the standby control card.

Step 2 If the condition fails to clear after the card reboots, complete the Remove and Reinsert (Reseat) Any Card , on page 393 procedure.

Step 3 If the condition does not clear, complete the Physically Replace a Card, on page 394 procedure for the card.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

COMP-CARD-MISSING

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: EQPT

When the 100G-LC-C and CFP-LC cards work in a combination, the COMP-CARD-MISSING alarm is raised under any of the following conditions:

- When the 100G-LC-C or CFP-LC card is removed from the slot.
- When the 100G-LC-C or CFP-LC card is reset.
- When any one of these alarms is raised on the 100G-LC-C or CFP-LC card:
  - AUTORESET , on page 116
  - MANRESET , on page 263
  - CLDRESTART , on page 139
  - PROV-MISMATCH, on page 321

Clear the COMP-Card-Missing Alarm

Procedure

Step 1 Add the missing 100G-LC-C or CFP-LC card. If the card is reset, wait for it to boot up. To add a card, see the "Turn Up a Node" chapter.

Step 2 Complete the appropriate procedure to clear the following alarms:

- Clear the AUTORESET Alarm, on page 117
- Clear the CLDRESTART Condition, on page 139

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

COMM-FAIL

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: EQPT

The Plug-In Module (card) Communication Failure indicates that there is a communication failure between the control card and the traffic card. The failure could indicate a broken card interface.

Clear the COMM-FAIL Alarm

Procedure

Step 1 Complete the Remove and Reinsert (Reseat) Any Card , on page 393 procedure for the reporting card.

Step 2 If the alarm does not clear, complete the Physically Replace a Card, on page 394 procedure for the card.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

COOL-MISM

Default Severity: Not Reported (NR), Service-Affecting (SA)

Logical Object: FAN

The Cool Mismatch (COOL-MISM) condition is raised when an incorrect cooling profile is chosen for the NCS shelf. To determine the cooling profile values for the cards, see the "Cooling Profile" section in the "Installing the NCS Shelf" chapter of the *Hardware Installation Guide*.

Clear the COOL-MISM Alarm

Set the correct cooling profile for the NCS shelf depending on the cards used.

Procedure

Step 1 Log in to a node on the network.

Step 2 Navigate to **Shelf view** > **Provisioning** > **General** > **Voltage/Temperature** tabs.

Step 3 From the Cooling Profile drop-down list, choose the correct cooling profile value for the shelf.

Step 4 Click **Apply**.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

CP-UNVER-CLEARED Alarm

Default Severity: Minor (MN)

Logical Object: NE

The CP-UNVER-CLEARED alarm is raised under the following conditions:

- When there is a failure in the original path and it is not fixed.
- After all the circuits are moved to the restored path, the port on the original path moves to OOS,DSBLD (ANSI) or Locked,disabled (ETSI) state. These alarms disappear on the original path and unverified alarms appear in **Maintenance** > **DWDM** > **WSON** tabs.

The CP-UNVER-CLEARED alarm is automatically cleared after acknowledging the unverified alarms in the WSON tab.

CTNEQPT-MISMATCH

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: EQPT

The Connection Equipment Mismatch condition is raised when there is a mismatch between the cross-connect card preprovisioned in the slot and the card actually present in the shelf. For example, an XC-VXL card could be preprovisioned in Slot 10, but another card could be physically installed.

Note Cisco does not support configurations of unmatched cross-connect cards in Slot 8 and Slot 10, although this situation could briefly occur during the upgrade process.

Note The cross-connect card you are replacing should not be the active card. (It can be in SBY state or otherwise not in use.)

Note During an upgrade, this condition occurs and is raised as its default severity, Not Alarmed (NA). However, after the upgrade has occurred, if you wish to change the condition severity so that it is Not Reported (NR), you can do this by modifying the alarm profile used at the node. For more information about modifying alarm severities, refer to the Manage Alarms chapter.

Clear the CTNEQPT-MISMATCH Condition

Procedure

Step 1 Determine what kind of card is preprovisioned in the slot by completing the following steps:

a) In node view, click the **Inventory** tab.
b) View the slot row contents in the Eqpt Type and Actual Eqpt Type columns.

The Eqpt Type column contains the equipment that is provisioned in the slot. The Actual Eqpt Type contains the equipment that is physically present in the slot.

Step 2 Complete the Physically Replace a Card, on page 394 procedure for the mismatched card.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

DATA-CRC

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: OCH, MSISC

A data cyclic redundancy check (CRC) bad packet count condition occurs when excessive CRC errors are received on the trunk ports of the GE-XP, GE-XPE, 10GE-XP, and 10GE-XPE cards.

The CRC error rate is measured and compared against a configured threshold. The system can be configured to perform an automatic FAPS switch when the DATA-CRC alarm occurs.

Clear the DATA-CRC Alarm

Procedure

For GE-XP, GE-XPE, 10GE-XP, and 10GE-XPE cards, perform the following:

a) Ensure that the fiber connector for the card is completely plugged in.
b) 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.
c) If the optical power level is good, verify that optical receive levels are within the acceptable range.
d) If the receive levels are good, clean the fibers at both the ends according to site practise. If no site practice exists, complete the procedure in the Maintain the Node chapter.
e) Clear the CRC alarm in CTC.
f) Wait for a time equivalent to (polling period * soak count).

DBOSYNC

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: NE

The Standby Database Out Of Synchronization alarm occurs when the standby controller card database does not synchronize with the active database on the active controller card.

Caution If you reset the active controller card while this alarm is raised, you lose current provisioning.

Clear the DBOSYNC Alarm

Procedure

Step 1 Save a backup copy of the active controller card database.

Step 2 Make a minor provisioning change to the active database to see if applying a provisioning change clears the alarm:

a) In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **General** > **General** tabs.

b) In the Description field, make a small change such as adding a period to the existing entry.

The change causes a database write but does not affect the node state. The write could take up to a minute.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

DCU-LOSS-FAIL

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: OTS

The DCU-LOSS-FAIL condition occurs when the DCU loss monitored value exceeds the maximum acceptable DCU loss of the board .

Clear the DCU-LOSS-FAIL Condition

Procedure

Step 1 Verify that the optical fibers connecting the board (OPT-PRE, OPT-PRE-L, 40-SMR1-C, or 40-SMR2-C) and the DCU unit are clean, correctly plugged in, and not damaged.

Step 2 If the condition does not clear, verify that appropriate DCU unit, according to the installation requirements, is connected to the board and is correctly working.

Step 3 If the condition still does not clear, verify that the optical power signal is present on the DCU-TX port.

Step 4 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/cisco/web/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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

Procedure

Restart the CTC application.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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.

If the alarm is raised for an extended period, the MXP or TXP card raises the DUP-IPADDR , on page 146 condition and could affect traffic.

Note DSP-COMM-FAIL is an informational alarm and does not require troubleshooting.

DSP-FAIL

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: TRUNK

The DSP Failure alarm indicates that a DSP-COMM-FAIL , on page 145, has persisted for an extended period on an MXP or TXP card. It indicates that the card is faulty.

Clear the DSP-FAIL Alarm

Procedure

Complete the Physically Replace a Card, on page 394 procedure for the reporting MXP or TXP card.

Warning **High-performance devices on this card can get hot during operation. To remove the card, hold it by the faceplate and bottom edge. Allow the card to cool before touching any other part of it or before placing it in an antistatic bag.** Statement 201

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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, no longer reliably connects to either node. Depending on how the packets are routed, could connect to either node (having the same IP address). If 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

Procedure

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 control card.
b) Begin a CTC session.
c) In the login dialog box, uncheck the **Network Discovery** check box.

Step 2 In node view (single-shelf mode) or multishelf view (multishelf mode), 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 Procedure Guide*Connect the PC and Log into the GUI document.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

DUP-NC

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: Shelf

(In R10.0) The DUP-NC (Duplicate Node Controller) alarm is raised in multishelf environment on both the node controllers, when two node controllers are connected to the same switch.

(In R10.1), The DUP-NC alarm is raised in multishelf environment on the NCS 2006 duplicate node controller, when two node controllers are connected to the same switch.

Clear the DUP-NC Alarm

Procedure

Step 1 (In R10.0) Pull the LAN cables out from both the node controllers connected to the switch.

Step 2 (In R10.1)

a. Disconnect the duplicate node controller's cable from switch. The DUP-NC alarm clears.

b. Perform soft reset of the control card to recover the MSM ASIC interface.

Step 3 (In R10.6.2)

a. Disconnect the duplicate node controller's cable from switch.

b. Perform soft reset of the active control card on both the node controllers. The DUP-NC alarm clears.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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

Procedure

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **General** > **General** tabs.

Step 2 In the Node Name field, enter a unique name for the node.

Step 3 Click **Apply.**

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

DUP-SHELF-ID

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: SHELF

The Duplicated Shelf Identifier alarm applies to a shelf that has multishelf management enabled when the control card detects that you have programmed an ID already in use by another shelf.

Clear the DUP-SHELF-ID Alarm

Procedure

Unprovision the shelf ID of the duplicate shelf by completing the following steps:

a) In shelf view (multishelf mode) or multishelf view (multishelf mode), click the node controller **Provisioning** > **General** > **Multishelf Config** tabs.

b) Enter a new value in the **Shelf ID** field.

c) Click **Apply**

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

EPROM-SUDI-SN-MISMATCH

Default Severity: Major (MJ), Non-Service-Affecting (NSA)

Logical Object: EQPT

The EPROM SUDI Serial Number Mismatch alarm is raised when the card serial number mismatches with certificate serial number.

Clear the EPROM-SUDI-SN-MISMATCH Alarm

Procedure

This alarm is cleared when the card serial number matches with certificate serial number.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

EFM-PEER-MISSING

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Objects: GE

The EFM Peer Missing (EFM-PEER-MISSING) alarm occurs in GE_XP or 10GE_XP cards under the following conditions:

- When an EFM session is established between two ports and EFM is disabled on one of the ports, the alarm is raised on the peer port.
- When an EFM session is established between two ports and one of the ports is moved to OOS-DSBLD state, the alarm is raised on the peer port.

Clear the EFM-PEER-MISSING Condition

Procedure

To clear the EFM PEER MISSING alarm, do the following:

a) In card view, click the Provisioning > EFM > Configuration tabs.
b) From the EFM State drop-down list, choose Enabled.
c) Click Apply to enable EFM for that port.

Peer port is in IS state.

EFM-RFI-CE

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: GE

The EFM Remote Failure Indication Critical Event (EFM-RFI-CE) alarm is raised if the peer interface defines the RFI CE.

Clear the EFM-RFI-CE Alarm

Procedure

Cisco devices do not generate RFI CE events. If a non-Cisco peer device generates an RFI CE event, a Cisco device can raise the EFM-RFI-CE alarm. Check the scenarios under which the non Cisco peer device generates the RFI CE and then clear the condition that lead to the RFI CE.

EFM-RFI-DG

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: GE

The EFM Remote Failure Indication Dying Gasp alarm indicates one of the following:

- The peer interface is administratively shut down.
- The EFM is not configured on the peer interface.
- The peer card is reloading.

Clear the EFM-RFI-DG Alarm

Procedure

To clear the EFM-RFI-DG alarm, check if the peer is administratively disabled. If it is, move the port to IS state.

Note If the peer device is not an GE-XP or 10GE-XP card, consult the peer device manual to find the scenarios under which the EFM-RFI-DG alarm is raised.

EFM-RFI-LF

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: GE

The EFM Remote Failure Indication Link Fault (EFM-RFI-LF) alarm indicates that the peer interface has a carrier loss.

Clear the EFM-RFI-LF Alarm

Procedure

Clear the EHIBATVG and CARLOSS alarms on the peer Ethernet interface.

Note If the peer device is not a GE_XP or 10GE_XP card, consult the user documentation of the peer device to understand scenarios under which the alarm is raised.

EFM-RLBK

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Objects: GE

TThe EFM Remote Loopback (EFM-RLBK) alarm indicates that the EFM port is participating in an EFM remote loopback.

Clear the EFM-RLBK Condition

Procedure

To clear the EFM-LPBK alarm, ensure that the EFM loopback is not configured on the port and the peer port.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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.

Clear the EHIBATVG Alarm

Procedure

The problem is external to the ONS system. Troubleshoot the power source supplying the battery leads.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

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.

Clear the ELWBATVG Alarm

Procedure

The problem is external to the ONS system. Troubleshoot the power source supplying the battery leads.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

ENCAP-MISMATCH-P

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: STSTRM

The Encapsulation C2 Byte Mismatch Path alarm applies to ML-Series Ethernet cards or the CE-1000 card. It occurs when the first three following conditions are met and one of the last two is false:

- The received C2 byte is not 0x00 (unequipped).
- The received C2 byte is not a PDI value.
- The received C2 does not match the expected C2.
- The expected C2 byte is not 0x01 (equipped unspecified).
- The received C2 byte is not 0x01 (equipped unspecified).

For an ENCAP-MISMATCH-P to be raised, there is a mismatch between the received and expected C2 byte, with either the expected byte or received byte value being 0x01.

For example, an ENCAP-MISMATCH-P alarm is raised if a circuit created between two ML-Series or two CE-1000 cards has generic framing procedure (GFP) framing provisioned on one end and HDLC framing with LEX encapsulation provisioned on the other. The GFP framing card transmits and expects a C2 byte of 0x1B, while the HDLC framing card transmits and expects a C2 byte of 0x01.

A mismatch between the transmit and receive cards on any of the following parameters can cause the alarm:

- Mode (HDLC, GFP-F)
- Encapsulation (LEX, HDLC, PPP)
- CRC size (16 or 32)
- Scrambling state (on or off)

This alarm is demoted by a PLM-P condition or a PLM-V condition.

Note By default, an ENCAP-MISMATCH-P alarm causes an ML-Series or CE-1000 card data link to go down. This behavior can be modified using the command line interface (CLI) command in interface configuration mode: **no pos trigger defect encap**.

Clear the ENCAP-MISMATCH-P Alarm

Procedure

Step 1 Ensure that the correct framing mode is in use on the receive card:

a) In node view, double-click the receive ML-Series or CE-1000 card to open the card view.

b) Click the **Provisioning** > **Card** tabs.

c) In the Mode drop-down list, ensure that the same mode (GFP or HDLC) is selected. If it is not, choose it and click **Apply**.

Step 2 Ensure that the correct framing mode is in use on the transmit card, and that it is identical to the receiving card:

a) In node view, double-click the transmit ML-Series or CE-1000 card to open the card view.
b) Click the **Provisioning** > **Card** tabs.
c) In the Mode drop-down list, ensure that the same mode (GFP or HDLC) is selected. If it is not, choose it and click **Apply**.

Step 3 If the alarm does not clear, use the CLI to ensure that the remaining settings are correctly configured on the ML-Series or CE-1000 card:

- Encapsulation
- CRC size
- Scrambling state

To open the interface, click the **IOS** tab and click **Open IOS Command Line Interface (CLI)**.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

ENC-CERT-EXP

Default Severity: Minor (MN), Service-Affecting (SA)

Logical Objects: EQPT

The SUDI 2029 MIC encryption certicate is expired on line cards like 400G-XP-LC, WSE, and MR-MXP.

Clear the ENC-CERT-EXP Alarm

Procedure

The alarm is cleared under the following conditions:

- Change the encryption certificate type to LSC (or)
- Disable the encryption (or)
- Both near-end and far-end line cards must have SUDI 2099 certificates and software package release 11.12 and above.

If the alarm is not cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into

http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

EMBEDDED-AMPLIFIER-SATURATED

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: OTS

The Embedded Amplifer Saturated condition is raised by the embedded EDFA in the AS-16-CCOFS cards. It means the incoming signal on the ADD or COM Rx port is saturating the internal amplifier.

Clear the EMBEDDED-AMPLIFIER-SATURATED Alarm

Procedure

Add an attenuator or decrease the power on the port if the alarm is raised on COM-Tx. Decrease the SMR-20 setpoint if the alarm is raised on COM-Rx.

If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

EOC-E

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Objects: OCN, STMN, FE, GE

The SONET DCC Termination Failure alarm occurs when the system loses its DCC. Although this alarm is primarily SONET, it can apply to DWDM. EOC-E is supported only on TNC/TNC-E with GE or FE OSC ports.

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 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 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-E Alarm

Procedure

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 troubleshooting guide.

Caution Always use the supplied electrostatic discharge wristband when working with a powered NCS 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.

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 to verify that the DCC is provisioned for the ports at both ends of the fiber span.

Step 5 Repeat Step 4 procedure 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, in node view (single-shelf mode) or shelf view (multishelf mode), double-click the card in CTC to open the card view.
c) In card view, 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 (or Locked,disabled), 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 "2.8.2 Protection Switching, Lock Initiation, and Clearing" section 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 Configuration guide for card power levels.

Step 9 If budget loss is within parameters, ensure that fiber connectors are securely fastened and properly terminated.

Step 10 If fiber connectors are properly fastened and terminated, complete the "Reset an Active Control Card and Activate the Standby Card" procedure.

Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card.

Resetting the active control card switches control to the standby control card. If the alarm clears when the system node switches to the standby control card, the user can assume that the previously active card is the cause of the alarm.

Step 11 If the control card 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) In node view (single-shelf mode) or multishelf view (multishelf mode), 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.

Step 13 Verify that both ends of the DCC have been recreated at the optical ports.

If the alarm has not cleared, call Cisco TAC (1 800 553-2447). If the Cisco TAC technician tells you to reseat the card,

If the Cisco TAC technician tells you to reseat the card, complete the "Reset an Active Control Card and Activate the Standby Card" procedure. If the Cisco TAC technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Card" procedure.

Warning **High-performance devices on this card can get hot during operation. To remove the card, hold it by the faceplate and bottom edge. Allow the card to cool before touching any other part of it or before placing it in an antistatic bag. Statement 201**

OSC ports in TNCP and TNCS cards might have the EOC-E alarm. Follow this procedure to clear the EOC-E alarm.

a. If you want to connect SFP ports with far end OTDR ports, use 1518 nm OSC SFP. For example, use the ONS-SC-OSC-18.0 SFP. Otherwise, OSC might not work as expected.

b. If you want to connect SFP OSC to SFP OSC ports, set proper Rx/Tx power values in both ends using optical attenuators. If SFP GREEN LED in both ends glow and EOC-E alarm is not still cleared, adjust the power values using attenuators until the EOC-E alarm clears.

c. Ensure to use same wavelength SFPs in both near end and far end. 1518 nm OSC SFP will not work with other wavelength SFPs.

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. EOC-L is not supported on OSCM or TNC/TNC-E cards.

The LDCC consists of nine bytes, D4 through D12, in the SONET overhead. The bytes convey information about OAM&P. The NCS system uses the LDCCs on the SONET line layer to communicate network management information.

Warning **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.

Clear the EOC-L Alarm

Procedure

Complete the "Clear the EOC Alarm" procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

Warning **High-performance devices on this card can get hot during operation. To remove the card, hold it by the faceplate and bottom edge. Allow the card to cool before touching any other part of it or before placing it in an antistatic bag.** Statement 201

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, 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 , on page 320, is raised. The standby path generates a path-type alarm. For more information about provisioning PPMs (SFPs), refer to the Installing the GBIC, SFP, SFP+, and XFP Optical Modules in Cisco ONS Platforms document.

Clear the EQPT Alarm

Procedure

Step 1 If traffic is active on the alarmed port, you could need to switch traffic away from it. See the Protection Switching, Lock Initiation, and Clearing, on page 387 procedure for commonly used traffic-switching procedures.

Step 2 Complete the Reset a Card in CTC, on page 391 procedure 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 , on page 393 procedure for the reporting card.

Warning **High-performance devices on this card can get hot during operation. To remove the card, hold it by the faceplate and bottom edge. Allow the card to cool before touching any other part of it or before placing it in an antistatic bag.** Statement 201

Step 5 If the physical reseat of the card fails to clear the alarm, complete the Physically Replace a Card, on page 394 procedure for the reporting card.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

EQPT-DEGRADE

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Objects: EQPT

The Equipment Degrade condition is raised when a permanent failure that limits or compromises the normal behavior of the card (without impact on traffic) is detected.

Clear the EQPT-DEGRADE Condition

Procedure

Remove and reinsert the card where the EQPT-DEGRADE condition is raised. If the reinsertion does not clear the alarm, replace the card. Complete the Physically Replace a Card, on page 394 procedure to replace the card.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

EQPT-DIAG

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: EQPT

e alarm indicates that a software or hardware failure has occurred on the reporting card. This alarm can be raised against a traffic card or a cross-connect card.

Clear the EQPT-DIAG Alarm

Procedure

Step 1 Complete the Remove and Reinsert (Reseat) Any Card , on page 393 procedure for the alarmed card

Step 2 If the alarm does not clear, complete the Physically Replace a Card, on page 394 procedure if it is raised against a traffic card, or complete the Generic Signal and Circuit Procedures, on page 394 procedure if the alarm is raised against the cross-connect card.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

EQPT-FAIL

Default Severity: Major (MJ), Non-Service-Affecting (NSA)

Logical Object: EQPT

An Equipment Failure (EQPT-FAIL) alarm is raised when diagnostic circuit detects a card ASIC failure. This alarm indicates that a hardware or communication failure has occurred on the reporting card.

Clear the EQPT-FAIL Alarm

Procedure

Step 1 Complete the procedure for the reporting card.

Step 2 Verify that the reset is complete and error-free and that no new related alarms appear in . Verify the LED status. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

Step 3 If reset does not clear the alarm, complete the Remove and Reinsert (Reseat) Any Card , on page 393 procedure for the reporting card.

Warning **High-performance devices on this card can get hot during operation. To remove the card, hold it by the faceplate and bottom edge. Allow the card to cool before touching any other part of it or before placing it in an antistatic bag.** Statement 201

Step 4 If the physical reseat of the card fails to clear the alarm, complete the Physically Replace a Card, on page 394 procedure for the reporting card.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

EQPT-FPGA-IMAGE-AVAILABLE

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

Logical Object: EQPT

The EQPT-FPGA-IMAGE-AVAILABLE condition occurs when there is a mismatch between the running trunk FPGA version and the package version.

Clear the EQPT-FPGA-IMAGE-AVAILABLE Condition

Procedure

Perform a manual FPGA upgrade.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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 NCS system. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Clear the EQPT-MISS Alarm

Procedure

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, on page 399 procedure.

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 Hardware Installation 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.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

ERFI-P-SRVR

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

Logical Object: STSMON, STSTRM

The Three-Bit ERFI Path Server condition is triggered on DS-1, DS-3, or VT circuits when the AIS-P , on page 102 or the LOP-P , on page 237 is raised on the transmission signal.

Clear the ERFI-P-SRVR Condition

Procedure

Complete the Clear the LOP-P Alarm, on page 238 procedure. This should clear the ERFI condition.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

ESMC-FAIL

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: GE, TRUNK

An Ethernet Synchronization Messaging Channel Fail (ESMC-FAIL) alarm is raised when a SyncE port fails to receive the ESMC protocol data units (PDU) for 5 seconds.

Clear the ESMC-FAIL Alarm

Procedure

Step 1 Verify if the far end port is enabled for SyncE and is sending ESMC PDUs.

Step 2 Verify if the Ethernet link is up on the client and SA alarms are not present on it.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

ETH-LINKLOSS

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: NE

The Rear Panel Ethernet Link Removed condition, if enabled in the network defaults, is raised under the following conditions:

- The node.network.general.AlarmMissingBackplaneLAN field in NE default is enabled.
- The node is configured as a gateway network element (GNE).
- The backplane LAN cable is removed.

Clear the ETH-LINKLOSS Alarm

Procedure

Step 1 To clear this condition, reconnect the backplane LAN cable. Refer to the Hardware Installation Guide for procedures to install this cable.

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.

EVAL-LIC

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: EQPT

The Evaluation License (EVAL-LIC) alarm is raised to indicate that an valid evaluation license is in use.

Clear the EVAL-LIC Alarm

The EVAL-LIC alarm clears in one of the following scenarios:

- When the user discontinues or disables the associated feature that raised the evaluation license alarm. After this alarm clears, the line card resumes normal operation. The line card tracks the remaining validity period of the evaluation license that was disabled by the user.
- When the validity period of the evaluation license is expired. After the validity period, the card raises an LICENSE-EXPIRED.
- When a permanent license is installed.

Procedure

Procure and install a permanent license. For more information on installing a license, see the Licensing Configuration Guide.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

EXC-BP

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Objects: OTS

The Excessive Back Propagation condition occurs due to excessive backscattered Raman pump power at the LINE-RX connector. This condition is caused either due to a dirty connector, bad optical patch panel connection, or disconnected LINE-RX connector. When the EXC-BP alarm is raised, the level of backscattered power is at a hazardous level, with the risk of possible damage to the unit and/or the external equipment.

Clear the EXC-BP Condition

Procedure

Step 1 Verify all the fibers between the LINE RX and patch-panel are connected.

Step 2 Clean the connectors using site practices or, if none exists, complete the procedure in the Maintain the Node chapter of the Procedure Guide.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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 system and CTC could be affected. The network management LAN is the data network connecting the workstation running the CTC software to the control card. The problem causing the alarm is external to the ONS system.

Troubleshoot the network management LAN connected to the control card 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

Procedure

Step 1 Verify that the network device port connected to the control card 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 control card and the network management LAN.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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

Procedure

Follow your standard operating procedure to remedy environmental conditions that cause alarms. The alarm clears when the situation is remedied.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

FAILTOSW (2R, EQPT, ESCON, FC, GE, ISC, OCN/STMN, TRUNK, OTS)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Objects: 2R, EQPT, ESCON, FC, GE, ISC, OCN, STMN, TRUNK, OTS

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 Procedure Guide*Manage the Node document.

Clear the FAILTOSW (2R, EQPT, ESCON, FC, GE, ISC, OCN/STMN, TRUNK, OTS) Condition

Procedure

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, on page 394 procedure. 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.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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 Procedure Guide*Manage the Node document.

Clear the FAILTOSW (TRUNK) Condition

Procedure

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, on page 394 procedure. 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.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

FAILTOSW-HO

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: VCMON-HP

The High-Order Path Failure to Switch to Protection condition occurs when a high-order path circuit fails to switch to the working or protect electrical circuit using the MANUAL command.

Clear the FAILTOSW-HO Condition

Procedure

Complete the Clear the FAILTOSW (2R, EQPT, ESCON, FC, GE, ISC, OCN/STMN, TRUNK, OTS) Condition, on page 167 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

FAILTOSW-PATH

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: STSMON, VT-MON

The Fail to Switch to Protection Path condition occurs when the working circuit does not switch to the protection circuit on a path protection configuration. Common causes of the FAILTOSW-PATH alarm include a missing or defective protect port, a lockout set on one of the path protection nodes, or path-level alarms that would cause a path protection switch to fail.

Clear the FAILTOSW-PATH Condition in a Path Protection Configuration

Procedure

Step 1 Look up and clear the higher-priority alarm. Clearing this alarm frees the standby card and clears the FAILTOSW-PATH condition.

Note A higher-priority alarm is an alarm raised on the working electrical card using the 1:N card protection group. The working DS-N card is reporting an alarm but not reporting a FAILTOSW condition.

Step 2 If the condition does not clear, replace the active OC-N card that is reporting the higher-priority alarm. Complete the Physically Replace a Card, on page 394 procedure. Replacing the active OC-N card that is reporting the higher-priority alarm allows traffic to revert to the active slot. Reverting frees the standby card, which can then take over traffic from the card reporting the lower-priority alarm and the FAILTOSW-PATH condition.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

FAN

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: FAN

The Fan Failure alarm indicates a problem with the fan-tray assembly. When the fan-tray assembly is not fully functional, the temperature of the ONS system can rise above its normal operating range.

The fan-tray assembly contains six fans and needs a minimum of five working fans to properly cool the shelf. However, even with five working fans, the fan-tray assembly could need replacement because a sixth working fan is required for extra protection against overheating.

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.

Note FAN-FAIL alarm is not raised if BAT-FAIL alarm appears on the power module.

Clear the FAN Alarm

Procedure

Step 1 Determine whether the air filter needs replacement. Complete the Inspect, Clean, and Replace the Air Filter, on page 397 procedure.

Step 2 If the filter is clean, complete the Remove and Reinsert a Fan-Tray Assembly, on page 398 procedure.

Step 3 If the fan does not run or the alarm persists, complete the Replace the Fan-Tray Assembly, on page 399 procedure. The fan should run immediately when correctly inserted.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

FAPS

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Objects: TRUNK

The Fast Automatic Protection Switching condition is applicable to GEXP/10GEXP cards. This condition occurs when the protection port, on the primary card, switches from blocking to forwarding state.

Clear the FAPS Alarm

Procedure

When the cause of switching disappears, the protection port switches from the forwarding to the blocking state, and the FAPS alarm clears.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

FAPS-CONFIG-MISMATCH

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: EQPT

The Fast Automatic Protection Switching (FAPS) Config Mismatch condition is raised when a GE-XP or 10GE-XP card that is provisioned as a primary card in a FAPS ring, resets or when one of the primary card's trunk port is not set to Blocking.

Clear the FAPS-CONFIG-MISMATCH Condition

Procedure

Check the configuration of the primary card. Ensure that at least one of the trunk ports of the primary card is in the blocking state and the FAPS ring is complete.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

FC-NO-CREDITS

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Objects: Client port

The Fibre Channel Distance Extension Credit Starvation alarm occurs on storage access networking (SAN) Fibre Channel/Fiber Connectivity (FICON) cards when the congestion prevents the GFP transmitter from sending frames to the card port. For example, the alarm can be raised when an operator configures a card to autodetect framing credits but the card is not connected to an interoperable FC-SW-standards-based Fibre Channel/FICON port.

FC-NO-CREDITS is raised only if transmission is completely prevented. (If traffic is slowed but still passing, this alarm is not raised.)

Clear the FC-NO-CREDITS Alarm

Procedure

Step 1 If the port is connected to a Fibre Channel/FICON switch, make sure it is configured for interoperation mode using the manufacturer's instructions.

Step 2 If the port is not connected to a switch, turn off Autodetect Credits by completing the following steps:

a) Double-click the card.
b) Click the **Provisioning** > **Port** > **General** tabs.
c) Under Admin State, click the cell and choose OOS,MT (or Locked,maintenance).
d) Click **Apply**.
e) Click the **Provisioning** > **Port** > **Distance Extension** tabs.
f) Uncheck the Autodetect Credits column check box.
g) Click **Apply**.
h) Click the **Provisioning** > **Port** > **General** tabs.
i) Under Admin State, click the cell and choose **IS** (or **Unlocked**).
j) Click **Apply**.

Step 3 Program the Credits Available value based on the buffers available on the connected equipment by completing the following steps:

Note The NumCredits entry must be provisioned to a value smaller than or equal to the receive buffers or credits available on the connected equipment.

a) Double-click the card.
b) Click the **Provisioning** > **Port** > **Distance Extension** tabs.
c) Enter a new value in the Credits Available column.
d) Click **Apply**.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into

http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

FDI

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Objects: OCH, OCH-TERM, OMS, OTS, EQPT

The Forward Defect Indication (FDI) condition is part of network-level alarm correlation. It is raised at the far end when the OCH optical payload is missing due to an optical channel signal (LOS), light (LOS-P), or optical power (OPWR-LFAIL) alarm root cause.

An LOS, LOS-P, or OPWR-LFAIL alarm on a circuit causes multiple alarms for each channel. Correlation simplifies troubleshooting by reporting a single alarm for multiple alarms having one root cause, then demoting the root alarms so that they are only visible in the Conditions window (showing their original severity.)

FDI clears when the optical channel is working on the aggregated or single-channel optical port.

Note Network-level alarm correlation is only supported for communication alarms. It is not supported for equipment alarms.

Clear the FDI Condition

Procedure

Clear the root-cause service-affecting alarm by using one of the following procedures, as appropriate:

- Clear the LOS (OTS) Alarm, on page 243
- Clear the LOS (TRUNK) Alarm, on page 245
- Clear the LOS-P (OCH) Alarm, on page 249
- Clear the LOS-P (AOTS, OMS, OTS) Alarm, on page 247
- Clear the LOS-P (TRUNK) Alarm, on page 252
- Clear the OPWR-LFAIL Alarm, on page 287

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

FE-FRCDWKSWBK-SPAN

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: STMN

The Far End Forced Switch Back to WorkingSpan condition is raised on a far-end 1+1 protect port when it is Force switched to the working port.

Note WKSWBK-type conditions apply only to nonrevertive circuits.

Clear the FE-FRCDWKSWBK-SPAN Condition

Procedure

Complete the Clear a 1+1 Force or Manual Switch Command, on page 388 procedure for the far-end port.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

FE-FRCDWKSWPR-SPAN

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: STMN

The Far End Working Facility Forced to Switch to Protection Span condition occurs from a far-end node when a span on a four-fiber BLSR is forced from working to protect using the Force Span command. This condition is only visible on the network view Conditions tab. The port where the Force Switch occurred is indicated by an F on the network view detailed circuit map. This condition is accompanied by WKSWPR.

Clear the FE-FRCDWKSWPR-SPAN Condition

Procedure

Step 1 To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE alarm.

Step 2 Log into the node that links directly to the card reporting the FE condition.

Step 3 Clear the main alarm.

Step 4 If the FE-FRCDWKSWPR-SPAN condition does not clear, complete the Clear a BLSR External Switching Command, on page 390procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

FE-MANWKSWBK-SPAN

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: STMN

The Far End Manual Switch Back to WorkingSpan condition occurs when a far-end span is Manual switches back to working.

Note WKSWBK-type conditions apply only to nonrevertive circuits.

Clear the FE-MANWKSWBK-SPAN Condition

Procedure

Step 1 To troubleshoot the FE condition, determine which node and card is linked directly to the card reporting the FE condition. For example, an FE condition on a card in Slot 12 of Node 1 could relate to a main alarm from a card in Slot 6 of Node 2.

Step 2 Log into the node that is linked directly to the card reporting the FE condition.

Step 3 Complete the Clear a BLSR External Switching Command, on page 390 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

FE-MANWKSWPR-SPAN

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: STMN

The Far-End Span Manual Switch Working Facility to Protect condition occurs when a four-fiber BLSR span is switched from working to protect at the far-end node using the Manual Span command. This condition is only visible on the network view Conditions tab and is accompanied by WKSWPR. The port where the Manual Switch occurred is indicated by an M on the network view detailed circuit map.

Clear the FE-MANWKSWPR-SPAN Condition

Procedure

Step 1 To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE alarm. For example, an FE condition on a card in Slot 12 of Node 1 could link to the main condition from a card in Slot 6 of Node 2.

Step 2 Log into the node that links directly to the card reporting the FE condition.

Step 3 Complete the Clear a BLSR External Switching Command, on page 390 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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_10E_C, TXP_MR_10E_L, TXP_MR_2.5G, TXPP_MR_2.5G, MXP_10G, MXP_MR_10E, ADM-10G, and OTU2_XP. 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 , on page 304 alarm.

The alarm is related to ITU-T G.709 encapsulation and is only raised against a trunk port.

When the OUT2 client is directly connected with another OTU2 client with standard FEC and Disabled FEC on either side, the FEC-MISM alarm is not raised on the 400G-XP-LC card. The Uncorrected FEC Word condition is raised on the standard FEC side.

Clear the FEC-MISM Alarm

Procedure

Step 1 In node view (single-shelf mode) or shelf view (multishelf mode), double-click the TXP_MR_10G, TXP_MR_10E, TXP_MR_10E_C, TXP_MR_10E_L, TXP_MR_2.5G, TXPP_MR_2.5G, MXP_MR_10G, MXP_MR_10E, ADM-10G, and OTU2_XP 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, on page 175 through Step 3, on page 175.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

FEED-MISMATCH

Default Severity: Major (MJ), Service Affecting (SA)

Logical Objects: EQPT

The Feed Mismatch alarm is raised when the mandatory power module input feed based on Power Supply Unit (PSU) configuration is disconnected or incorrectly connected.

The alarm is cleared when the mandatory feed connection of power module is connected as per the PSU configuration. To re-configure the feed connection, refer to Power Redundancy .

FEPRLF

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: OCN

The Far-End Protection Line Failure alarm occurs when there was an SF (TRUNK) , on page 342 condition on the protect card APS channel coming into the node.

Note The FEPRLF alarm occurs on the NCS only when bidirectional protection is used on optical (traffic) cards in a 1+1 protection group configuration.

Clear the FEPRLF Alarm on an BLSR

Procedure

Step 1 To troubleshoot the FE alarm, determine which node and card is linked directly to the card reporting the FE alarm. For example, an FE alarm or condition on a card in Slot 16 of Node 1 could relate to a main alarm from a card in Slot 16 in Node 2.

Step 2 Log into the node that is linked directly to the card reporting the FE alarm.

Step 3 Clear the main alarm. Refer to the appropriate alarm section in this chapter for procedures.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

FIBERTEMP-DEG

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: AOTS

The Fiber Temperature Degrade alarm occurs when a DWDM card (OPT-AMP-C) internal heater-control circuit fails. Degraded temperature can cause some signal drift.

Note For general information about DWDM cards, refer to the Card Reference chapter in the *Cisco ONS 15454 DWDM Reference Manual*. For information about changing their settings, refer to the Change DWDM Card Settings chapter in the *Cisco ONS 15454 DWDM Procedure Guide*.

Clear the FIBERTEMP-DEG Alarm

Procedure

For the alarmed card, complete the Physically Replace a Card, on page 394 procedure.

Warning **High-performance devices on this card can get hot during operation. To remove the card, hold it by the faceplate and bottom edge. Allow the card to cool before touching any other part of it or before placing it in an antistatic bag.** Statement 201

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

FIPS-TEST-FAILED

Default Severity: Critical (CR)

Logical Object: EQPT

The FIPS Test Failed alarm is raised on the WSE card. This alarm is raised when the FIPS test fails on the WSE card.

A secure library is used for the FIPS test. A self-test is run on the card during startup to check that the library works with all the algorithms that are supported by FIPS. The FIPS TEST Failed alarm is raised when there is an issue during the self-test on the card.

Clearing the FIPS-TEST-FAILED Alarm

Before you begin

You must have Security super user privileges to clear the alarm.

Procedure

Step 1 Complete the Reset a Card in CTC, on page 391 procedure for the card.

Caution Always use the supplied electrostatic discharge wristband when working with a powered NCS. 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, complete the Physically Replace a Card, on page 394 procedure.

If the troubleshooting procedure does not clear the alarm, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html or call the Cisco Technical Assistance Center (1 800 553-2447) to report the problem.

FORCED-REQ

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: EQPT, ML1000, ML100T, MLFX, STSMON, VT-MON

The Force Switch Request on Facility or Port condition occurs when you enter the Force command on a port to force traffic from a working port to a protect port or protection span (or from a protect port to a working port or span). You do not need to clear the condition if you want the Force switch to remain.

FORCED-REQ is raised for an IEEE 802.17b-based RPR span if the force was requested in the Cisco IOS CLI using the rpr-ieee protection request force-switch {east | west} command. It clears from the RPR-IEEE span when you remove the switch in the CLI. For the IEEE 802.17b-based RPR interface, FORCED-REQ is suppressed by the RPR-PASSTHR alarm. It also suppresses the following alarms:

- MAN-REQ (for an ML-Series object)
- RPR-SF
- RPR-SD
- WTR (for an ML-Series object)

Clear the FORCED-REQ Condition

Procedure

Step 1 Complete the Clear a 1+1 Force or Manual Switch Command, on page 388 procedure.

Step 2 If the condition is raised on an IEEE 802.17b-based RPR span, enter the following command in the CLI in RPR-IEEE interface configuration mode:

```
router(config-if)#no rpr-ieee protection request force-switch {east | west}
```

If the troubleshooting procedure does not clear the alarm, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html or call the Cisco Technical Assistance Center (1 800 553-2447) to report the problem.

FORCED-REQ-SPAN (2R, ESCON, FC, GE, ISC, OCN/STMN, OTS)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Objects: 2R, ESCON, FC, GE, ISC, OCN/STMN, OTS

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 Procedure Guide*.

Note For more information about protection schemes, refer to the Manage the Node document.

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 Procedure Guide*.

Note For more information about protection schemes, refer to the Manage the Node document.

FP-LINK-LOSS

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: EQPT

The Front Port Link Loss condition occurs when a LAN cable is not connected to the front port of the control card.

Clear the FP-LINK-LOSS Condition

Procedure

Connect a LAN cable to the front port of the control card.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

FPGA-UPGRADE-FAILED

Default Severity: Critical (CR), Service Affecting (SA)

Logical Object: Equipment

The FPGA-UPGRADE-FAILED alarm is raised when the FPGA upgrade on the TNCS-2 or TNCS-2O control card fails.

Clear the FPGA-UPGRADE-FAILED Alarm

Procedure

Reboot the TNCS-2/TNCS-2O control card on the chassis.

If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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.

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.

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.

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.

FRNGSYNC

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: NE-SREF

The Free Running Synchronization Mode condition occurs when the reporting NCS 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 NCS system node relying on an internal clock.

Note If the NCS system is configured to operate from its internal clock, disregard the FRNGSYNC condition.

Clear the FRNGSYNC Condition

Procedure

Step 1 If the 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 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 , on page 359 alarm and the SYNCSEC , on page 360 alarm.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

Note FSTSYNC is an informational condition. It does not require troubleshooting.

FTA-MISMATCH

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: EQPT

The Fan Tray Mismatch condition is raised on the ADM-10G card and OTU2_XP. It indicates that an unsupported version of the fan tray assembly is installed in the shelf. The ADM-10G and OTU2_XP card must be installed in a shelf that has FTA version 4 or higher.

Clear the FTA-MISMATCH Condition

Procedure

Obtain the correct fan tray assembly, and replace the existing FTA with the new one by following the Replace the Fan-Tray Assembly, on page 399 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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-AMP-C),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.

Note This alarm is applicable only when the amplifier working mode is set to Control Gain.

Clear the GAIN-HDEG Alarm

Procedure

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 the procedure 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, 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, on page 394 procedure for the reporting card.

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 **High-performance devices on this card can get hot during operation. To remove the card, hold it by the faceplate and bottom edge. Allow the card to cool before touching any other part of it or before placing it in an antistatic bag.** Statement 201

Note Before disconnecting any optical amplifier card fiber for troubleshooting, ensure that the optical amplifier card is unplugged.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

GAIN-HFAIL

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: AOTS

The Gain High Degrade alarm is raised on an amplifier card (OPT-AMP-C) 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.)

Note This alarm is applicable only when the amplifier working mode is set to Control Gain.

Clear the GAIN-HFAIL Alarm

Procedure

For the alarmed card, complete the Clear the GAIN-HDEG Alarm, on page 183 procedure.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

GAIN-LDEG

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: AOTS

Gain Low Degrade (GAIN-LDEG) alarm is raised on an amplifier card (OPT-BST, OPT-PRE, OPT-AMP-C, or OPT-AMP-17-C), 40-SMR1-C, or 40-SMR2-C card when the amplifier does not reach the Gain Low Degrade Threshold. (This value is automatically provisioned with the gain setpoint, but the alarm threshold is 2 dBm lower than the setpoint.)

Note This alarm is applicable only when the amplifier working mode is set to Control Gain.

Clear the GAIN-LDEG Alarm

Procedure

For the alarmed card, complete the Clear the GAIN-HDEG Alarm, on page 183 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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, OPT-PRE, OPT-AMP-C, or OPT-AMP-17-C) 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.

Clear the GAIN-LFAIL Alarm

Procedure

For the alarmed card, complete the Clear the GAIN-HDEG Alarm, on page 183 alarm.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

GAIN-NEAR-LIMIT

Default Severity: Minor (MN), Non-Service Affecting (NSA)

Logical Objects: AOTS

The GAIN-NEAR-LIMIT alarm is raised against optical amplifier cards and SMR cards. It is raised when the Automatic Power Control (APC) regulates an amplifier gain and its value reaches +2 or -2 dB, within the minimum and maximum gain range. The gain check is performed automatically every hour and during the APC run.

Clear the GAIN-NEAR-LIMIT Alarm

Procedure

GAIN-NEAR-LIMIT alarm clears in one of these scenarios:

a) To clear the alarm manually, correct the span loss changes from previous configuration. It reduces AMP gain and clears the alarm.
b) The clear the alarm manually, diable the gain limit check by using .
c) The alarm clears automatically when the periodic check determines that the amplifier gain and its value is not in the range of +2 or -2 dB, within the minimum and maximum gain range.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

GCC-EOC

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: TRUNK, EQPT

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, TXP_MR_10E_C, TXP_MR_10E_L, MXP_2.5G_10G, MXP_2.5G_10E, ADM-10G, and OTU2_XP 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.

Clear the GCC-EOC Alarm

Procedure

Complete the "Clear the EOC Alarm" procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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_10E_C, TXP_MR_10E_L, TXP_MR_2.5G,TXPP_MR_2.5G,MXP_MR_2.5G, MXPP_MR_2.5G, GE-XP, 10GE, and ADM-10G cards when the Ethernet signal incoming on the Client-Rx port is out of synchronization.

Clear the GE-OOSYNC (FC, GE, ISC) Alarm

Procedure

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 Installing the GBIC, SFP, SFP+, and XFP Optical Modules in Cisco ONS Platforms document.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

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_10E_C, TXP_MR_10E_L, TXP_MR_2.5G,TXPP_MR_2.5G,MXP_MR_2.5G, MXPP_MR_2.5G, GE-XP, 10GE, and ADM-10G cards only when the ITU-T G.709 encapsulation framer is disabled.

Clear the GE-OOSYNC (TRUNK) Alarm

Procedure

Step 1 Verify that ITU-T G.709 encapsulation is disabled:

a) In node view (single-shelf mode) or shelf view (multishelf mode), 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.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

GFP-CSF-SIGLOSS

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: GFP-FAC

The GFP Client Signal Fail due to Sigloss is a secondary alarm raised on local GFP data ports when a remote Service-Affecting (SA) alarm causes invalid data transmission. The alarm is raised locally on AR_MXP and

AR_XP GFP data ports and does not indicate that a Service-Affecting (SA) failure is occurring at the local site, but that a SIGLOSS alarm caused by an event is affecting a remote data port's transmission capability.

Clear the GFP-CSF-SIGLOSS Alarm

Procedure

Clear the Service-Affecting (SA) alarm at the remote data port.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

GFP-CSF-SYNCLOSS

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: GFP-FAC

The GFP Client Signal Fail Due to Syncloss alarm is a secondary alarm raised on local GFP data ports when a remote Service-Affecting (SA) alarm causes invalid data transmission. The alarm is raised locally on AR_MXP and AR_XP GFP data ports and does not indicate that a Service-Affecting (SA) failure is occurring at the local site, but that a SYNCLOSS alarm caused by an event such as a pulled receive cable is affecting a remote data port's transmission capability.

Clear the GFP-CSF-SYNCLOSS Alarm

Procedure

Clear the Service-Affecting (SA) alarm at the remote data port.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

GFP-LFD

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: CEMR, CE1000, CE100T, FCMR, GFP-FAC, ML1000, ML100T, MLFX

The GFP Loss of Frame Delineation alarm applies to Fibre Channel, FICON GFP, and Ethernet ports. This alarm occurs if there is a faulty SONET connection, if SONET path errors cause GFP header errors in the check sum calculated over payload length (PLI/cHEC) combination, or if the GFP source port sends an invalid PLI/cHEC combination. This loss causes traffic stoppage.

Clear the GFP-LFD Alarm

Procedure

Look for and clear any associated SONET path errors such as LOS or the AU-AIS, on page 113 alarm that originate at the transmit node.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

GFP-UP-MISMATCH

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: CEMR, CE1000, CE100T, FCMR, GFP-FAC, ML1000, ML100T, MLFX

The GFP User Payload Mismatch is raised against Fibre Channel/FICON ports supporting GFP. It occurs when the received frame user payload identifier (UPI) does not match the transmitted UPI and all frames are dropped. The alarm is caused by a provisioning error, such as the port media type not matching the remote port media type. For example, the local port media type could be set to Fibre Channel—1 Gbps ISL or Fibre Channel—2 Gbps ISL and the remote port media type could be set to FICON—1 Gbps ISL or FICON—2 Gbps ISL.

Clear the GFP-UP-MISMATCH Alarm

Procedure

Step 1 Ensure that the transmit port and receive port are identically provisioned for distance extension by completing the following steps:

a) Double-click the card to open the card view.
b) Click the **Provisioning** > **Port** > **Distance Extension** tabs.
c) Check the check box in the **Enable Distance Extension** column.
d) Click **Apply**.

Step 2 Ensure that both ports are set for the correct media type. For each port, complete the following steps:

a) Double-click the card to open the card view (if you are not already in card view).
b) Click the **Provisioning** > **Port** > **General** tabs.
c) Choose the correct media type (**Fibre Channel - 1Gbps ISL**, **Fibre Channel - 2 Gbps ISL**, **FICON - 1 Gbps ISL**, or **FICON - 2 Gbps ISL**) from the drop-down list.
d) Click **Apply**.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into

http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

HELLO

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: OCN

The Open Shortest Path First (OSPF) Hello alarm is raised when the two end nodes cannot bring an OSPF neighbor up to the full state. Typically, this problem is caused by an area ID mismatch, and/or OSPF HELLO packet loss over the DCC.

Clear the HELLO Alarm

Procedure

Ensure that the area ID is correct on the missing neighbor by completing the following steps:

a) In node view, click the **Provisioning** > **Network** > **OSPF** tabs.
b) Ensure that the IP address in the Area ID column matches the other nodes.
c) If the address does not match, click the incorrect cell and correct it.
d) Click **Apply**.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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.

Clear the HIBATVG Alarm

Procedure

The problem is external to the system. Troubleshoot the power source supplying the battery leads.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

HI-BER

(Supported only in Release 9.2.2)

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Objects: FC, GE

The High Bit Error Rate (HI-BER) alarm is raised on the OTU2_XP card when the client and trunk ports receive 16 or more invalid sync-headers in 125 microseconds. The HI-BER alarm occurs when the OTU2_XP card is configured with 10 GE or 10 G FC payloads.

Clear the HI-BER Alarm

Procedure

The alarm clears under the following conditions:

- When high bit error rate is not received on the card port.
- When one of the following OTN alarms are raised on the trunk port:
  - LOF (TRUNK)
  - LOM
  - LOS-P (TRUNK)
  - ODUK-AIS-PM
  - ODUK-LCK-PM
  - ODUK-OCI-PM
  - OTUK-AIS

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

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

Procedure

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.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

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, TXP_MR_10E_C, TXP_MR_10E_L, MXP_2.5G_10G, OC192-XFP, ADM-10G, and OTU2_XP 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.

Clear the HI-LASERBIAS Alarm

Procedure

Complete the Physically Replace a Card, on page 394 procedure. Replacement is not urgent and can be scheduled during a maintenance window.

Warning **High-performance devices on this card can get hot during operation. To remove the card, hold it by the faceplate and bottom edge. Allow the card to cool before touching any other part of it or before placing it in an antistatic bag.** Statement 201

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 Protection Switching, Lock Initiation, and Clearing, on page 387 section for commonly used traffic-switching procedures.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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, MXP, and ADM-10G 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 , on page 146 alarm, is raised at the near end.

Clear the HI-LASERTEMP Alarm

Procedure

Step 1 In node view (single-shelf mode) or shelf view (multishelf mode), 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, on page 391 procedure for the MXP or TXP card.

Step 5 If the alarm does not clear, complete the Physically Replace a Card, on page 394 procedure for the reporting MXP or TXP card.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

HI-RXPOWER

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Objects: 2R, ESCON, FC, GE, ISC, OCN/STMN, TRUNK, EQPT

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, TXP_MR_10E_C, TXP_MR_10E_L, MXP_2.5G_10G, OC192-XFP, GE-XP, 10GE-XP, ADM-10G, or OTU2_XP card. HI-RXPOWER occurs when the measured optical power of the received signal exceeds the threshold. The threshold value is user-provisionable.

Clear the HI-RXPOWER Alarm

Procedure

Step 1 Check the PM of the TRUNK-RX port. Verify that received power is above the optics threshold:

a) In node view (single-shelf mode) or shelf view (multishelf mode), 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. 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, or 40DMX). If no site cleaning practices are available, refer to the fiber cleaning procedure in the Maintain the Node chapter of the Configuration Guide.

Step 3 Determine whether a bulk attenuator is specified by the Cisco Transport Planner 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, or 40DMX) 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 cards belonging to the OCHNC circuit destinating at the faulty TXP/MXP. Possible alarms include amplifier Gain alarms (the GAIN-HDEG , on page 183 alarm, the GAIN-HFAIL , on page 184 alarm, the GAIN-LDEG , on page 185 alarm, or GAIN-LFAIL , on page 185) alarm; APC alarms (APC-CORR-SKIPPED , on page 104 alarm or APC-OUT-OF-RANGE , on page 106 alarm), or LOS-P alarms on the Add or Drop ports involved in the OCHNC circuit.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

HITEMP

Default Severity: Critical (CR), Service-Affecting (SA) for NE; Default Severity: Minor (MN), Non-Service-Affecting (NSA) for EQPT

Logical Objects: EQPT, NE

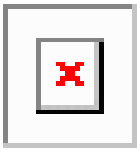
The High Temperature alarm occurs when the temperature of the ONS system is above 122 degrees F (50 degrees C).

Clear the HITEMP Alarm

Procedure

Step 1 View the temperature displayed on the system LCD front panel. For example, the front panel is illustrated in Figure 23: Shelf LCD Panel, on page 196.

Figure 23: 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 system shelf.

Step 4 If airflow is not blocked, physically ensure that blank faceplates fill the 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 Air Filter, on page 397 procedure.

Step 6 If the fan does not run or the alarm persists, complete the Replace the Fan-Tray Assembly, on page 399 procedure.

Note The fan should run immediately when correctly inserted.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

HI-RXTEMP

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Objects: TRUNK

The Equipment High Receive temperature alarm refers to the temperature of the trunk card port for the TXP and MXP cards. The HI-RXTEMP threshold is user-provisionable.

Clear the HI-RXTEMP Alarm

Procedure

Step 1 If a shelf HITEMP alarm is also present, complete the Clear the HITEMP Alarm.

Step 2 If a HI-LASERTEMP alarm is also present, complete the Clear the HI-LASERTEMP Alarm .

Note If no data alarms have occurred, the card does not need to be replaced immediately.

Step 3 If the alarm does not clear, log onto http://www.cisco.com/tac for more information or call TAC (1-800-553-2447).

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, OC192-XFP, ADM-10G, or OTU2_XP card transmitted optical signal power. HI-TXPOWER occurs when the measured optical power of the transmitted signal exceeds the threshold.

Clear the HI-TXPOWER Alarm

Procedure

Step 1 Check the PM of the Trunk-Tx port. Verify that received power is above the optics threshold:

a) In node view (single-shelf mode) or shelf view (multishelf mode), 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 SVO Web Interface** > **SVO Topology** > **Rack View** > **Performance Tab** > **History 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 SVO Web Interface** > **SVO Topology** > **Rack View** > **Performance Tab** > **PM Live Data**tabs.

d) Ensure that a proper threshold has been provisioned for the receive value. 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 (40MUX, 32WSS-O, or 40WSS-C) 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, on page 394 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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

Procedure

Step 1 Clear additional alarms that relate to timing, such as:

- FRNGSYNC , on page 182
- FSTSYNC , on page 182
- LOF (BITS) , on page 232
- LOS (BITS) , on page 240
- MANSWTOINT, on page 264
- MANSWTOPRI , on page 264
- MANSWTOSEC , on page 264
- MANSWTOTHIRD , on page 264
- SWTOPRI , on page 356
- SWTOSEC , on page 357
- SWTOTHIRD , on page 357
- SYNC-FREQ , on page 358
- SYNCPRI , on page 359
- SYNCSEC , on page 360
- SYNCTHIRD , on page 360

Step 2 Reestablish a primary and secondary timing source according to local site practice. If none exists, refer to the Turn Up the Network chapter in the Configuration Guide.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

HP-DEG

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: VMMON-HP, VCTRM-HP

An HP-DEG condition is similar to the SD (TRUNK) , on page 338 condition, but it applies to the HP layer of the SDH overhead. A HP-DEG alarm travels on the B3 byte of the SDH overhead.

For path protection protected circuits, the BER threshold is user-provisionable and has a range for HP-DEG from 1E–9 dBm to 1E–5 dBm. For MS-SPRing 1+1 and unprotected circuits, the BER threshold value is not user-provisionable and the error rate is hard-coded to 1E–6 dBm.

On path protection configurations, an HP-DEG condition causes a switch from the working card to the protect card at the path level. On MS-SPRing, 1+1, and on unprotected circuits, an HP-DEG condition does not cause switching.

The BER increase that causes the condition is sometimes caused by a physical fiber problem such as a poor fiber connection, a bend in the fiber that exceeds the permitted bend radius, or a bad fiber splice.

HP-DEG clears when the BER level falls to one-tenth of the threshold level that triggered the alarm.

Clear the HP-DEG Condition

Procedure

Complete the Clear the SD (TRUNK) Condition, on page 338 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

HP-ENCAP-MISMATCH

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: VCTRM-HP

The High-Order Path Encapsulation C2 Byte Mismatch alarm applies to ML-Series Ethernet cards. It occurs when the first three following conditions are met and one of the last two is false:

- The received C2 byte is not 0x00 (unequipped).

- The received C2 byte is not a PDI value.
- The received C2 does not match the expected C2.
- The expected C2 byte is not 0x01 (equipped unspecified).
- The received C2 byte is not 0x01 (equipped unspecified).

(This is in contrast to LP-PLM, which must meet all five criteria.) For an HP-ENCAP-MISMATCH to be raised, there is a mismatch between the received and expected C2 byte, with either the expected byte or received byte value being 0x01.

An example situation that would raise an HP-ENCAP-MISMATCH alarm is if a circuit created between two ML-Series cards has GFP framing provisioned on one end and high-level data link control (HDLC) framing with LEX encapsulation provisioned on the other. The GFP framing card transmits and expects a C2 byte of 0x1B, while the HDLC framing card transmits and expects a C2 byte of 0x01.

A mismatch between the transmit and receive cards on any of the following parameters can cause the alarm:

- Mode (HDLC, GFP-F)
- Encapsulation (LEX, HDLC, PPP)
- CRC size (16 or 32)
- Scrambling state (on or off)

This alarm is demoted by a path label mismatch (PLM) such as LP-PLM.

Note By default, an HP-ENCAP-MISMATCH alarm causes an ML-Series card data link to go down. This behavior can be modified using the command-line interface (CLI) command **no pos trigger defect encap**.

Clear the HP-ENCAP-MISMATCH Alarm

Procedure

Step 1 Ensure that the correct framing mode is in use on the receiving card by completing the following steps:

a) In node view, double-click the ML-Series card to display the card view.
b) Click the **Provisioning** > **Card** tabs.
c) In the Mode drop-down list, ensure that the correct mode (GFP-F or HDLC) is selected. If it is not, choose it and click **Apply**.

Step 2 Ensure that the correct framing mode is in use on the transmit card, and that it is identical to the framing mode used on the receiving card by completing the following steps:

a) In node view, double-click the ML-Series card to display the card view.
b) Click the **Provisioning** > **Card** tabs.
c) In the Mode drop-down list, ensure that the same mode (GFP-F or HDLC) is selected. If it is not, choose it and click **Apply**.

Step 3 If the alarm does not clear, use the ML-Series card CLI to ensure that the remaining settings are correctly configured:

- Encapsulation
- CRC size
- Scrambling state

To open the interface, click the card view **IOS** tab and click **Open IOS Connection**.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

HP-EXC

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Objects: VCMON-HP, VCTRM-HP

An HP-EXC condition is similar to the SF (TRUNK) , on page 342 condition, but it applies to the path layer B3 byte of the SONET overhead. It can trigger a protection switch.

The HP-EXC condition clears when the BER level falls to one-tenth of the threshold level that triggered the condition. A BER increase is sometimes caused by a physical fiber problem, including a poor fiber connection, a bend in the fiber that exceeds the permitted bend radius, or a bad fiber splice.

Clear the HP-EXC Condition

Procedure

Complete the Clear the SF (TRUNK) Condition, on page 342 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

HP-PLM

The HP-PLM condition is not used in this platform in this release. It is reserved for development.

HP-RFI

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

Logical Object: VCMON-HP

The High-Order Remote Failure Indication (RFI) condition indicates that there is a remote failure indication in the high-order (VC-4 or VC-3) path, and that the failure has persisted beyond the maximum time allotted for transmission system protection. The HP-RFI is sent as the protection switch is initiated. Resolving the fault in the adjoining node clears the HP-RFI condition in the reporting node.

Clear the HP-RFI Condition

Procedure

Step 1 Log into the node at the far end of the reporting NCS.

Step 2 Determine whether there are any related alarms, especially the LOS(STM1E, STMN).

Step 3 Clear the main alarm. See the appropriate alarm section in this chapter for procedures.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

HP-TIM

Default Severities: Critical (CR), Service-Affecting (SA) for VCTRM-HP; Minor (MN), Non-Service-Affecting (NSA) for VCMON-HP

Logical Objects: VCMON-HP, VCTRM-HP

The TIM High-Order TIM Failure alarm indicates that the trace identifier J1 byte of the high-order (VC-4 or VC-3) overhead is faulty. HP-TIM occurs when there is a mismatch between the transmitted and received J1 identifier byte in the SONET path overhead. The error can originate at the transmit end or the receive end.

Clear the HP-TIM Alarm

Procedure

Step 1 Use an optical test set capable of viewing SONET path overhead to determine the validity of the J1 byte. For specific procedures to use the test set equipment, consult the manufacturer. Examine the signal as near to the reporting card as possible.

- Examine the signal as close as possible to the output card.

Step 2 If the output card signal is valid, complete the Clear the SYNCPRI Alarm, on page 359 procedure.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

HP-UNEQ

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: VCMON-HP, VCTRM-HP

The signal label mismatch fault (SLMF) Unequipped High-Order Path alarm applies to the C2 path signal label byte in the high-order (VC-4) path overhead. HP-UNEQ occurs when no C2 byte is received in the SONET path overhead.

Clear the HP-UNEQ Alarm

Procedure

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Right-click the alarm to display the Select Affected Circuits shortcut menu.

Step 3 Click **Select Affected Circuits**.

Step 4 When the affected circuits appear, look in the Type column for a virtual circuit (VC).

Step 5 If the Type column does not contain a VC, there are no VCs. Go to Step 7, on page 203.

Step 6 If the Type column does contain a VC, attempt to delete these row(s) by completing the following steps:

Note The node does not allow you to delete a valid VC.

a) Click the VC row to highlight it. Complete the Delete a Circuit, on page 395 procedure.
b) If an error message dialog box appears, the VC is valid and not the cause of the alarm.
c) If any other rows contain VT, repeat Steps 6.a, on page 203through 6.b, on page 203.

Step 7 If all ONS nodes in the ring appear in the CTC network view, verify that the circuits are all complete by completing the following steps:

a) Click the **Circuits** tab.
b) Verify that INCOMPLETE is not listed in the Status column of any circuits.

Step 8 If you find circuits listed as incomplete, verify that these circuits are not working circuits that continue to pass traffic, using an appropriate optical test set and site-specific procedures. For specific procedures to use the test set equipment, consult the manufacturer.

Step 9 If the incomplete circuits are not needed or are not passing traffic, delete the incomplete circuits.

Complete the Delete a Circuit, on page 395 procedure.

Step 10 Recreate the circuit with the correct circuit size. Refer to the Create Circuits and Tunnels chapter in the configuration guide for circuit procedures.

Step 11 Log back in and verify that all circuits terminating in the reporting card are active by completing the following steps:

a) Click the **Circuits** tab.

b) Verify that the **Status** column lists all circuits as active.

Step 12 If the alarm does not clear, clean the far-end optical fiber according to site practice. If no site practice exists, complete the procedure in the Maintain the Node chapter in the Configuration guide.

On the OC192 LR/STM64 LH 1550 card:

Warning **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

Step 13 If the alarm does not clear, complete the Physically Replace a Card, on page 394 procedure for the optical and/or electrical cards.

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.

Note When you replace a card with the identical type of card, you do not need to make any changes to the database.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

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 , on page 195 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

Procedure

Complete the Clear the HITEMP Alarm, on page 196 procedure.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

ILK-FAIL

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: TRUNK

The ADM Peer Group Interlink Failure condition is raised on the ADM-10G card. This condition occurs when one of the following SONET/OTN alarms is detected on the interlink ports of the ADM-10G card.

- LOS (TRUNK) , on page 244 alarm
- LOF (TRUNK) , on page 233 alarm
- SF (TRUNK) , on page 342 alarm

Clear the ILK-FAIL Alarm

Procedure

Clear the root-cause service-affecting alarm by using one of the following procedures, as appropriate:

- Clear the LOS (TRUNK) Alarm, on page 245 procedure
- Clear the LOF (TRUNK) Alarm, on page 234 procedure
- Clear the SF (TRUNK) Condition, on page 342 procedure

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

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 deleted from CTC before physically removing the card from its slot. It is recommended that the card be physically removed from its slot before deleting it from CTC.

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 control 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.

  The working port raises the CR,IMPROPRMVL,SA alarm and the protected port raises the MN,IMPROPRMVL,NSA alarm. The severity on the client ports is changed according to the protection switch state.
- Electrical issues such as short circuit or failure of DC-DC conversion.

Clear the IMPROPRMVL Alarm

Procedure

Step 1 In node view (single-shelf mode) or shelf view (multishelf mode), 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 (or Locked,disabled), ensure that no live traffic is present.

a) In node view (single-shelf mode) or shelf view (multishelf mode), 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, on page 395 procedure.

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 (single-shelf mode) or shelf view (multishelf mode).
b) If you are already in node view (single-shelf mode) or shelf view (multishelf mode), 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) In node view (single-shelf mode) or multishelf view (multishelf mode), 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) In node view (single-shelf mode) or shelf view (multishelf mode), 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**.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

INHSWPR

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: EQPT

The Inhibit Switch To Protect Request on Equipment condition occurs on traffic cards when the ability to switch to protect has been disabled. If the card is part of a 1:1 or 1+1 protection scheme, traffic remains locked onto the working system. If the card is part of a 1:N protection scheme, traffic can be switched between working cards when the switch to protect is disabled.

Clear the INHSWPR Condition

Procedure

Step 1 If the condition is raised against a 1+1 port, complete the Initiate a 1+1 Manual Switch Command, on page 387 procedure.

Step 2 If it is raised against a 1:1 card, complete the Initiate a 1:1 Card Switch Command, on page 388 procedure to switch it back.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

INHSWWKG

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: EQPT

The Inhibit Switch To Working Request on Equipment condition occurs on traffic cards when the ability to switch to working has been disabled. If the card is part of a 1:1 or 1+1 protection scheme, traffic remains locked onto the protect system. If the card is part of a 1:N protection scheme, traffic can be switched between protect cards when the switch to working is disabled.

Clear the INHSWWKG Condition

Procedure

Step 1 If the condition is raised against a 1+1 port, complete the Initiate a 1+1 Manual Switch Command, on page 387 procedure.

Step 2 If it is raised against a 1:1 card, complete the Initiate a 1:1 Card Switch Command, on page 388 procedure to switch it back.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

INCOMPATIBLE-SEND-PDIP

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: SYSTEM

The Incompatible Software alarm is raised when CTC send PDI-P provisioning differs from the host node's provisioning.

Clear the INCOMPATIBLE-SEND-PDIP Alarm

Procedure

Reconfigure CTC send PDI-P alarm capability to align with the host node settings.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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.

The INCOMPATIBLE-SW alarm is also raised when CTC nodes in the network have R10.6 packages and earlier and password policy is greater than 80 characters (127 characters).

Clear the INCOMPATIBLE-SW Alarm

Procedure

Restart the CTC application.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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

Procedure

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 Procedure Guide*Connect the PC and Log into the GUI document.)

Step 2 In node view (single-shelf mode) or multishelf view (multishelf mode), click the .

Step 3 Click **Clear Security Intrusion Alarm**.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

INVALID-SYSDB

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: EQPT

An Invalid SYSDB alarm is raised when the valid system DB file is not available on the controller card.

Clear the INVALID-SYSDB Alarm

Procedure

Step 1 Soft Reboot the ACT controller card if reported on Active.

Step 2 Soft Reboot the Standby card if reported on Standby.

Step 3 If the alarm is raised on Active and Standby at the same instance, contact TAC.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

INVALID-MUXCONF

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: EQPT

The INVALID-MUXCONF alarm is raised when the 10x10G muxponder operation mode is created between an unlicensed 10x10G-LC card and a licensed 100G-LC-C card.

Clear the INVALID-MUXCONF Alarm

Procedure

Replace the unlicensed 10x10G-LC card with a licensed 10x10G-LC card.

To replace the card, complete the procedure "Physically Replace a Card, on page 394".

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

INVMACADR

Default Severity: Major (MJ), Service Affecting (SA)

Logical Objects: AIP, BP

The Invalid MAC Address alarm occurs when the system MAC address is invalid. Each system has a unique, permanently assigned MAC address. The address resides on an AIP or backplane EEPROM. BP or backplane applies to NCS 2002, NCS 2006, and NCS 2015 chassis. The control cards read the address value from the AIP or backplane chip during boot-up and keeps this value in its synchronous dynamic RAM (SDRAM).

An invalid MAC address can be caused when:

- There is a read error from the backplane EEPROM during boot-up. The TNC/TNCE/TSCE/TNCS/TNCS-O cards use the default MAC address (00:11:22:33:44:55).
- There is a read error occurring on one of the redundant control cards that read the address from the backplane; these cards read the address independently and could therefore each read different address values.

Clear the INVMACADR Alarm

Procedure

Step 1 Complete the Resetting the Controller Card procedure for TNC/TNCE/TSC/TSCE/TNCS/TNCS-O cards.

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, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

IMPROPRMVL-FS

Default Severity: Minor (MI), Non-Service-Affecting (NSA)

Logical Objects: PSHELF

The Improper Removal of Fiber Shuffle (IMPROPRMVL-FS) condition occurs when a provisioned and associated Passive Shelf is unplugged from its USB Port. It occurred due to an improper removal of the device.

The condition will clears when the Passive Shelf is plugged back in the USB port. This transient condition does not result in a standing condition.

IPC-LASER-FAIL

Default Severity: Minor (MI), Non-Service-Affecting (NSA)

Logical Objects: EQPT

The Internal Patch-cord Connection (IPC) Laser Fail alarm is raised when the laser fails to produce output power. The laser failure is detected when the laser is powered up. The laser is embedded inside 20SMR FS CV card for connection verification.

The alarm is cleared automatically when laser output power is detected during or after a power module reset.

IPC-LOOPBACK-MISS

Default Severity: Minor (MI), Non-Service-Affecting (NSA)

Logical Objects: OTS

The Internal Patchcord Connection (IPC) Loopback Miss alarm is raised when the MF-DEG-5-CV, MF-UPG-4-CV, or MF-M16LC-CV modules contain one or more than one disconnected port (port without a patchcord cord or loopback cap). These passive modules are provided with loopback cap on disconnected ports in order to pre-test all possible optical paths inside the node. The uninstalled loopback will raise the alarm.

A false IPC-LOOPBACK-MISS alarm is raised if, a fibre inside an MPO has a very high insertion loss.

Clear the IPC-LOOPBACK-MISS Alarm

Procedure

To clear the IPC-LOOPBACK-MISS alarm, do one of the below mentioned steps, as required:

a) Replace the missing loopback cap on the disconnected port.
b) Install a patchcord on the disconnected port if you cannot replace the missing loopback. Update the node IPC list .

The alarm will be cleared during the nest manual/automatic connection verification. The automatic connection verification occurs every six hours.

If the troubleshooting procedure does not clear the alarm, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html or call the Cisco Technical Assistance Center (1 800 553-2447) to report the problem.

IPC-VERIFICATION-DEGRADE

Default Severity: Minor (MI), Non-Service-Affecting (NSA)

Logical Objects: NE

The Internal Patchcord Connection (IPC) Verification Degrade condition occurs when the connection verification detects a minor problem in the internal patchcords that includes:

- A minimum of one patchcord with insertion loss more than minor degrade threshold and less than major degrade threshold
- A minimum of one patchcord is in Not Measurable state.

For more information on connection verification procedure, refer to NTP-G356 Verify Connections in Optical Cables.

The condition is cleared automatically when no minor problem is detected during the connection verification process.

IPC-VERIFICATION-FAIL

Default Severity: Major (MJ), Non-Service-Affecting (NSA)

Logical Objects: NE

The Internal Patchcord Connection (IPC) Verification Fail condition occurs when the connection verification detects a major problem in the internal patchcords that includes:

- A minimum of one patchcord is disconnected
- A minimum of one patchcord with insertion loss greater than the major degrade threshold (measured loss is greater than 3 dBm).

Note 1 dBm (degrade) and 3 dBm (fail) are the default threshold values, these are the NE default values and can be changed in the range from 0 dBm to 20 dBm.

For more information on connection verification procedure, refer to NTP-G356 Verify Connections in Optical Cables.

The condition is cleared automatically when no major problem is detected during the connection verification process.

ISIS-ADJ-FAIL

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: OCN

The Open System Interconnection (OSI) Intermediate System to Intermediate-System (IS-IS) Adjacency Failure alarm is raised by an intermediate system (node routing IS Level 1 or Level 1 and 2) when no IS or end system (ES) adjacency is established on a point-to-point subnet. The Intermediate-System Adjacency Failure alarm is not supported by ES. It is also not raised by IS for disabled routers.

The alarm is typically caused by a misconfigured router manual area adjacency (MAA) address.

Clear the ISIS-ADJ-FAIL Alarm

Procedure

Step 1 Ensure that both ends of the communication channel are using the correct Layer 2 protocol and settings (LAPD or PPP). To do this, complete the following steps:

a) At the local node, in node view, click the **Provisioning** > **Comm Channels** >**MSDCC** tabs.
b) Click the row of the circuit. Click **Edit**.
c) In the Edit MSDCC termination dialog box, view and record the following selections: Layer 2 protocol (LAPD or PPP); Mode radio button selection (AITS or UITS); Role radio button selection (Network or User); MTU value; T200 value, and T203 selections.
d) Click **Cancel**.
e) Log in to the remote node and follow the same steps, also recording the same information for this node.

Step 2 If both nodes do not use the same Layer 2 settings, you will have to delete the incorrect termination and recreate it. To delete it, click the termination and click **Delete**. To recreate it, refer to the Turn Up Node chapter in the Configuration guide for the procedure.

Step 3 If the nodes use PPP Layer 2, complete the Clear the RS-EOC Alarm, on page 335 procedure. If the alarm does not clear, go to Step 7, on page 214.

Step 4 If both nodes use the LAPD Layer 2 protocol but have different Mode settings, change the incorrect node entry by clicking the correct setting radio button in the Edit MSDCC termination dialog box and clicking **OK**.

Step 5 If the Layer 2 protocol and Mode settings are correct, ensure that one node is using the Network role and the other has the User role. If not (that is, if both have the same mode settings), correct the incorrect one by clicking the correct radio button in the Edit MSDCC termination dialog box and clicking **OK**.

Step 6 If the Layer 2, Mode, and Role settings are correct, compare the MTU settings for each node. If one is incorrect, choose the correct value in the Edit MSDCC dialog box and click **OK**.

Step 7 If all of the preceding settings are correct, ensure that OSI routers are enabled for the communications channels at both ends by completing the following steps:

a) Click **Provisioning** > **OSI** > **Routers** > **Setup**.
b) View the router entry under the **Status** column. If the status is Enabled, check the other end.
c) If the Status is Disabled, click the router entry and click **Edit**.
d) Check the **Enabled** check box and click **OK**.

Step 8 If the routers on both ends are enabled and the alarm still has not cleared, ensure that both ends of the communications channel have a common MAA by completing the following steps:

a) Click the **Provisioning** > **OSI** > **Routers** > **Setup** tabs.
b) Record the primary MAA and secondary MAAs, if configured.

Tip You can record long strings of information such as the MAA address by using the CTC export and print functions. Export it by choosing File > Export > html. Print it by choosing File > Print.

c) Log into the other node and record the primary MAA and secondary MAAs, if configured.
d) Compare this information. There should be at least one common primary or secondary MAA in order to establish an adjacency.
e) If there is no common MAA, one must be added to establish an adjacency. Refer to the Turn Up Node chapter of the Configuration guide for procedures to do this.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

IPC-VERIFICATION-RUNNING

Default Severities: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Objects: EQPT

The Internal Patchcord Connection (IPC) Verification Running alarm is raised when the patchcord verification tasks start.

Clear the IPC-VERIFICATION-RUNNING Alarm

Procedure

This alarm is cleared automatically when the patchcord verification tasks are complete.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

KEY-EX-FAIL

Default Severity: Major (MJ)

Logical Object: TRUNK (OTU)

The Key Exchange Fail (KEY-EX-FAIL) alarm is raised on the OTU trunk port of the WSE card when the source and destination WSE cards do not exchange primary keys used for encryption.

Note The KEY-EX-FAIL alarm is raised and cleared(within one minute) during provision or de-provision of Corresponding Client Payload on the 400G-XP-LC card. This is a known behaviour.

Note The KEY-EX-FAIL alarm is raised on the trunk port. However, there is no correlation with the OTN alarms that are raised on the trunk.

Note The KEY-EX-FAIL alarm is raised on the 400G-XP-LC, MR-MXP, and WSE cards when the near-end node has older release and the far-end node has R11.12 or vice versa and encryption is enabled between the nodes. However, the encrypted traffic is not affected.

This alarm may be raised during these scenarios:

- A loss of signal on a fibre that may occur during key exchange. This results in failure of primary key exchange.
- Bit errors on the line during key exchange.
- Incorrect configuration of destination IP address, destination port or both in **Provisioning** > **Encryption** > **GCC2 Settings** in CTC.
- Card authentication enabled on one end and disabled on the other end.

Clearing the KEY-EX-FAIL Alarm

Note To clear the alarm raised on the 400G-XP-LC, MR-MXP, and WSE cards due to mismatch of release between near-end and far-end nodes running encrypted traffic, upgrade the node having lower release to R11.12.

Before you begin

You must have Security user or Security super user privileges to clear the alarm.

Procedure

Step 1 Ensure that there are no alarms on the client or trunk ports. This is because a loss of synchronization in the client port may result in an AIS in the trunk port, which in turn cascades on the TLS.

Step 2 Reset the primary key from CTC:

a) In node view (single shelf mode), or shelf view (multi-shelf mode), double-click the WSE card for which you want to reset the primary key.
b) Go to **Provisioning** > **Encryption** > **Key Management**.
c) Click the **Reset Master Key** button for the port to reset the primay key.

d) Click **Apply**.

If the troubleshooting procedure does not clear the alarm, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html or call the Cisco Technical Assistance Center (1 800 553-2447) to report the problem.

KEY-WRITE-FAIL

Default Severity: Major (MJ)

Logical Object: TRUNK (OTU)

The Key Write Failure alarm is raised on the OTU trunk port in the WSE card. This alarm is raised when the programming of the key to the crypto FPGA fails.

Clearing the KEY-WRITE-FAIL Alarm

Before you begin

You must have Security user or Security super user privileges to clear the alarm.

Procedure

Step 1 In node view (single shelf mode), or shelf view (multi-shelf mode), double click the WSE card for which you want to reset the primary key.

Step 2 Go to **Provisioning** > **Encryption** > **Key Management**.

Step 3 Click the **Reset Master Key** button for the port to reset the primary key.

Step 4 Click **Apply**.

If the troubleshooting procedure does not clear the alarm, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html or call the Cisco Technical Assistance Center (1 800 553-2447) to report the problem.

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 OPT-AMP-C, and OPT-AMP-17-C 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.

Warning Invisible laser radiation may be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments. Statement 1051.

Note Only inactivate the APR function temporarily for installation or maintenance reasons. Activate APR immediately after maintenance or installation.

Note LASER-APR is an informational condition and does not require troubleshooting.

LASER-OFF-WVL-DRIFT

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Objects: OCN, TRUNK, CLIENT

The Laser shutdown due to wavelength drift condition is raised when the transmit wavelength of the ONS-XC-10G-C XFP drifts beyond the threshold limit. This causes the TX laser to shut down to avoid transmitting a wavelength that is not provisioned in the network.

Clear the LASER-OFF-WVL-DRIFT Condition

Procedure

Provision a different wavelength or replace the affected ONS-XC-10G-C XFP. Refer to the NTP-G326 Install, Provision, and Delete PPMs section in the Installing the GBIC, SFP, SFP+, and XFP Optical Modules in Cisco ONS Platforms to replace the affected XFP.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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-AMP-C when laser aging causes a degrade, but not failure, of laser transmission.

Clear the LASERBIAS-DEG Alarm

Procedure

For the alarmed card, complete the Physically Replace a Card, on page 394 procedure.

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

Note Before disconnecting any optical amplifier card fiber for troubleshooting, ensure that the optical amplifier card is unplugged.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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-AMP-C) when the laser control circuit fails or if the laser itself fails service.

Clear the LASERBIAS-FAIL Alarm

Procedure

For the alarmed card, complete the Physically Replace a Card, on page 394 procedure.

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

Note Before disconnecting any optical amplifier card fiber for troubleshooting, ensure that the optical amplifier card is unplugged.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

LASEREOL

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: OCN

The Laser Approaching End of Life alarm applies to cards. It is typically accompanied by the HI-LASERBIAS , on page 193 alarm. It is an indicator that the laser in the card must be replaced. How soon the replacement must happen depends upon the HI-LASERBIAS alarm 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, LASEREOL indicates the card must be replaced sooner.

Clear the LASEREOL Alarm

Procedure

Complete the Physically Replace a Card, on page 394 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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-AMP-C). The Peltier control provides cooling for the amplifier.

Clear the LASERTEMP-DEG Alarm

Procedure

For the alarmed card, complete the Physically Replace a Card, on page 394 procedure.

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

Note Before disconnecting any optical amplifier card fiber for troubleshooting, ensure that the optical amplifier card is unplugged.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

LICENSE-EXPIRED

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: EQPT

The License Expired (LICENSE-EXPIRED) alarm is raised when an evaluation license or a temporary license expires and there is no other valid license installed on the device.

Traffic continues to flow even after this alarm is raised. However, the traffic will stop once the CPT 50 panel, TNC card, TSC card, fabric card, or line card is resetthe licensed card or the controller card is reset, or there is a side-switch of the controller card. To prevent traffic disruption, ensure that a valid license is installed on the device.

Traffic on the base functionality is not affected when LICENSE-EXPIRED alarm is raised.

Clear the LICENSE-EXPIRED Alarm

The LIC-EXPIRED alarm clears in one of the following scenarios:

- When the user discontinues or disables the associated feature that raised the license expired alarm. After this alarm clears, the line card resumes normal operation. The line card maintains the associated license status as expired and does not raise an alarm.
- When a switchover of control card or soft reboot/hard reboot of the target line card is performed. After the reboot, the card raises an LIC-MISSING.
- When a permanent license is installed.

Procedure

Procure and install a permanent license. For more information on installing a license, see the Licensing Configuration Guide.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

LIC-EXPIRING-SHORTLY

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: EQPT

The License Expiring Shortly (LIC-EXPIRING-SHORTLY) alarm is raised when the cumulative validity period of the existing evaluation and temporary licenses is in the range of 0 to 24 hours.

An evaluation license and multiple temporary licenses can co-exist on a device and the validity period of each license can vary.

Clear the LIC-EXPIRING-SHORTLY Alarm

Procedure

Procure and install a permanent license. For more information on installing a license, see the Licensing Configuration guide.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

LIC-EXPIRING-SOON

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: EQPT

The License Expiring Soon (LIC-EXPIRING-SOON)alarm is raised when the cumulative validity period of the existing evaluation and temporary licenses is in the range of 1 to 14 days.

An evaluation license and multiple temporary licenses can co-exist on a device and the validity period of each license can vary.

Clear the LIC-EXPIRING-SOON Alarm

Procedure

Procure and install a permanent license. For more information on installing a license, see the Licensing Configuration guide.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

LIC-MISSING

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: PORT

The License Missing (LIC-MISSING) alarm is raised when a valid license on the one Gigabit Ethernet port of the CPT 50 panel licensed port expires.

Clear the LIC-MISSING Alarm

Procedure

Procure and install a valid license for the one Gigabit Ethernet port on CPT 50 panelport. For more information on installing a license, see the Licensing Configuration guide.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

LMP-FAIL

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: GE

The Link Management Protocol Fail alarm is raised by the control card when an LMP control channel fails or when there is a traffic engineering (TE) link correlation error. When the alarm is raised against a control channel, it uses a control channel (CTRLx) AID. When the alarm is raised against a TE link, a TE link AID (TLINKx) is used.

The alarm clears when the control channel or TE link is restored.

Note LMP-FAIL occurs independently of the condition hierarchy between LMP-SD, on page 225, LMP-SF, on page 226, or LMP-UNALLOC, on page 227.

Note When the LMP-FAIL alarm is reported against a control channel (CTRLx) AID, it only refers to control channel failure. It does not directly indicate data link or traffic engineering link status.

Note When the LMP-FAIL alarm is reported against a TE link AID (TLINKx), it refers only to TE link status, not to control channel or data link status.

Clear the LMP-FAIL Alarm

Procedure

Step 1 Verify the AID (CTRLx or TLINKx) of the alarm.

Step 2 If the alarm is against the control channel AID, this is caused by mismatched control channel parameters between the near-end NCS and the far-end node (which may be another vendor's equipment). Complete the following steps:

a) Determine whether both near-end and far-end sides of the control channel are in the IS administrative state:

- Click the **Provisioning** > **Comm Channels** > **LMP** > **Control Channels** tabs and view the Admin State column content for the channel.
- If the status does not say IS, change it and click **Apply**.

b) Determine whether the near-end node LMP configuration contains the far-end node's IP address as its remote node IP. Also verify that the near-end node's LMP configuration uses the LMP node ID as its own remote node ID. If one or more of these values is incorrect, enter it correctly.

c) Determine whether the far-end node LMP configuration contains the near-end node's IP address as its remote node IP. Also verify that the far-end node's LMP configuration uses the LMP node ID as its own remote node ID. If one or more of these values is incorrect, enter it correctly.

d) Verify that the far-end node is using the near-end node's IP address as its remote node IP address, and that the far end is also using the LMP node ID as its remote node ID. Update the far end's values if they are incorrect.

Step 3 If instead the alarm is raised against the TE link AID, complete the following steps:

a) Determine whether both near-end and far-end sides of the TE link are in the IS administrative state. If either end is currently down, update its administrative state to IS:

- Click the **Provisioning** > **Comm Channels** > **LMP** > **TE links** tab.
- If the status does not say IS, change it and click **Apply**.

b) Determine whether the near-end node's remote TE link ID matches the far-end node's local TE link ID. If the near-end node's remote value is incorrect, enter it correctly.

c) Determine whether the far-end node's remote TE link ID corresponds to the near-end node's local TE link ID. If the far-end node's remote value is incorrect, enter it correctly.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

LMP-SD

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: GE

The LMP Data Link Signal Degrade condition occurs for when the control card receives an LMP link summary or channel status message that the control channel is not available from the far end, so the data link level of service is not guaranteed. The degrade range is provisionable.

LMP-SD clears when the control card receives a link summary or channel status message reporting that the data link is in the Signal Okay (OK) state.

LMP-SD is part of an alarm hierarchy that includes LMP-SF, on page 226, and LMP-UNALLOC, on page 227. The hierarchy is as follows: If LMP-UNALLOC is raised, LMP-SF and LMP-SD are suppressed. If LMP-SF is raised, it suppresses LMP-SD. LMP-SF and LMP-UNALLOC both suppress near-end LOS-type alarms for DWDM clients. LMP-SD, however, does not suppress LOS alarms.

This condition clears when the far-end trouble has been cleared.

Clear the LMP-SD Condition

Procedure

Look for and clear any of the following alarms in Table 12: Transponder Trunk Alarms that Cause LMP-SD, on page 225 and Table 13: Transponder Client Alarm that Causes LMP-SD, on page 225 occurring on the far-end port.

Table 12: Transponder Trunk Alarms that Cause LMP-SD

Trunk Port Alarm	LMP Failure	Direction
SD	SD	Tx
OTUK-SD	SD	Tx
ODUK-SD-PM	SD	Tx
ODUK-SD-TCM1	SD	Tx
ODUK-SD-TCM2	SD	Tx

Table 13: Transponder Client Alarm that Causes LMP-SD

Client Port Alarm	LMP Failure	Direction
SD	SD	Rx

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

LMP-SF

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: GE

The LMP Data Link Signal Fail condition notifies the near-end user of a far-end problem (and thus is NSA for the near end). The near-end control card receives an LMP link summary or channel status message that the data link service has failed. The signal fail threshold provisionable.

LMP-SF clears when the control card receives a link summary or channel status message reporting that the data link is in the Signal Okay (OK) state.

LMP-SF is part of an alarm hierarchy that includes LMP-SD, on page 225, and LMP-UNALLOC, on page 227. The hierarchy is as follows: If LMP-UNALLOC is raised, LMP-SF and LMP-SD are suppressed. If LMP-SF is raised, it suppresses LMP-SD. LMP-SF and LMP-UNALLOC both suppress near-end LOS-type alarms for DWDM clients, but LMP-SD does not suppress LOS-type alarms.

This condition clears when the far-end trouble has been cleared.

Clear the LMP-SF Condition

Procedure

Look for and clear any of the following alarms in Table 14: Transponder Card Alarms that Cause LMP-SF, on page 226, Table 15: Transponder Trunk Alarms that Cause LMP-SF, on page 226, or Table 16: Transponder Client Alarms that Cause LMP-SF, on page 227 occurring on the far-end port.

Table 14: Transponder Card Alarms that Cause LMP-SF

Card Alarm	LMP Failure	Direction
EQPT	SF	Tx
IMPROPRMVL	SF	Tx

Table 15: Transponder Trunk Alarms that Cause LMP-SF

Trunk Port Alarm	LMP Failure	Direction
LOS	SF	Tx
OTUK-LOF	SF	Tx
OTUK-AIS	SF	Tx

Trunk Port Alarm	LMP Failure	Direction
LOM	SF	Tx
OTUK-SF	SF	Tx
ODUK-SF-PM	SF	Tx
ODUK-SF-TCM1	SF	Tx
ODUK-SF-TCM2 SF	SF	Tx
FEC-MISM	SF	Tx

Table 16: Transponder Client Alarms that Cause LMP-SF

Client Alarm	LMP Failure	Direction
LOS	SF	Rx
SIGLOSS	SF	Rx
SYNCLOSS	SF	Rx
CARLOSS	SF	Rx
LOF	SF	Rx

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

LMP-UNALLOC

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: GE

The LMP Data Link Unallocated condition is raised when the control card receives an LMP link summary or channel status message reporting that the data link as unallocated for data traffic. The condition clears when the data link is allocated and sends an LMP link summary or channel status message to this effect. If a data link has the LMP-UNALLOC alarm raised against it, this should suppress all other alarms on the client port, since the far-end node is not using the errored port. (Consequently you do not have to clear any alarms on the far-end node unused port.)

LMP-UNALLOC is part of an alarm hierarchy that includes LMP-SD, on page 225, and LMP-SF, on page 226. The hierarchy is as follows: If LMP-UNALLOC is raised, LMP-SF and LMP-SD are suppressed. If LMP-SF is raised, it suppresses LMP-SD. LMP-SF and LMP-UNALLOC both suppress near-end LOS-type DWDM client alarms, but LMP-SD does not.

In most cases, this condition is an informational notice at the near-end node that the far-end port is not being utilized. If, however, the far-end port should be allocated for traffic, log into the Technical Support Website

at http://www.cisco.com/cisco/web/support/index.html for more information or call Cisco TAC (1 800 553-2447)..

LOCAL-CERT-CHAIN-VERIFICATION-FAILED

Default Severity: Major (MJ), Non-Service-Affecting (NSA)

Logical Object: EQPT

The Local Certificate Chain Verification Failed alarm is raised when the verification of an active certificate chain in the card fails.

Clear the LOCAL-CERT-CHAIN-VERIFICATION-FAILED Alarm

Procedure

This alarm is cleared when the verification of an active certificate chain in the card is pass.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

LOCAL-CERT-ISSUED-FOR-FUTURE-DATE

Default Severity: Major (MJ), Non-Service-Affecting (NSA)

Logical Object: EQPT

The Local Certificate Issued for Further Date alarm is raised when the validity time of the active certificate chain is greater than the node time.

Clear the LOCAL-CERT-ISSUED-FOR-FUTURE-DATE Alarm

Procedure

This alarm is cleared when the validity time of the active certificate chain is less than or equal to the node time.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

LOCAL-CERT-EXPIRING-WITHIN-30-DAYS

Default Severity: Major (MJ), Non-Service-Affecting (NSA)

Logical Object: EQPT

The Local Certificate Expiring Within 30 Days alarm is raised when the validity time of the active certificate chain expires within 30 days.

Clear the LOCAL-CERT-EXPIRING-WITHIN-30-DAYS Alarm

Procedure

This alarm is cleared when the validity time of the active certificate chain expires on or after 30 days.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

LOCAL-SUDI-CERT-VERIFICATION-FAILED

Default Severity: Major (MJ), Non-Service-Affecting (NSA)

Logical Object: EQPT

The Local SUDI Certificate Verification Failed alarm is raised when the active SUDI certificate verification fails.

Clear the LOCAL-SUDI-CERT-VERIFICATION-FAILED Alarm

Procedure

This alarm is cleared when the verification of an active SUDI certificate passes.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

LOCAL-CERT-EXPIRED

Default Severity: Major (MJ), Non-Service-Affecting (NSA)

Logical Object: EQPT

The Local Certificate Expired alarm is raised when the validity of an active certificate chain expires.

Clear the LOCAL-CERT-EXPIRED Alarm

Procedure

Procure and install a the local active certificate chain.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

LOCAL-FAULT

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Objects: ETH

The LOCAL-FAULT alarm is raised on the GE_XP, GE_XPE, 10GE_XP, and 10GE_XPE card ports provisioned in 10 GE LAN PHY mode under the following conditions:

- when there is a loss of signal on the port.
- when a local fault character sequence is received in the incoming MAC stream as defined in IEEE 802.3ae, 10 GE fault signaling scheme.

The LOCAL-FAULT alarm is raised on the 40G-MXP-C, 40E-MXP-C, and 40ME-MXP-C card client ports provisioned with 10 GE or 10 GE FC payloads when a local fault character sequence is received in the incoming MAC stream as defined in IEEE 802.3ae, 10 Gigabit Ethernet fault signaling scheme.

The 40G-MXP-C, 40E-MXP-C, and 40ME-MXP-C cards pass the loss of signal and local fault errors transparently.

Clear the LOCAL-FAULT Alarm

Procedure

Verify and resolve the loss of signal on the port where the alarm is raised.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

LOCKOUT-REQ

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Objects: 2R, EQPT, ESCON, FC, GE, ISC, OTS, TRUNK

The Lockout Switch Request on Facility or Equipment condition occurs when a user initiates a lockout switch request for an OC-N port in a 1+1 facility protection group. This can be accomplished by locking traffic onto the working port with the LOCK ON command (thus locking it off the protect port), or locking 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 Condition

Procedure

Complete the Clear a Lock-On or Lockout Command, on page 390 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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

Procedure

Complete the Clear a Lock-On or Lockout Command, on page 390 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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

Procedure

Complete the Clear a Lock-On or Lockout Command, on page 390 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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 the control card 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

Procedure

Step 1 Verify that the line framing and line coding match between the BITS input and the control card :

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) In node view (single-shelf mode) or shelf view (multishelf mode), 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 control card, complete the Physically Replace a Card, on page 394 procedure for the control card.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

LOF (TRUNK)

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: TRUNK, OCN

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, TXP_MR_10E_C, TXP_MR_10E_L, MXP_2.5G_10G, ADM-10G and OTU2_XP 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.

Note In R7.01, when an LOF alarm occurs on TXP or MXP trunks, G709/SONET/SDH TCAs are suppressed. For details, see the Alarm and TCA Monitoring and Management chapter in the *Cisco ONS 15454 DWDM Reference Manual*.For details, see the Alarm and TCA Monitoring and Management document.

Clear the LOF (TRUNK) Alarm

Procedure

Step 1 Using site practices, verify fiber continuity to the port. Refer to the Network Reference chapter of the Configuration 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, in node view (single-shelf mode) or shelf view (multishelf mode), 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 (or Locked,disabled), 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 Configuration 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 Configuration guideHardware Specifications document.)

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 Step 1, on page 234 to Step 6, on page 234 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, on page 394 procedure for the reporting card.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

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.

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

Procedure

Restart the CTC sessions.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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.

Clear the LO-LASERBIAS Alarm

Procedure

Complete the Physically Replace a Card, on page 394 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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 , on page 146 alarm is raised at the near end. (Both of these alarms are described in the Alarm Troubleshooting chapter of the Troubleshooting guide. Maximum, minimum, and average laser temperatures are shown in the Current column entries in the Laser Temp rows.

Clear the LO-LASERTEMP Alarm

Procedure

Step 1 In node view (single-shelf mode) or shelf view (multishelf mode), complete the procedure for the reporting MXP or TXP card.

Step 2 If the alarm does not clear, complete the Physically Replace a Card, on page 394 procedure for the reporting MXP or TXP card.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

LOM

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: TRUNK, EQPT

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, TXP_MR_10E_C, TXP_MR_10E_L, TXPP_MR_2.5G, ADM-10G, and OTU2_XP cards when the MFAS) overhead field is errored for more than five frames and persists for more than 3 milliseconds.

Clear the LOM Alarm

Procedure

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 Configuration 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.

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 Configuration 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 Physical Card Reseating, Resetting, and Replacement, on page 392 section.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

LOP-P

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: STSMON, STSTRM

A Loss of Pointer Path alarm indicates that the SONET path pointer in the overhead has been lost. LOP occurs when valid H1/H2 pointer bytes are missing from the overhead. Receiving equipment monitors the H1/H2 pointer bytes to locate the SONET payload. An LOP-P alarm occurs when eight, nine, or ten consecutive frames do not have valid pointer values. The alarm clears when three consecutive valid pointers are received.

The LOP-P alarm can occur when the received payload does not match the provisioned payload. The alarm is caused by a circuit type mismatch on the concatenation facility. For example, if an STS-1 is sent across a circuit provisioned for STS-3c, an LOP-P alarm occurs.

For the FC_MR-4 card, an LOP-P is raised if a port is configured for a SONET signal but receives an SONET signal instead. (This information is contained in the H1 byte bits 5 and 6.)

Clear the LOP-P Alarm

Caution Always use the supplied electrostatic discharge wristband when working with a powered NCS. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Procedure

Step 1 In node view, click the **Circuits** tab and view the alarmed circuit.

Step 2 Verify the circuit size listed in the Size column. If the size is different from what is expected, such as an STS3c instead of an STS1, this causes the alarm.

Step 3 If you have been monitoring the circuit with optical test equipment, a mismatch between the provisioned circuit size and the size expected by the test set can cause this alarm. For specific procedures to use the test set equipment, consult the manufacturer. Ensure that the test set monitoring is set up for the same size as the circuit provisioning.

Refer to the manufacturer instructions for test-set use.

Step 4 If the error is not due to an incorrectly configured test set, the error is in the provisioned CTC circuit size. Complete the Delete a Circuit, on page 395 procedure.

Step 5 Recreate the circuit for the correct size. For procedures, refer to the Create Circuits and VT Tunnels chapter in the Configuration guide.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

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, TXP_MR_10E_C, TXP_MR_10E_L, MXP_2.5G_10G, OC192-XFP, ADM-10G, and OTU2_XP 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.

Clear the LO-RXPOWER Alarm

Procedure

Step 1 Check the PM of the TRUNK-RX port. Verify that received power is above the optics threshold:

a) In node view (single-shelf mode) or shelf view (multishelf mode), double-click the card to display the card view.

b) For the TRUNK-RX port, double-click the card and click the .

c) Compare the refreshed PM values with the threshold (ensuring that they are above the threshold value) by clicking the .

d) Ensure that a proper threshold has been provisioned for the receive value. (Refer to the Provision Transponder and Muxponder Cards chapter in the Configuration 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

Step 3 Determine whether a bulk attenuator is specified by the Cisco TransportPlanner design. If so, verify that the proper fixed attenuation value has been used.

Step 4

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 , on page 183 alarm, the GAIN-HFAIL , on page 184 alarm, the GAIN-LDEG , on page 185 alarm, or GAIN-LFAIL , on page 185 alarm); APC alarms (the APC-CORR-SKIPPED , on page 104 alarm or APC-OUT-OF-RANGE , on page 106 alarm), and LOS-P alarms on the Add or Drop ports belonging to the OCHNC circuit.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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, TXP_MR_10E_C, TXP_MR_10E_L, 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 NCS 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.

Clear the LOS (2R) Alarm

Procedure

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 in the Configuration guide. Refer to the SFP/XFP plug-in specifications located in the Installing the GBIC, SFP, SFP+, and XFP Optical Modules in Cisco ONS PlatformsInstalling the GBIC, SFP, SFP+, QSFP, XFP, CXP, CFP and CPAK Optical Modules in Cisco NCS Platforms document.) 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 Configuration guide, and a fiber-cleaning procedure is located in the Maintain the Node chapter of the same guide.

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 Install an SFP, SFP+, or XFP Connector, on page 51 procedure or the Physically Replace a Card, on page 394 procedure as appropriate for your purposes.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

LOS (BITS)

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: BITS

Resource Type: OCn/STMn/Port

The LOS (BITS) alarm indicates that the control card 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 NCS system. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Procedure

Step 1 Verify the wiring connection from the BITS clock pin fields on the NCS system backplane to the timing source.

Step 2 If wiring is good, verify that the BITS clock is operating properly.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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

Procedure

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 NCS 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 Configuration guide.

Step 4 Ensure that the PPM (SFP) is correctly configured for this payload:

a) In node view (single-shelf mode) or shelf view (multishelf mode), 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 Configuration guide. PPM (SFP) specifications are listed in the the Installing the GBIC, SFP, SFP+, and XFP Optical Modules in Cisco ONS PlatformsInstalling the GBIC, SFP, SFP+, QSFP, XFP, CXP, CFP and CPAK Optical Modules in Cisco NCS Platforms document.

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 (or Locked,disabled), 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 Configuration guide.

Step 8 If a valid signal exists but the alarm does not clear, replace the cable connector on the NCS system.

Step 9 Repeat Steps Step 2, on page 241 through Step 6, on page 242 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 Configuration 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, on page 394 procedure for the reporting card.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

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.

Clear the LOS (ISC) Alarm

Before you begin

Caution Always use the supplied electrostatic discharge wristband when working with a powered NCS system. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Procedure

Complete the Clear the LOS (2R) Alarm, on page 240 procedure.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

LOS (OTS)

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: OTS

The Loss of Signal for the OTS applies to the OSC-3-RX port of the OPT-BST, OPT-AMP-C, or OPT-AMP-17-C amplifier card, LINE-2-RX port of the OSCM or OSC-CSM card, and LINE-RX port of the 40-SMR1-C or 40-SMR2-C 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

Procedure

Step 1 To troubleshoot this alarm, see the steps below.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

Step 2 Isolate the span affected by the fiber cut.

a) Go to CTC network view.
b) Identify the span connection that is gray.

Step 3 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 Fix a Fiber Cut. 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 Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447) in order to report a service-affecting problem.

Step 4 If the network ALS setting on the DWDM nodes that you are troubleshooting is Auto Restart, continue with Fix a Fiber Cut; if the network ALS setting is DISABLE, go to Fix a Fiber Cut.

Step 5 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 Fix a Fiber Cut; 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 6 Repair the identified broken fiber to restore the internode link.

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

Note Before disconnecting any optical amplifier card fiber for troubleshooting, ensure that the optical amplifier card is unplugged.

LOS (TRUNK)

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: TRUNK

The Loss of Signal (LOS) for a TRUNK applies to GE-XP, 10GE-XP, TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, TXP_MR_10E_C, TXP_MR_10E_L, MXP_2.5G_10G, AR_MXP, AR_XP, AR_XPE, ADM-10G, and OTU2_XP cards.

Note The MXP_2.5G_10E card has no LOS (TRUNK) option, because G.709 cannot be disabled on the card.

The alarm is raised when the card port is not receiving input. An AIS is sent upstream.

The purpose of the LOS (TRUNK) alarm is to alert the user that no optical power is being received from the fiber. A typical fault condition signalled by the LOS (TRUNK) alarm is a fiber cut. In this case, neither the payload nor the overhead signals are being received.

Note With G.709 off, the alarm coming from the trunk is LOS (TRUNK) in accordance with SONET standards.

Note In R7.01, when an LOS (TRUNK) alarm occurs on TXP and MXP trunks, G709/SONET/SDH TCAs are suppressed.

Clear the LOS (TRUNK) Alarm

Check the PMs of the TRUNK-RX port and verify that the received power is above the optics threshold.

Procedure

Step 1 Check that a proper threshold has been provisioned. (For procedures, refer to the Provision Transponder and Muxponder Cards chapter in the Configuration 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 2

Step 3 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 4 Verify whether a bulk attenuator is specified in the Cisco TransportPlanner design. If so, verify that the proper fixed attenuation value has been used.

Step 5 If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

Step 6 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 , on page 183 alarm, the GAIN-HFAIL , on page 184 alarm, the GAIN-LDEG , on page 185 alarm or GAIN-LFAIL , on page 185 alarm); APC alarms (the APC-CORR-SKIPPED , on page 104 alarm and APC-OUT-OF-RANGE , on page 106 alarm), OR LOS-P alarms on the Add or Drop ports belonging to the OCHNC circuit.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into

http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

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-AMP-C card. 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

Procedure

Step 1 Verify fiber continuity to the port by following site practices. Refer to the Network Reference chapter of the Configuration 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-AMP-C card, .

Step 4 Verify that OSC Fail Low thresholds are correct . To identify the MP value:

a) In node view (single-shelf mode) or shelf view (multishelf mode), .

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 Configuration 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 Turn Up Node chapter of the Configuration 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 Configuration 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, on page 394 procedure for the reporting card.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

LOS-P (AOTS, OMS, OTS)

Clear the LOS-P (AOTS, OMS, OTS) Alarm

Procedure

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, on page 394 procedure and call Cisco TAC (1 800 553-2447).

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 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) In node view (single-shelf mode) or shelf view (multishelf mode), 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:

c) Display the proper Power Failure Low threshold by clicking one of the following tabs as appropriate:

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, on page 247.
- 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, on page 391 procedure for the card.

If the alarm does not clear, complete the Physically Replace a Card, on page 394 procedure and and call Cisco TAC (1 800 553-2447).

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 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 Configuration guide for a procedure to detect a fiber cut.

Step 4 Check the Internal Connections file generated by Cisco Transport Planner 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 Configuration 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 Configuration guide.

Note Unplugging the fiber can cause a traffic hit. To avoid this, perform a traffic switch if possible. Refer to the Configuration guide for detailed information.

Step 6 If the port on which the alarm is raised is connected to a remote CRS-1 or ASR 9000 series router, verify that the wavelength configured on the router interface is the same as that configured for the port. Check the router configuration by using these steps:

a) Enter the following command on the router to validate the remote node configuration.

`Router>` **show controllers dwdm** *interface id x/x/x/x*

b) Check the information displayed under Optics Status to verify the configured wavelength.

c) If the wavelength is different from that configured for the port, reset it by entering the following command on the router in global configuration mode.

`Router (config)#` **controller dwdm** *interface id x/x/x/x* **wavelength** *channel number*

Note The wavelength configured for the port can be checked in CTC card view.

Step 7 If the alarm does not clear, follow the general troubleshooting rules in the Network Reference chapter in the Configuration guide for identifying any other upstream alarm in the logical signal flow that could be the root cause of the outstanding alarm.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

LOS-P (OCH)

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: OCH

For the 32WSS-O and 40WSS-C, 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 the chapter, General Troubleshooting, on page 1 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.

Clear the LOS-P (OCH) Alarm

Procedure

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, on page 394 procedure and continue with Step 9, on page 251.

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) In node view (single-shelf mode) or shelf view (multishelf mode), 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 ADM-10G card, click **Performance** > **Optics PM** > **Current Values** tabs.
- For the 32WSS-O and 40WSS-C cards, click the **Provisioning** > **Optical Chn: Optical Connector** x > **Parameters** tabs.
- For the 40-SMR1-C and 40-SMR2-C cards, 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 ADM-10G card, click **Provisioning** > **Optics Thresholds** tabs.
- For the 32WSS-O and 40WSS-C cards, click the **Provisioning** > **Optical Chn: Optical Connector** x > **Optics Thresholds** tabs.
- For the 40-SMR1-C and 40-SMR2-C cards, 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 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, on page 250.
- 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, on page 391 procedure for the card.

If the alarm does not clear, complete the Physically Replace a Card, on page 394 procedure and continue to Step 9, on page 251.

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 Configuration guide for a procedure to detect a fiber cut.

Step 4 Check the Internal Connections file generated by Cisco TransportPlanner 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 Configuration guide.

Note If no LOS-P (OTS) alarm is present on the COM port of the 80-WXC-C card that is configured in the DMX mode and a LOS-P (OCH) alarm is raised on the wavelengths passing through the COM port, it can indicate incorrect cabling of the COM and MON ports. In this case, swap the fiber between the COM and MON ports to clear the alarm

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 ADM-10G card, click the **Provisioning** > **Line** > **Ports** tabs.
- 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, on page 251.

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 Configuration guide. To display the provisioned transmit optical power values, click the following tabs as appropriate:

- For the ADM-10G card, click **Performance** > **Optics PM** > **Current Values** tabs.

- 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:

- GE-XP
- 10GE-XP
- ADM-10G
- 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, on page 251. If the actual power value is outside the specification range, complete the Physically Replace a Card, on page 394. When the newly installed card becomes active, verify that the LOS-P (OCH) alarm clears. If it does not, continue with Step 9, on page 251.

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 Configuration guide. For more information about provisioning VOA setpoints, refer to the Network Reference chapter of the Configuration 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 Configuration guide.

Note Unplugging the fiber can cause a traffic hit. To avoid this, perform a traffic switch if possible.

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 Configuration guide to remedy the problem.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

LOS-P (TRUNK)

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: TRUNK

The Loss of Signal Payload (LOS-P) alarm for the trunk layer indicates that the incoming payload signal is absent at the input trunk port. There still may be optical power on the fiber, but the payload data is missing. This alarm applies to the following cards: TXP_MR_10G, TXP_MR_10E, MXP_2.5G_10G, TXP_MR_2.5G, TXPP_MR_2.5G, MXP_MR_2.5G, MXPP_MR_2.5G, GE-XP, 10GE-XP, ADM-10G, OTU2_XP, 40G-MXP-C, 40E-MXP-C, 40ME-MXP-C, 40E-TXP-C, 40-ME-TXP-C, and every ITU-T line card.

Note The MXP_2.5G_10E has no LOS-P (TRUNK) option, because ITU-T G.709 encapsulation on the card cannot be disabled.

Note With ITU-T G.709 encapsulation on, the alarm coming from the trunk is LOS-P (TRUNK) in accordance with the OTN standards.

Note When the near-end and far-end trunk ports of the 1.2T-XP-LC card are set at different frequencies, traffic is affected. The LOS-P alarm is raised on the trunk ports instead of the Wavelength Mismatch (WAV_UNLOCK) condition. This is hardware limitation as the WAV_UNLOCK condition is related to hardware laser failure.

Note In R7.01, when an LOS-P (TRUNK) alarm occurs on TXP and MXP trunks, G709/SONET/SDH TCAs are suppressed. For details, see the Alarm and TCA Monitoring and Management chapter in the *Cisco ONS 15454 DWDM Reference Manual*.For details, see the Alarm and TCA Monitoring and Management document.

Clear the LOS-P (TRUNK) Alarm

Procedure

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, on page 394 procedure and continue to Step 7, on page 253.

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) In node view (single-shelf mode) or shelf view (multishelf mode), 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 Configuration 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, on page 253.
   - 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, on page 391 procedure for the card.

Step 3 If the alarm does not clear, complete the Physically Replace a Card, on page 394 procedure for the reporting card and then call Cisco TAC (1 800 553-2447) .

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 Configuration guide for a procedure to detect a fiber cut.

Step 5 Check the Internal Connections file generated by Cisco TransportPlanner 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 Configuration guide.

Step 6

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 Configuration guide.

Note Unplugging the fiber can cause a traffic hit. To avoid this, perform a traffic switch if possible.

Step 8 If the alarm does not clear, follow the general troubleshooting rules stated in the Network Reference chapter of the Configuration guide to identify upstream alarms in the logical signal flow that could cause an LOS-P.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

LOS-RAMAN (OTS)

Default Severity: Critical (CR), Service-Affecting (SA)

SONET Logical Objects: OTS

The Loss of Raman signal alarm indicates that the Raman signal has not received by the RX RAMAN port on the OPT-RAMP-C, OPT-RAMP-CE, EDRA-1-xx, EDRA-2-xx, and RAMAN-CTP card.

Clear the LOS-RAMAN Condition

Procedure

Step 1 Verify no RLS alarm is raised by the card. If there is an RLS alarm, seeClear the RLS Condition for more details.

Step 2 Verify that the fiber cable is properly connected and attached to the correct port. For more information about fiber connections and terminations, refer to the Install Cards and Fiber-Optic Cables chapter in the Configuration guide.

Caution Always use the supplied electrostatic discharge wristband when working with a powered system. Plug the wristband cable into the ESD jack located lower-right edge of the shelf assembly.

Step 3 Verify the card facing to this card in the far end site. If the facing card has an RLS alarm, the problem is on that card, see Clear the RLS Condition for more details.

Step 4 If no other alarms are present that could be the source of the LOS-RAMAN condition, or if clearing an alarm did not clear the LOS-RAMAN condition, complete the Physically Replace a Card, on page 394 procedure for the reporting card.

Note When you replace a card with the identical type of card, you do not need to make any changes to the database.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

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, TXP_MR_10E_C, TXP_MR_10E_L, MXP_2.5G_10G, OC192-XFP, ADM-10G, and OTU2_XP 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.

The LO-TX-POWER alarm is raised and the traffic is dropped when TX and RX connectors of the ONS-XC-10G-C or ONS-XC-10G-96C XFP connected to the trunk port of an ADM-10G, OTU2_XP, GE_XP, GE_XPE, 10GE_XP, or 10GE_XPE card are swapped.

Clear the LO-TXPOWER Alarm

Procedure

Step 1 To clear the LO-TXPOWER alarm on the TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, TXP_MR_10E_C, TXP_MR_10E_L, MXP_2.5G_10G, OC192-XFP, ADM-10G, or OTU2_XP card, perform the following:

a) In node view (single-shelf mode) or single-shelf view (multishelf mode), display the TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, TXP_MR_10E_C, TXP_MR_10E_L, MXP_2.5G_10G, OC192-XFP, ADM-10G, or OTU2_XP card view.

b) Click the .

c) For the ADM-10G card, click the .

d) Increase the TX Power Low column value by 0.5 dBm.

e) If the card transmit power setting cannot be increased without affecting the signal, complete the Physically Replace a Card, on page 394 procedure.

Step 2 To clear the LO-TXPOWER alarm raised due to swapping of TX and RX connectors of the ONS-XC-10G-C or ONS-XC-10G-96C XFP connected to the trunk port of an ADM-10G, OTU2_XP, GE_XP, GE_XPE, 10GE_XP, or 10GE_XPE card , perform the following:

a) Reconnect the TX and RX connectors of the ONS-XC-10G-C or ONS-XC-10G-96C XFP correctly.

b) Set the trunk port to OOS,DSBLD (ANSI) or Locked,disabled (ETSI) state and then back into the IS (ANSI) or Unlocked (ETSI) state.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

LPBKCRS

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Objects: STSMON, STSTRM

The Loopback Cross-Connect condition indicates that there is a software cross-connect loopback active between an optical card and an OC-192 card. A cross-connect loopback test occurs below line speed and does not affect traffic.

Note Cross-connect loopbacks occur below line speed. They do not affect traffic.

Clear the LPBKCRS Condition

Procedure

Step 1 To remove the loopback cross-connect condition, double-click the optical card in CTC to display the card view.

Step 2 Complete the Clear an STM-N Card XC Loopback Circuit, on page 397 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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 Troubleshooting MXP, TXP, XP, or ADM-10G Circuit Paths With Loopbacks, on page 6 section.

Clear the LPBKFACILITY (ESCON) Condition

Procedure

Complete the Clear an MXP, TXP, GE-XP, 10GE-XP, and ADM-10G Card Loopback Circuit, on page 396 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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 Troubleshooting MXP, TXP, XP, or ADM-10G Circuit Paths With Loopbacks, on page 6.

Note For general information about MXP and TXP cards, refer to the Card Reference chapter in the *Cisco ONS 15454 DWDM Reference Manual*. For information about provisioning them, refer to the Provision Transponder and Muxponder Cards chapter in the *Cisco ONS 15454 DWDM Procedure Guide*.

Note For general information about MXP and TXP cards and provisioning them, refer to the Provision Transponder and Muxponder Cards chapter in the *Cisco ONS 15454 DWDM Configuration GuideCisco NCS 2000 Series Configuration Guide*.

Clear the LPBKFACILITY (FC) Condition

Procedure

Complete the Clear an MXP, TXP, GE-XP, 10GE-XP, and ADM-10G Card Loopback Circuit, on page 396 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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, TXPP_MR_2.5G, GE-XP, 10GE-XP, and ADM-10G 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 Troubleshooting MXP, TXP, XP, or ADM-10G Circuit Paths With Loopbacks, on page 6 section.

Clear the LPBKFACILITY (GE) Condition

Procedure

Complete the Clear an MXP, TXP, GE-XP, 10GE-XP, and ADM-10G Card Loopback Circuit, on page 396 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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 Troubleshooting MXP, TXP, XP, or ADM-10G Circuit Paths With Loopbacks, on page 6 section.

Clear the LPBKFACILITY (ISC) Condition

Procedure

Complete the Clear an MXP, TXP, GE-XP, 10GE-XP, and ADM-10G Card Loopback Circuit, on page 396 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

LPBKFACILITY (TRUNK)

Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)

Logical Object: TRUNK

A Loopback Facility condition on MXP, TXP, GE-XP, 10GE-XP, and ADM-10G 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 Troubleshooting MXP, TXP, XP, or ADM-10G Circuit Paths With Loopbacks, on page 6 section.

Caution CTC permits loopbacks on an in-service (IS) circuit. Loopbacks are service-affecting.

Clear the LPBKFACILITY (TRUNK) Condition

Procedure

Complete the Clear an MXP, TXP, GE-XP, 10GE-XP, and ADM-10G Card Loopback Circuit, on page 396 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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 Troubleshooting MXP, TXP, XP, or ADM-10G Circuit Paths With Loopbacks, on page 6 section.

Clear the LPBKTERMINAL (ESCON) Condition

Procedure

Complete the Clear an MXP, TXP, GE-XP, 10GE-XP, and ADM-10G Card Loopback Circuit, on page 396 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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 MXP_MR_2.5G, MXPP_MR_2.5G, TXP_MR_2.5G, TXPP_MR_2.5G, GE-XP, and 10GE-XP 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 Troubleshooting MXP, TXP, XP, or ADM-10G Circuit Paths With Loopbacks, on page 6 section.

Clear the LPBKTERMINAL (FC) Condition

Procedure

Complete the Clear an MXP, TXP, GE-XP, 10GE-XP, and ADM-10G Card Loopback Circuit, on page 396 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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 Troubleshooting MXP, TXP, XP, or ADM-10G Circuit Paths With Loopbacks, on page 6 section.

Clear the LPBKTERMINAL (GE) Condition

Procedure

Complete the Clear an MXP, TXP, GE-XP, 10GE-XP, and ADM-10G Card Loopback Circuit, on page 396 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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 Troubleshooting MXP, TXP, XP, or ADM-10G Circuit Paths With Loopbacks, on page 6 section.

Clear the LPBKTERMINAL (ISC) Condition

Procedure

Complete the Clear an MXP, TXP, GE-XP, 10GE-XP, and ADM-10G Card Loopback Circuit, on page 396 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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 Troubleshooting MXP, TXP, XP, or ADM-10G Circuit Paths With Loopbacks, on page 6 section.

Clear the LPBKTERMINAL (TRUNK) Condition

Procedure

Complete the Clear an MXP, TXP, GE-XP, 10GE-XP, and ADM-10G Card Loopback Circuit, on page 396 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

LSC-NOT-PRESENT-MIC-IN-USE

Default Severity: Major (MJ), Non-Service-Affecting (NSA)

Logical Object: EQPT

The LSC Not Present Mic In Use alarm is raised when the LSC is not present, and use LSC option is checked.

Clear the LSC-NOT-PRESENT-MIC-IN-USE Alarm

Procedure

Install LSC if use MIC or use LSC option is checked in CTC.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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 Configuration guide.

Clear the LWBATVG Alarm

Procedure

The problem is external to the NCS system. Troubleshoot the power source supplying the battery leads.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

MAN-LASER-RESTART

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Objects: OTS, AOTS

The Manual Laser Restart condition is raised when a ALS mode is set to Manual Restart or Manual Restart for test.

Clear the MAN-LASER-RESTART Condition

Procedure

Set the ALS Mode to a value different from Manual Restart or Manual Restart for test.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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

Procedure

Complete the Initiate a 1+1 Manual Switch Command, on page 387 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

MANRESET

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: EQPT

Note MANRESET is an informational condition and does not require troubleshooting.

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.

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.

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.

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.

MANUAL-REQ-SPAN (2R, ESCON, FC, GE, ISC, OCN/STMN, OTS)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Objects: 2R, ESCON, FC, GE, ISC, OCN/STMN, OTS

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.

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.

MEA (AIP)

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: AIP

If the Mismatch of Equipment Attributes (MEA) alarm is reported against the AIP, the fuse in the AIP board blew or is missing. The MEA alarm also occurs when an old AIP board with a 2-A fuse is installed in a newer ANSI 10-Gbps-compatible shelf assembly.

Clear the MEA (AIP) Alarm

Procedure

Complete the Replace the Alarm Interface Panel, on page 400 procedure.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

MEA (PPM)

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: PPM

The Missing Equipment Attributes alarm for the PPM (SFP) is raised 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 When the TNCS-2 card is replacing the TNC card pre-provisioned with OC3 payload on a chassis, the PROV-MISMATCH/MEA alarm is raised. Delete the pre-provisioning on the TNCS-2 card to proceed.

Clear the MEA (PPM) Alarm

Procedure

Step 1 To provision the PPM (SFP), you must first create it in CTC. To do this, complete the following steps:

a) In node view (single-shelf mode) or shelf view (multishelf mode), 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, on page 266.)

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 Configuration guide. For information to provision PPMs (SFPs) for the MRC-12 and OC192/STM64-XFP, refer to the Optical Cards chapter in the Configuration guide.

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 Configuration 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, on page 266 to correctly provision the port rate.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

MEA (SHELF)

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: SHELF

The MEA (Shelf) condition is raised when ANSI and ETSI shelves exist in the same node. For example, an ANSI subtended shelf is configured on an ETSI node controller or an ETSI subtended shelf is configured on an ANSI node controller.

The MEA (Shelf) condition is also raised when the original subtended shelf is disconnected and another subtended shelf of different shelf type is connected with the same shelf ID.

Clear the MEA (SHELF) Condition

Procedure

Step 1 (For the first scenario) Ensure that the shelves in the node are either ANSI only or ETSI only.

Step 2 (For the second scenario) Disconnect the newly connected subtended shelf.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

MEM-GONE

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: EQPT

The Memory Gone alarm occurs when data generated by software operations exceeds the memory capacity of the control cards. The control 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.

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 control cards. The alarm clears when additional memory becomes available. If additional memory is not made available and the memory capacity of the card is exceeded, the user interface ceases to function.

The alarm does not require user intervention.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

MFGMEM

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Objects: AICI-AEP, AICI-AIE, AIP, BPLANE, FAN, PPM, ECU, LCD, PWRM

EEPROM stores manufacturing data that a system uses to determine system compatibility and shelf inventory information.

The Manufacturing Data Memory Failure alarm occurs when:

- EEPROM fails on a card or component.
- The control card cannot read data from EEPROM.

Clear the MFGMEM Alarm

Procedure

Step 1 Soft reset the standby control card.

Step 2 When the standby control card boots up, soft reset the active control card.

Step 3 Reset the specific card on which the EEPROM has failed.

Step 4 If the reset card has not rebooted successfully, or the alarm has not cleared, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

MS-AIS

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

Logical Object: STM1E, STMN

The Multiplex Section (MS) AIS condition indicates that there is a defect in the multiplexing section layer of the SONET overhead. The multiplex section refers to the segment between two SONET devices in the circuit and is also known as a maintenance span. The multiplex section layer of the SONET overhead deals with payload transport, and its functions include multiplexing and synchronization.

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 MS-AIS Condition

Procedure

Complete the Clear the AIS Condition, on page 102 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

MS-DEG

Default Severity:Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: STM1E

The Multiplex Section Signal Degrade condition is similar to the SDBER-EXCEED-HO , on page 340 alarm, but applies only to the multiplex section overhead of the EQPT object.

Clear the MS-DEG Condition

Procedure

Complete the Clear the SDBER-EXCEED-HO Condition, on page 341 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

MS-EOC

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: STMN

The MS-DCC Termination Failure alarm occurs when the system loses its data communications channel. The DCC is nine bytes, D4 through D12, in the SONET overhead. The bytes convey information about Operation, Administration, Maintenance, and Provisioning (OAM&P). The system uses the DCC on the SONET section overhead to communicate network management information.

Clear the MS-EOC Alarm

Procedure

Complete the Clear the RS-EOC Alarm, on page 335 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

MS-EXC

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: STM1E

The Multiplex Section Signal Excessive BER condition is similar to the SDBER-EXCEED-HO , on page 340 alarm, but applies only to the multiplex section overhead of the EQPT object.

Clear the MS-EXC Condition

Procedure

Complete the Clear the SDBER-EXCEED-HO Condition, on page 341 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

MS-RFI

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

Logical Object: STM1E, STMN

The MS Remote Fault Indication (RFI) condition indicates that there is an RFI occurring at the SONET overhead multiplexing section level.

An RFI occurs when the NCS detects an RFI in the SONET overhead because of a fault in another node. Resolving the fault in the adjoining node clears the MS-RFI condition in the reporting node.

Clear the MS-RFI Condition

Procedure

Step 1 Log into the far-end node of the reporting NCS.

Step 2 Determine whether there are other alarms, especially the LOS(STM1E, STMN).

Step 3 Clear the main alarm. See the appropriate alarm section in this chapter for the procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

MT-OCHNC

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: OTS

The MT-OCHNC condition occurs when the user provisions a specific wavelength for maintenance on a WXC card from an input port (EXP1-8, ADD-RX) to the output port (COM-TX).

Clear the MT-OCHNC Condition

Procedure

Delete the provisioned wavelength that was specifically tuned for maintenance purposes on a WXC card.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

NO-SHARED-CIPHERS Alarm

Default Severity: Major (MJ), Service Affecting (SA)

Logical Object: OTS

The NO-SHARED-CIPHERS alarm is raised when the certificates with different encryption cipher or algorithm are provisioned on either the server or the client.

Clear the NO-SHARED-CIPHERS Alarm

Procedure

Verify the same encryption cipher or algorithm is provisioned on both the server and the client.

If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

NO-VALID-USB-DB

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: USB MODULE

The NO-VALID-USB-DB alarm occurs when all USB database partition validations fail.

Clearing the NO-VALID-USB_DB Alarm

The NO-VALID-USB-DB alarm clears automatically when at least one USB database partition is written and verified successfully during the USBSYNC operation.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

NON-CISCO-PPM

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: PPM

The Non-Cisco PPM Inserted condition occurs when a PPM that is plugged into a card port fails the security code check. The check fails when the PPM used is not a Cisco PPM.

Clear the NON-CISCO-PPM Condition

Procedure

Obtain the correct Cisco PPM and replace the existing PPM with the new one.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

NON-TRAF-AFFECT-SEC-UPG-REQUIRED

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

Logical Objects: EQUIPMENT

The NON-TRAF-AFFECT-SEC-UPG-REQUIRED alarm is raised when the partition of the control FPGA is not locked.

When you downgrade the WSE card from Release 11.12 to older releases such as R11.1.1.2, R11.0, R10 and so on, the NON-TRAF-AFFECT-SEC-UPG-REQUIRED alarm is raised and does not clear.

Clear the NON-TRAF-AFFECT-SEC-UPG-REQUIRED alarm

Procedure

Step 1 (For WSE card) Place the client and trunk ports in OOS-MT state.

(For WSE card) Place the client and trunk ports in OOS-DSBLD state, if both the NON-TRAF-AFFECT-SEC-UPG-REQUIRED and TRAF-AFFECT-SEC-UPG-REQUIRED alarms are raised on the card.

Step 2 (For WSE card) Perform the FPGA/firmware upgrade.

Step 3 Upgrade the FPGA image and lock the partition of the control FPGA.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

NODE-FACTORY-MODE

Default Severity: Critical (CR)

Logical Object: NE

The Node Factory Mode alarm is raised when the database is not available due to the following:

- New installation.
- Reset NE to factory defaults.
- Mode conversion from ANSI to ETSI.

Clear the NODE-FACTORY-MODE Alarm

Procedure

Reset to the default setting using 'Rebuild DB' option.

(or)

Restore the database.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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 , on page 209 alarm, because INTRUSION-PSWD occurs when a user exceeds the login failures threshold.

The NOT_AUTHENTICATED alarm is also raised, when CTC nodes in the network have R10.6 packages and earlier and password policy is less than 80 characters.

Note NOT-AUTHENTICATED is an informational alarm and is resolved when CTC successfully logs into the node.

OCHNC-BDI

Default Severities: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Objects: OTS

The Optical Channel Network Connection (OCHNC) Backward Defect Indication (BDI) alarm is raised when an OCHNC signal is interrupted along the circuit path and the system is not able to recover it.

Clear the OCHNC-BDI Alarm

Procedure

This alarm is cleared automatically when the interrupt is rectified and the signal flows properly.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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 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.

Clear the OCHNC-INC Alarm

Procedure

Step 1 To recreate the missing cross-connect, 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 SONET TL1 Reference guide. For more information about ENT-WLEN and other TL1 commands, as well as their syntax, refer to the 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 Configuration guide.

Note When you restore a database on a node, it replaces the database being used on both (ACT and SBY) the control cards as the cards synchronize this version into their active flash memory. If the active (ACT) control card is reset, the standby (SBY) control cards will therefore use the same database version from its active flash memory. In the case of a power-up, both the control cards 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).

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

OCHNC-SIP

Default Severities: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Objects: OTS

The OCHNC Startup in Progress(SIP) alarm is raised when an OCHNC is created and the optical regulation to bring up the traffic is in progress.

Clear the OCHNC-SIP Alarm

Procedure

This alarm is cleared automatically when the OCHNC is successfully created and the optical regulation is complete.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

OCHTERM-INC

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

Logical Object: OCHTERM

The Optical Termination Incomplete condition is raised against an OCH termination when there is no peer OCH termination at the other end of a span.

Clear the OCHTERM-INC Condition

Procedure

Create an OCH termination at the other end of the span. For procedures to do this, refer to the Configuration guide.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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 and ADM-10G cards 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

Procedure

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.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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 and ADM-10G cards 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

Procedure

Complete the Clear the ODUK-1-AIS-PM Condition, on page 277 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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 and ADM-10G cards 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

Procedure

Complete the Clear the Clear the ODUK-1-AIS-PM Condition, on page 277 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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 and ADM-10G cards 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

Procedure

Complete the Clear the ODUK-1-AIS-PM Condition, on page 277 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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 is raised 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. 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 ODUK-OCI-PM , on page 281.

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).

Clear the ODUK-AIS-PM Condition

Procedure

Step 1 Determine whether the 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 Troubleshooting guide.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

ODUK-BDI-PM

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

Logical Object: TRUNK

The ODUK Backward Defect Indicator (BDI) PM condition is raised 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.

Clear the ODUK-BDI-PM Condition

Procedure

Complete the Clear the OTUK-BDI Condition, on page 303 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

ODUK-LCK-PM

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

Logical Object: TRUNK

The ODUK Locked Defect (LCK) PM condition is raised 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.

Clear the ODUK-LCK-PM Condition

Procedure

Unlock the upstream node signal.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

ODUK-OCI-PM

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

Logical Object: TRUNK

The ODUK Open Connection Indication (OCI) PM condition is raised 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 , on page 280 alarm.

Clear the ODUK-OCI-PM Condition

Procedure

Verify the fiber connectivity at nodes upstream.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

ODUK-SD-PM

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: TRUNK

The ODUK Signal Degrade (SD) PM condition is raised 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.

Clear the ODUK-SD-PM Condition

Procedure

Complete the Clear the OTUK-SD Condition, on page 305 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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) is raised 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.

Clear the ODUK-SF-PM Condition

Procedure

Complete the Clear the SF (DS1, DS3) Condition procedure located in the Alarm Troubleshooting chapter of the Troubleshooting guide.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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. The condition occurs when there is a trace identifier mismatch in the data stream. ODUK-TIM-PM causes an ODUK-BDI-PM , on page 280, 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).

Clear the ODUK-TIM-PM Condition

Procedure

Complete the Clear the TIM-P Condition procedure located in the Alarm Troubleshooting chapter of the Troubleshooting guide.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

OPEN-SLOT

Default Severity: Minor (MN)

Logical Object: SHELF

The Open Slot alarm is raised when an empty slot is detected in a chassis. Empty slots in a chassis lead to thermal failures due to increased temperature of the line cards. Use passive cards such as fillers to prevent air leakage in the chassis.

Note It is recommended to use filler cards to fill in the empty slots. Blank cards are not detected by the software.

Clear the OPEN-SLOT Alarm

Procedure

Use filler cards to fill the empty slots. Blank cards are not detected by the software. For more details about the filler cards, see the Cisco NCS 2000 Series Hardware Installation Guide.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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 Configuration guide.

When the OPTNTWMIS alarm occurs, the APC-DISABLED , on page 104 alarm could also be raised.

Clear the OPTNTWMIS Alarm

Procedure

Step 1 In node view (single-shelf mode) or multishelf view (multishelf mode) 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**.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

OPWR-HDEG

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Objects: AOTS, OCH, OCH-TERM, OMS, OTS

The OPWR- HDEG alarm is raised on the 80-WXC-C ports when the optical power level exceeds the saturation limit of the OCM. The OCM saturation is caused by a power level that is outside the set power range of the OCM. The OCM power range is tuned using the LOS or OPWR-LFAIL threshold values associated with the 80-WXC-C port. The saturation level is +30dBm.

Note The OPWR-HDEG alarm may be raised on the WSS pass through ports of a ROADM configuration when the attenuation is increased at the span level.

Clear the OPWR-HDEG Alarm

Procedure

Step 1 Verify fiber continuity to the port by following site practices. Refer to the Network Reference chapter of the Configuration 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 TransportPlanner. 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 Configuration guide.) Refer to the *Cisco Transport Planner DWDM Operations Guide* and decide what value to use for modifying the power level:

a) In node view (single-shelf mode) or shelf view (multishelf mode), double-click the card to open the card view.

b) Display the optical thresholds by clicking the following tabs:

- For the OPT-BST, OPT-AMP-C, or OPT-AMP-17-C cards, click the **Provisioning** > **Opt. Ampli. Line** > **Optics Thresholds** tabs.
- For the OPT-PRE, OPT-AMP-C, or OPT-AMP-17-C cards, 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 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.
- For the 40-SMR1-C and 40-SMR2-C cards, click the **Provisioning** > **Optical Line** > **Optics Thresholds** tabs.

Step 5 If the received optical power level is within specifications, refer to the *Cisco Transport Planner DWDM Operations Guide* to determine the correct levels and check the opwrMin threshold. (These are listed in the Configuration 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, on page 249 procedure. (These specifications are listed in the Configuration 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 Configuration guide.

Note Unplugging fiber can cause a traffic hit. To avoid this, perform a traffic switch if possible. Refer to the procedures in the Protection Switching, Lock Initiation, and Clearing, on page 387 section. For more detailed protection switching information, refer to the Configuration guide.

Step 9 Repeat Steps Step 1, on page 284 to Step 8, on page 286 for any other port on the card reporting the OPWR-HDEG alarm.

Step 10 If the optical power is outside of the expected range for the 80-WXC-C card, check the power level coming from the another card port that is connected to the alarmed 80-WXC-C port and verify if a bulk attenuator was installed as provisioned by CTP.

Step 11 If the OCM power range is incorrect for the 80-WXC-C card, verify if the Channel LOS Threshold parameter associated with the failing port and wavelength was imported correctly from CTP to CTC using the NE update file and if the parameter was applied to the card ports using the Launch ANS function.

Step 12 If the alarm does not clear, look for and troubleshoot any other alarm that could identify the source of the problem.

Step 13 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 14 Complete the Physically Replace a Card, on page 394 procedure for the reporting card.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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, OPT-PRE, OPT-AMP-C, EDRA-x-xx, or OPT-AMP-17-C) AOTS port; 40-SMR1-C and 40-SMR2-C card LINE-RX port; and WXC card OCH port. This alarm is raised in the control gain mode and the control power working mode.

Clear the OPWR-HFAIL Alarm

Procedure

Step 1 In the amplifier card view, navigate to **Provisioning** → **Optical Line** → **Parameters** tab to check whether the value of the Transmit Optical Power on the adjacent site is within the limit.

Step 2 If the Transmit Optical Power is too high, check for the OSC PPM mode in network view by navigating to **Provisioning** → **WDM-ANS** → **Provisioning** tab. Validate if it is correct.

Step 3 Set the OSC PPM mode in the TNCS-O card view by navigating to **Provisioning** → **Line**→ **Ports** tab as per the requirement (LX, SX, ULH, LR2, T, FX, LX_10). Rate may vary the transmit power value from high power to low power.

Step 4 Check if the alarm clears on the other end.

Note There is no threshold value for this alarm on the card to validate and change.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

OPWR-LDEG

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Objects: AOTS, OCH, OCH-TERM, OMS, OTS

The OPWR-LDEG alarm is raised on the 80-WXC-C ports when the optical power level is lower than the saturation limit of the OCM.

Clear the OPWR-LDEG Alarm

Procedure

Complete the Clear the OPWR-HDEG Alarm, on page 284 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

OPWR-LFAIL

Default Severity: Critical (CR), Service-Affecting (SA

Logical Objects: AOTS, OCH, OCH-TERM, OMS, OTS

Clear the OPWR-LFAIL Alarm

Procedure

Complete the Clear the OPWR-HDEG Alarm, on page 284 procedure.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

OSRION

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Objects: AOTS, OTS

The Optical Safety Remote Interlock On (OSRION) condition is raised on an amplifier card when OSRI is set to ON. The condition does not correlate with the OPWR-LFAIL , on page 287 alarm, which is also reported on the same port.

Clear the OSRION Condition

Procedure

Turn the OSRI off:

a) In node view (single-shelf mode) or shelf view (multishelf mode), 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.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

OTDR-ABSOLUTE-A-EXCEEDED-RX

Default Severities: Major (MJ), Non-Service-Affecting (NSA)

Logical Object: EQPT

The Optical Time Domain Reflectometer (OTDR) Absolute Attenuation Threshold Exceeded in Rx direction alarm is raised when the attenuation event in the last scan exceeds the absolute threshold in the Rx direction.

Clear the OTDR-ABSOLUTE-A-EXCEEDED-RX Alarm

Procedure

The alarm is cleared automatically when one of the following conditions is satisfied in the last scan:

- The attenuation event causing the alarm disappears.
- The attenuation event in the last scan is below the threshold.
- The absolute check is deactivated.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

OTDR-ABSOLUTE-A-EXCEEDED-TX

Default Severities: Major (MJ), Non-Service-Affecting (NSA)

Logical Object: EQPT

The Optical Time Domain Reflectometer (OTDR) Absolute Attenuation Threshold Exceeded in Tx direction alarm is raised when the attenuation event in the last scan exceeds the absolute threshold in Tx direction.

Clear the OTDR-ABSOLUTE-A-EXCEEDED-TX Alarm

Procedure

The alarm is cleared automatically when one of the following conditions is satisfied in the last scan:

- The attenuation event causing the alarm disappears.
- The attenuation event in the last scan is below the threshold.
- The absolute threshold check is deactivated.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

OTDR-ABSOLUTE-R-EXCEEDED-RX

Default Severities: Major (MJ), Non-Service-Affecting (NSA)

Logical Object: EQPT

The Optical Time Domain Reflectometer (OTDR) Absolute Reflectance Threshold Exceeded in Rx Direction alarm is raised when the reflectance event in the last scan exceeds the absolute threshold in the Rx direction.

Clear the OTDR-ABSOLUTE-R-EXCEEDED-RX Alarm

Procedure

The alarm is cleared automatically when one of the following conditions is satisfied in the last scan:

- The reflectance event causing the alarm disappears.
- The reflectance event in the last scan is below the threshold.
- The absolute threshold check is deactivated.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

OTDR-ABSOLUTE-R-EXCEEDED-TX

Default Severities: Major(MJ), Non-Service-Affecting (NSA)

Logical Object: EQPT

The Optical Time Domain Reflectometer (OTDR) Absolute Reflectance Threshold Exceeded in Tx Direction alarm is raised when the reflectance event in the last scan exceeds the absolute threshold in the Tx direction.

Clear the OTDR-ABSOLUTE-R-EXCEEDED-TX Alarm

Procedure

The alarm is cleared automatically when one of the following conditions is satisfied in the last scan:

- The reflectance event causing the alarm disappears.
- The reflectance event in the last scan is below the threshold.
- The absolute threshold check is deactivated.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

OTDR-BASELINE-A-EXCEEDED-RX

Default Severities: Major (MJ), Non-Service-Affecting (NSA)

Logical Object: EQPT

The Optical Time Domain Reflectometer (OTDR) Baseline Attenuation Threshold Exceeded Rx alarm is raised when an existing attenuation event in the last scan or a new attenuation event exceeds the baseline threshold in the Rx direction.

Clear the OTDR-BASELINE-A-EXCEEDED-RX Alarm

Procedure

The alarm is cleared automatically when one of the following conditions is satisfied:

- The attenuation event causing the alarm disappears.
- The attenuation event is below the threshold.
- The absolute check is activated.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

OTDR-BASELINE-A-EXCEEDED-TX

Default Severities: Major (MJ), Non-Service-Affecting (NSA)

Logical Objects: EQPT

The Optical Time Domain Reflectometer (OTDR) Baseline Attenuation Threshold Exceeded Tx alarm is raised when an existing attenuation event in the last scan or a new attenuation event exceeds the baseline threshold in the Tx direction.

Clear the OTDR-BASELINE-A-EXCEEDED-TX Alarm

Procedure

The alarm is cleared automatically when one of the following conditions is satisfied:

- The attenuation event causing the alarm disappears.
- The attenuation event is below the threshold.
- The absolute check is activated.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

OTDR-BASELINE-R-EXCEEDED-RX

Default Severities: Major (MJ), Non-Service-Affecting (NSA)

Logical Objects: PPM

The Optical Time Domain Reflectometer (OTDR) Baseline Reflectance Threshold Exceeded Rx alarm is raised when an existing reflectance event in the last scan or a new reflectance event exceeds the baseline threshold in the Rx direction.

Clear the OTDR-BASELINE-R-EXCEEDED-RX Alarm

Procedure

The alarm is cleared automatically when one of the following conditions is satisfied:

- The reflectance event causing the alarm disappears.
- The reflectance event is below the threshold.
- The absolute threshold check is activated.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

OTDR-BASELINE-R-EXCEEDED-TX

Default Severities: Major (MJ), Non-Service-Affecting (NSA)

Logical Object: PPM

The Optical Time Domain Reflectometer (OTDR) Baseline Reflectance Threshold Exceeded Tx alarm is raised when an existing reflectance event in the last scan or a new reflectance event exceeds the baseline threshold in the Tx direction.

Clear the OTDR-BASELINE-R-EXCEEDED-TX Alarm

Procedure

The alarm is cleared automatically when one of the following conditions is satisfied:

- The reflectance event causing the alarm disappears.
- The reflectance event is below the threshold.
- The absolute threshold check is activated.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

OTDR-FAST-FAR-END-IN-PROGRESS

Default Severity: Minor (MN)

Logical Object: EQUIPMENT

The OTDR-FAST-FAR-END-IN-PROGRESS alarm is raised when a fast scan is started on the remote side.

Clear the OTDR-FAST-FAR-END-IN-PROGRESS Alarm

Procedure

Step 1 Wait until the scan on the remote side is completed. The time varies depending on the type of scan.

Step 2 Alternatively, stop the scan by navigating to: **Maintenance**->**DWDM**->**OTDR**; select the side where the scan is ongoing and click **Cancel**. The scan is stopped on both the sides.

If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

OTDR-FAST-SCAN-IN-PROGRESS-RX

Default Severities: Minor (MI), Non-Service-Affecting (NSA)

Logical Object: EQPT

The Optical Time Domain Reflectometer (OTDR) Fast Scan In Progress Rx alarm is raised when the fast OTDR scan starts in the Rx direction.

Clear the OTDR-FAST-SCAN-IN-PROGRESS-RX Alarm

Procedure

Step 1 This alarm is cleared automatically when the fast OTDR scan in the RX direction is complete.

Step 2 Alternatively, stop the scan by navigating to: **Maintenance**->**DWDM**->**OTDR**; select the side where the scan is ongoing and click **Cancel**. The scan is stopped on both the sides.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

OTDR-FAST-SCAN-IN-PROGRESS-TX

Default Severities: Minor (MI), Non-Service-Affecting (NSA)

Logical Object: EQPT

The Optical Time Domain Reflectometer (OTDR) Fast Scan In Progress TX alarm is raised when the fast OTDR scan starts in the TX direction.

Clear the OTDR-FAST-SCAN-IN-PROGRESS-TX Alarm

Procedure

Step 1 This alarm is cleared automatically when the fast OTDR scan in the TX direction is complete.

Step 2 Alternatively, stop the scan by navigating to: **Maintenance**->**DWDM**->**OTDR**; select the side where the scan is ongoing and click **Cancel**. The scan is stopped on both the sides.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

OTDR-FIBER-END-NOT-DETECTED-RX

Default Severity: NA

Logical Object: EQUIPMENT

The OTDR-FIBER-END-NOT-DETECTED-RX alarm is raised when the OTDR module cannot return a valid fiber end.

Clear the OTDR-FIBER-END-NOT-DETECTED-RX Alarm

Procedure

Execute the Auto Scan.

Note If the fiber is affected by high reflections or if the fiber is longer than 100 km, the fiber end cannot be found. Hence, the alarm will not be cleared.

If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

OTDR-FIBER-END-NOT-DETECTED-TX

Default Severity: NA

Logical Object: EQUIPMENT

The OTDR-FIBER-END-NOT-DETECTED-TX alarm is raised when the OTDR module cannot return a valid fiber end.

Clear the OTDR-FIBER-END-NOT-DETECTED-TX Alarm

Procedure

Execute the Auto Scan.

Note If the fiber is affected by high reflections or if the fiber is longer than 100 km, the fiber end cannot be found. Hence, the alarm will not be cleared.

If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

OTDR-HYBRID-FAR-END-IN-PROGRESS

Default Severity: NA

Logical Object: EQUIPMENT

The OTDR-HYBRID-FAR-END-IN-PROGRESS alarm is raised when a hybrid scan is started on the remote side.

Clear the OTDR-HYBRID-FAR-END-IN-PROGRESS Alarm

Procedure

Step 1 Wait until the scan on the remote side is completed.

The time varies depending on the type of scan.

Step 2 Alternatively, stop the scan by navigating to: **Maintenance->DWDM->OTDR**; select the side where the scan is ongoing and click **Cancel**. The scan is stopped on both the sides.

If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

OTDR-HYBRID-SCAN-IN-PROGRESS-RX

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Objects: PPM

The Optical Time Domain Reflectometer (OTDR) Hybrid Scan In Progress RX condition occurs when a hybrid OTDR scan starts in the RX direction.

Clear the OTDR-HYBRID-SCAN-IN-PROGRESS-RX Alarm

Procedure

Step 1 This alarm is cleared automatically when the hybrid OTDR scan in the RX direction is complete.

Step 2 Alternatively, stop the scan by navigating to: **Maintenance**->**DWDM**->**OTDR**; select the side where the scan is ongoing and click **Cancel**. The scan is stopped on both the sides.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

OTDR-HYBRID-SCAN-IN-PROGRESS-TX

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Objects: PPM

The Optical Time Domain Reflectometer (OTDR) Hybrid Scan In Progress TX condition occurs when a hybrid OTDR scan starts in the TX direction.

Clear the OTDR-HYBRID-SCAN-IN-PROGRESS-TX Alarm

Procedure

Step 1 This alarm is cleared automatically when the hybrid OTDR scan in the TX direction is complete.

Step 2 Alternatively, stop the scan by navigating to: **Maintenance**->**DWDM**->**OTDR**; select the side where the scan is ongoing and click **Cancel**. The scan is stopped on both the sides.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

OTDR-ORL-THRESHOLD-EXCEEDED-RX

Default Severity: Minor (MN)

Logical Object: EQUIPMENT

The OTDR-ORL-THRESHOLD-EXCEEDED-RX alarm is raised if the current ORL value crosses its threshold value.

Clear the OTDR-ORL-THRESHOLD-EXCEEDED-RX Alarm

Procedure

Step 1 Clean the fiber on the major reflection contribution.

Major reflection contribution can be found in the OTDR Scans.

Step 2 Alternatively, change the ORL threshold from Provisioning > WDM-ANS > OTDR > Side > Baseline Thresholds tab.

If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

OTDR-ORL-THRESHOLD-EXCEEDED-TX

Default Severity: Minor (MN),

Logical Object: EQUIPMENT

The OTDR-ORL-THRESHOLD-EXCEEDED-TX alarm is raised if the current ORL value crosses its threshold value.

Clear the OTDR-ORL-THRESHOLD-EXCEEDED-TX Alarm

Procedure

Step 1 Clean the fiber on the major reflection contribution.

Major reflection contribution can be found in the OTDR Scans.

Step 2 Alternatively, change the ORL threshold from Provisioning > WDM-ANS > OTDR > Side > Baseline Thresholds tab.

If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

OTDR-ORL-TRAINING-FAILED-RX

Default Severity: Minor (MN)

Logical Object: EQUIPMENT

The OTDR-ORL-TRAINING-FAILED-RX alarm is raised if the training phase cannot find valid calibration data.

Clear the OTDR-ORL-TRAINING-FAILED-RX Alarm

Procedure

Execute the scan in the RX direction.

Note If the scan shows high reflections, clean the connectors where the reflections are too high or change the corresponding patchcords.

If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

OTDR-ORL-TRAINING-FAILED-TX

Default Severity: Minor (MN)

Logical Object: EQUIPMENT

The OTDR-ORL-TRAINING-FAILED-TX alarm is raised if the training phase cannot find valid calibration data.

Clear the OTDR-ORL-TRAINING-FAILED-TX Alarm

Procedure

Execute the scan in the TX direction.

Note If the scan shows high reflections, clean the connectors where the reflections are too high or change the corresponding patchcords.

If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

OTDR-ORL-TRAINING-IN-PROGRESS-RX

Default Severity: NA

Logical Object: EQUIPMENT

The OTDR-ORL-TRAINING-IN-PROGRESS-RX alarm is raised if the ORL is started in the fast mode on the Rx side.

Clear the OTDR-ORL-TRAINING-IN-PROGRESS-RX Alarm

Procedure

Wait until ORL training is completed in the Rx side. ORL training takes 10 seconds.

If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

OTDR-ORL-TRAINING-IN-PROGRESS-TX

Default Severity: NA

Logical Object: EQUIPMENT

The OTDR-ORL-TRAINING-IN-PROGRESS-TX alarm is raised if the Optical Return Loss (ORL) is started in the fast mode on the Tx side.

Clear the OTDR-ORL-TRAINING-IN-PROGRESS-TX Alarm

Procedure

Wait until ORL training is completed in the Tx side. ORL training takes 10 seconds.

If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

OTDR-OTDR-TRAINING-FAILED-RX

Default Severity: NA

Logical Object: EQUIPMENT

The OTDR-OTDR-TRAINING-FAILED-RX alarm is raised if the training phase cannot find valid calibration data.

Clear the OTDR-OTDR-TRAINING-FAILED-RX Alarm

Procedure

Execute the training scan in the RX direction.

Note If the scan shows high reflections, clean the connectors where the reflections are too high or change the corresponding patchcords.

If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

OTDR-OTDR-TRAINING-FAILED-TX

Default Severity: NA

Logical Object: EQUIPMENT

The OTDR-OTDR-TRAINING-FAILED-TX alarm is raised if the training phase cannot find valid calibration data.

Clear the OTDR-OTDR-TRAINING-FAILED-TX Alarm

Procedure

Execute the training scan in the TX direction.

Note If the scan shows high reflections, clean the connectors where the reflections are too high or change the corresponding patchcords.

If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

OTDR-SCAN-FAILED

Default Severities: Major (MJ), Non-Service-Affecting (NSA)

Logical Object: EQPT

The Optical Time Domain Reflectometer (OTDR) scan failed alarm is raised when the OTDR scan fails and no result is sent to the user.

Clear the OTDR-SCAN-FAILED Alarm

Procedure

This alarm is automatically cleared when no failed scan remains on for all sectors of the target PPM.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

OTDR-SCAN-IN-PROGRESS

Default Severity: Minor (MI), Non-Service-Affecting (NSA)

Logical Objects: PPM

The Optical Time Domain Reflectometer (OTDR) Scan In Progress condition occurs under one of the following conditions:

A scan is initiated on a node which is running a release that does not support new scan initiated alarms (reporting, scan type, and direction) and full duplex scan (scan started on both nodes).

If communication between the two nodes is available, then the alarm is also raised on remote node (even if the node is running a newer release, supporting new OTDR scan in progress alarms).

The condition is cleared automatically when the OTDR scan is completed (either successfully or by timeout/error). When the scan successfully completes, a graph is obtained in the user interface and OSC links gets re-established. This transient condition does not result in a standing condition.

OTDR-SCAN-NOT-COMPLETED

Default Severity: Minor (MN)

Logical Object: EQUIPMENT

The OTDR-SCAN-NOT-COMPLETED alarm is raised when the scan has not been executed on the span in the TX direction.

Clear the OTDR-SCAN-NOT-COMPLETED Alarm

Procedure

Step 1 Execute a manual OTDR scan over the port or direction where the alarm has been raised.

Step 2 Alternatively, stop the scan by navigating to: **Maintenance**->**DWDM**->**OTDR**; select the side where the scan is ongoing and click **Cancel**. The scan is stopped on both the sides.

If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

OTUK-AIS

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

Logical Object: TRUNK

The Optical Transport Unit (OTUK) AIS condition applies 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).

Clear the OTUK-AIS Condition

Procedure

Complete the Clear the AIS Condition, on page 102 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

OTUK-BDI

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

Logical Object: TRUNK

The Section Monitoring Backward Defect Indication (OTUK-BDI) condition 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.

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).

Clear the OTUK-BDI Condition

Procedure

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.

Step 2 At the far-end node, determine whether an OTUK-AIS , on page 302 condition, 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 , on page 304 condition or OTUK-SD , on page 305 condition 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.)

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

OTUK-IAE

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: TRUNK

The OTUK Section-Monitoring Incoming Alignment Error (IAE) alarm occurs 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 , on page 304 alarm.

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.

Clear the OTUK-IAE Alarm

Procedure

Step 1 At the near-end 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.

Step 2 If the OTUK-IAE alarm does not clear, look for other OTU-related alarm, such as the OTUK-LOF , on page 304 alarm, 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.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

OTUK-LOF

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: TRUNK

The Optical Transport Unit Loss of Frame (OTUK-LOF) alarm applies when ITU-T G.709 encapsulation is enabled for the cards. The ITU-T G.709 encapsulation refers to a digital data wrapper that is transparent across networking standards such as SONET, Ethernet or IP protocols. 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.

The OTUK-LOF alarm is raised under one of the following conditions:

- FEC settings on the trunk ports of the source and destination cards are different.
- Wavelength received on the trunk port and the wavelength configured on the trunk port is different.

Clear the OTUK-LOF Alarm

Procedure

Step 1 Verify cabling continuity to the port reporting the alarm.

Caution Always use the supplied electrostatic discharge wristband when working with a powered NCS 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.

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 the 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.)

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

OTUK-SD

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: TRUNK

The OTUK-SD condition applies 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 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).

Clear the OTUK-SD Condition

Procedure

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 Configuration 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 Configuration 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 Physical Card Reseating, Resetting, and Replacement, on page 392 section.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

OTUK-SF

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: TRUNK

The OTUK-SF condition applies 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 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).

Clear the OTUK-SF Condition

Procedure

Complete the Clear the OTUK-SD Condition, on page 305 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

OTUK-TIM

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: TRUNK

The OTUK-TIM alarm applies 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 , on page 302 alarm.

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).

When the trace mode is set to manual at the section and path level and the OTUk-TTI string is 64 bytes, the OTUK-TIM alarm is triggered. This error condition occurs when the OTUk-TTI string is configured along with ODUk-TTI string and the OTUk-TTI string is 64 Bytes. If the OTUk-TTI string is 63 bytes or if you configure all the 64 bytes of the OTUk-TTI string without configuring the ODUk TTI string, the alarm is not triggered.

For the above error condition, you can restrict the length of the provisioned OTUk-TIM messages to 32 bytes, or disable manual insertion of TTI in the ODUk layer if you want to configure all the 64 bytes.

Clear the OTUK-TIM Condition

Procedure

Complete the Clear the TIM Alarm, on page 363 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

OUT-OF-BUNDLE

Default Severity:

- On GE physical ports: Minor (MN), Non-Service-Affecting (NSA)
- On Channel Group port: Major (MJ), Service-Affecting (SA)

Logical Objects: ETH, CHGRP

The Out Of Bundle (OUT-OF-BUNDLE) condition occurs on GE_XP and 10GE_XP cards when the physical port is placed outside the channel group bundle. It can also be raised on a channel group when all the members of the bundle are placed outside the channel group bundle.

Clear the OUT-OF-BUNDLE Condition

Procedure

Step 1 Make sure that the ports' expected speed and duplex settings are same as that of the channel group.

Step 2 LACP mode configured between the peer ports must be valid. For example, you cannot have a passive-passive combination.

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, TXPP_MR_2.5, GE-XP, 10GE-XP, and ADM-10G cards when the PPM (SFP) port is not correctly configured for the Gigabit Ethernet payload rate.

Clear the OUT-OF-SYNC Condition

Procedure

Step 1 In node view (single-shelf mode) or shelf view (multishelf mode), 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 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**.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

OVER-TEMP-UNIT-PROT

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: EQPT

The OVER_TEMP-UNIT-PROT alarm applies to the 100G-LC-C card. The alarm occurs when the temperature of any one of the internal measurement points exceeds its predefined threshold. The alarm is raised because of one of these reasons:

- An improper rack installation
- Abnormally high environmental temperature
- An unclean air filter
- A hardware failure of the card

When the card raises this alarm, the TX output power is shut down. This mechanism prevents the card from damage.

Clearing the OVER-TEMP-UNIT-PROT Alarm

Procedure

Step 1 Verify that the rack is installed properly. For proper airflow and cooling of the shelf, the shape of the vertical posts of the rack should be such that the airflow vents are not covered. For more information about the installation, refer to the *Hardware Installation Guide*.

Step 2 If the rack installation is proper, verify that the environmental temperature of the room is not abnormally high.

Step 3 If the room temperature is not abnormally high, ensure that nothing prevents the fan-tray assembly from passing air through the NCS system shelf.

Step 4 If airflow is not blocked, determine whether the air filter needs replacement. Refer to the Inspect, Clean, and Replace the Air Filter, on page 397 procedure.

Step 5 If the air filter is clean, complete the Remove and Reinsert (Reseat) Any Card , on page 393 procedure.

Step 6 If the alarm fails to get cleared, complete the Physically Replace a Card, on page 394 procedure.

Note When you replace a card with an identical card, you do not need to make any changes to the database.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

PARAM-MISM

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Objects: AOTS, OCH, OCH-TERM, OMS, OTS

The PARAM-MISM condition is raised on the OPT-EDFA-17 card, when an invalid Gain setpoint is provisioned by the control card.

The Gain setpoint for the OPT-EDFA-17 card is automatically calculated by the control card when the amplifier is turned up. The Gain Degrade Low threshold value is always 2 dB lower than the Gain setpoint value.

The APC-OUT-OF-RANGE alarm is raised on the OPT-EDFA-17 card when the Gain setpoint value that was calculated by the control card sets the Gain Degrade Low threshold to a value that is lower than the minimum setpoint value. The APC-OUT-OF-RANGE alarm triggers the PARAM-MISM alarm. This is because the Gain setpoint or the Gain Degrade Low Threshold value is outside the Gain setpoint range of the OPT-EDFA-17 card.

PATCH-ACTIVATION-FAILED

Default Severity: Critical (CR), Non-Service-Affecting (NSA)

Logical Object: EQPT

The Patch-Activation-Failed alarm is raised when the patch fails to activate. The alarm is cleared when the patch is disabled or when a different patch is activated.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

PATCH-DOWNLOAD-FAILED

Default Severity: Critical (CR), Non-Service-Affecting (NSA)

Logical Object: NE

The Patch-Download-Failed alarm is raised when the patch fails to download. The patch might not download under the following conditions:

- Wrong patch header
- Communication failure between the user interface and the node controller or standalone shelf. In multishelf setup, communication failure between the node controller and the subtended shelf controller.

The alarm is cleared when the patch is downloaded successfully.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

PAYLOAD-UNKNOWN

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: PPM

The AR_MXP and AR_XP cards support auto-sensing of client payloads. The PAYLOAD-UNKNOWN alarm occurs when the port is unable to detect a valid signal.

Clear the PAYLOAD-UNKNOWN Alarm

Procedure

Clear the PAYLOAD-UNKNOWN alarm with either of these procedures:

a) Ensure that a valid payload signal is received by the port. The alarm clears after detecting a valid signal.

b) Disable the auto-sense option:

1. Login to CTC.
2. In node view (single-shelf mode) or shelf view (multishelf view), double-click the AR_MXP or AR_XP card where you want to disable auto-sensing.
3. Click the **Provisioning** > **Line** > **Auto Ports** tabs.
4. Uncheck the **Auto Sensing** check box.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

PDI-P

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: STSMON, STSTRM

PDI-P is a set of application-specific codes indicating a signal label mismatch failure (SLMF) in the NCS STS path overhead. The condition indicates to downstream equipment that there is a defect in one or more of the directly mapped payloads contained in that STS synchronous payload envelope (SPE). For example, the mismatch could occur in the overhead to the path selector in a downstream node configured as part of a path protection. The PDI-P codes appear in the STS Signal Label (C2 byte).

An SLMF often occurs when the payload (for example, ATM) does not match what the signal label is reporting. The AIS , on page 101 condition often accompanies a PDI-P condition. If the PDI-P is the only condition reported with the AIS, clearing PDI-P clears the AIS. PDI-P can also occur during an upgrade, but usually clears itself and is not a valid condition.

A PDI-P condition reported on an OC-N port supporting a G1000-4 card circuit could result from the end-to-end Ethernet link integrity feature of the G1000-4 card. If the link integrity is the cause of the path defect, it is typically accompanied by the TPTFAIL (G1000) or the CARLOSS (G1000) reported against one or both Ethernet ports terminating the circuit. If this is the case, clear the TPTFAIL and CARLOSS alarms to resolve the PDI-P condition.

A PDI-P condition reported on an OC-N port supporting an ML-Series card circuit could result from the end-to-end Ethernet link integrity feature of the ML-Series card. If the link integrity is the cause, it is typically accompanied by the TPTFAIL (ML100T, ML1000, MLFX) reported against one or both POS ports terminating the circuit. If TPTFAIL is reported against one or both of the POS ports, troubleshooting the accompanying alarm clears the PDI-P condition. Refer to the SDH Ethernet Card Software Feature and Configuration Guide for more information about ML-Series cards.

Warning **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 For more information about Ethernet cards, refer to the SDH Ethernet Card Software Feature and Configuration Guide.

Clear the PDI-P Condition

Procedure

Step 1 Verify that all circuits terminating in the reporting card are DISCOVERED:

a) Click the **Circuits** tab.
b) Verify that the **Status** column lists the circuit as active.
c) If the Status column lists the circuit as PARTIAL, wait 10 minutes for the NCS to initialize fully. If the PARTIAL status does not change after full initialization, call Cisco TAC (1 800 553-247).

Step 2 After determining that the circuit is DISCOVERED, ensure that the signal source to the card reporting the alarm is working.

Caution Always use the supplied electrostatic discharge wristband when working with a powered NCS. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 3 If traffic is affected, complete the Delete a Circuit, on page 395 procedure.

Caution Deleting a circuit can affect existing traffic.

Step 4 Recreate the circuit with the correct circuit size. Refer to the Create Circuits and VT Tunnels chapter in the Configuration guide for detailed procedures to create circuits.

Step 5 If circuit deletion and re-creation does not clear the condition, verify that there is no problem stemming from the far-end OC-N card providing STS payload to the reporting card.

Step 6 If the condition does not clear, confirm the cross-connect between the OC-N card and the reporting card.

Step 7 If the condition does not clear, clean the far-end optical fiber according to site practice. If no site practice exists, complete the procedure in the Maintain the Node chapter of the Configuration guide.

Step 8 If the condition does not clear, complete the Physically Replace a Card, on page 394 procedure for the optical/electrical cards.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

PEER-CERT-VERIFICATION-FAILED

Default Severity: Major (MJ), Non-Service-Affecting (NSA)

Logical Object: OTN

The Peer Certificate Verification Failed alarm is raised when the verification of a peer certificate in the card fails.

Clear the PEER-CERT-VERIFICATION-FAILED Alarm

Procedure

This alarm is cleared when the verification of a peer certificate in the card is successful.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

PEER-CSF

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: STM/OCN

The Peer Client Signal Fail alarm that is a secondary alarm raised on local OCN, OTU1, or SDI_3G_VIDEO ports when a remote Service-Affecting (SA) alarm causes an invalid data transmission. The alarm is raised locally on AR_MXP and AR_XP ports and does not indicate that a Service-Affecting (SA) failure has occured at the local site. Instead it indicates that an alarm such as LOS, LOS-P, LOF, OTU-AIS is caused by an event affecting the transmission capability of the remote port.

Clear the PEER-CSF Alarm

Procedure

Clear the Service-Affecting (SA) alarm at the remote data port.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

PEER-NORESPONSE

Default Severity: Major (MJ), Service-Affecting (SA)

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

Procedure

Step 1 Complete the Reset a Card in CTC, on page 391 procedure 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.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

PMD-DEG

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: Trunk port (dir RX)

The PMD Degrade alarm is raised when the device experiences PMD in excess of 11ps for 40ME-MXP-C and 40-ME-TXP-C cards, 30ps for 40E-MXP-C and 40E-TXP-C cards, and 180ps for 100G-LC-C card.

Clear the PMD-DEG Alarm

Procedure

Switch the traffic on a lower PMD link.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

PMI

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical objects: OCH, OMS, OTS

The Payload Missing Indication (PMI) condition is part of MSTP network-level alarm correlation. It is raised at the far end when OTS or OMS optical payload is missing due to an LOS, LOS-P, or OPWR-LFAIL alarm root cause. A single PMI condition is sent when each channel on the aggregated port is lost.

An LOS, LOS-P, or OPWR-LFAIL alarm on an MSTP circuit causes multiple alarms for each channel. The correlation simplifies troubleshooting by reporting a single alarm for multiple alarms having one root cause, then demoting the root alarms so that they are only visible in the Conditions window (with Not Reported [NR] severity.)

PMI clears when the optical channel is working on the aggregated or single-channel optical port.

Note Network-level alarm correlation is only supported for MSTP communication alarms. It is not supported for equipment alarms.

Clear the PMI Condition

Procedure

Clear the root-cause service-affecting alarm by using one of the following procedures, as appropriate:

- Clear the LOS (OTS) Alarm, on page 243 procedure
- Clear the LOS (TRUNK) Alarm, on page 245 procedure
- Clear the LOS-P (OCH) Alarm, on page 249 procedure
- Clear the LOS-P (AOTS, OMS, OTS) Alarm, on page 247 procedure
- Clear the LOS-P (TRUNK) Alarm, on page 252 procedure

- Clear the OPWR-LFAIL Alarm, on page 287 procedure

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

PORT-COMM-FAIL

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: DWDM_CLIENT, DWDM_TRUNK

The port module communication failure (PORT-COMM-FAIL) alarm is raised on the OTU2XP, GE_XP, GE_XPE, 10GE_XP, 10GE_XPE, 40G-MXP-C, 40E-MXP-C, 40ME-MXP-C, AR-MXP, and AR-XP line cards when there is a pluggable port module (PPM) communication failure. The PPM communication failure is caused due to physical damage or internal errors on the PPM.

Clear the PORT-COMM-FAIL Alarm

Procedure

To Clear the PORT-COMM-FAIL alarm, perform the following:

a) Soft reset the line card.
b) Delete PPM provisioning from the line card.
c) Re-provision the PPM on the line card.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

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, OPT-AMP-C, or OPT-AMP-17-C port gain higher than 20 dBm (the maximum setpoint) or its attenuation on Express VOA lower than 0 dBm (the minimum setpoint).

Clear the PORT-FAIL Alarm

Procedure

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 Configuration 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 Configuration 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 Configuration guide. If the alarm does not clear, go to Step 4, on page 317.

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

Note Before disconnecting any optical amplifier card fiber for troubleshooting, ensure that the optical amplifier card is unplugged.

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.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

PPR-BDI

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Objects: TRUNK

The Path Protection Regen -Backward Defect Indication (PPR-BDI) alarm occurs in OTU2_XP cards when the card is used as a regenerator in standard regen or enhanced FEC modes and Proactive Protection Regen is enabled. The alarm occurs when the downstream router triggers a PF-BDI signal.

Clear the PPR-BDI Condition

Procedure

To clear the PPR-BDI condition, clear the PPR-FDI and PPR-TRIG-EXCD alarm on the OTU2_XP card.

If the problem does not clear, see to the CRS documentation for more information.

PPR-FDI

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Objects: TRUNK

The Path Protection Regen-Forward Defect Indication (PPR-FDI) occurs in OTU2_XP cards as soon as the Bit Error Rate (BER) of the optical signal between the upstream router and the NCS node exceeds the trigger threshold value for the duration set as the trigger window. The PPR-FDI alarm is sent to the downstream router which in turn triggers the switch over to the backup path.

Clear the PPR-FDI Condition

Procedure

To clear the PPR-FDI condition, clear the PPR-TRIG-EXCD alarm on the upstream OTU2XP card.

PPR-MAINT

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Objects: TRUNK

The Path Protection Regen-Maintenance signal (PPR-MAINT) alarm occurs in OTU2_XP cards when the used as a regenerator (standard regen or enhanced FEC) and proactive protection regen is enabled. The alarm occurs when the port receives a maintenance signal from a router (CRS) interface.

PPR-TRIG-EXCD

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Objects: ETH

The Path Protection Regen-Trigger Crossed (PPR-TRIG-EXCD) alarm applies to OTU2_XP cards when the card is used as a regenerator in standard regen or enhanced FEC modes and Proactive Protection Regen is enabled. The alarm occurs when the pre-FEC BER of the incoming optical signal exceeds the trigger threshold value.

Clear the PPR-TRIG-EXCD Condition

Procedure

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 Configuration guide.

Step 2 If the BER threshold is correct and at the expected level, use an optical power meter 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 Configuration 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 according to site practice to avoid a signal degrade.

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 “Physical Card Reseating, Resetting, and Replacement” section .

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

PRBS-ENABLED

Default Severities: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Objects: OCH

The Pseudo−Random Bit Sequence (PRBS) Enable alarm is raised when the PRBS is enabled on an interface.

Clear the PRBS-ENABLED Alarm

Procedure

This alarm is cleared automatically when the PRBS is disabled on an interface.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

PROT-SOFT-VERIF-FAIL

On the active control card, the alarm severity is Major (MJ) and Service Affecting (SA).

On the standby control card, the alarm severity is Minor (MN) and Non-Service affecting (NSA).

Logical Object: EQPT

The Protect Volume Software Signature Verification Failed (PROT-SOFT-VERIF-FAIL) alarm occurs under the following conditions:

- The software present on the protect volume of control card is tampered with or the software present on the system did not originate from Cisco.
- Problem present in the software is stored in the protect volume of the control card.

Clear the PROT-SOFT-VERIF-FAIL Alarm

Procedure

To clear the PROT-SOFT-VERIF-FAIL alarm, download the software on the standby partition or the standby code volume on the protect flash.

If the troubleshooting procedure does not clear the alarm, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html or call the Cisco Technical Assistance Center (1 800 553-2447) to report the problem.

PROTNA

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: EQPT

The Protection Unit Not Available (PROTNA) alarm is raised when a standby control card is not available.

Clear the PROTNA Alarm

Procedure

Ensure that the standby control card is installed and provisioned in the chassis.

PROV-MISMATCH

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: EQPT and control cards

The Provisioning Mismatch alarm is raised against a PPM connector under one of the following circumstances:

- The physical PPM range or wavelength does not match the provisioned value. PPMs have static wavelength values which must match the wavelengths provisioned for the card in the case of non-DWDM PPMs.
- The PPM reach (loss) value does not meet the reach value needed for the card.
- The reach of the inserted PPM does not match the physical PPM.

The Provisioning Mismatch (PROV-MISMATCH) alarm is raised against a TNC/TNCS/TNCE/TNCS-O card under one of the following circumstances:

- The card mode is set to TNC (default value) with OC3/GE ports provisioned and a TNCS-O card is plugged.
- The card mode is set to TNCO and the plugged card is a TNC/TNCE/TNCS.

The Provisioning Mismatch (PROV-MISMATCH) alarm is raised when a TNCS-O card is replaced by TNCS card. The alarm is also raised when TNCS card is replaced by a TNCS-O card with OC3/GE ports provisioned.

Note When the TNCS-2 card is replacing the TNC card pre-provisioned with OC3 payload on a chassis, the PROV-MISMATCH/MEA alarm is raised. Delete the pre-provisioning on the TNCS-2 card to proceed.

Clear the PROV-MISMATCH Alarm

To clear the alarm when the physical PPM range or wavelength does not match the provisioned value, perform the following steps:

Procedure

Step 1 To clear the PROV-MISMATCH alarm on MXP_2.5G_10E, MXP_2.5G_10E_C, MXP_2.5G_10E_L, MXP_2.5G_10G, MXP_MR_2.5G, MXPP_MR_2.5G, TXP_MR_2.5G, TXP_MR_10E, TXP_MR_10E_C, TXP_MR_10E_L, TXPP_MR_2.5G, GE_XP, 10GE_XP, ADM-10G, OTU2_XP, MR-MXP, WSE, 10x10G-LC, 100G-LC-C, 100G-CK-LC, 200G-CK-LC, 100GS-CK-LC, 400G-XP, CFP-LC, AR-XP, AR-MXP, AR-XPE, 40G-MXP, 40G-TXP, 40E-MXP, and 40E-TXP cards, perform the following steps:

a) Determine what the PPM wavelength range should be by viewing the frequency provisioned for the card:

i. In node view (single-shelf mode) or shelf view (multishelf mode), double-click the card to open the card view.

ii. Click the **Maintenance** > **Info** tabs.

iii. Record the value shown in the Value column.

b) Remove the incorrect PPM connector:

i. Unplug the PPM connector and fiber from the reporting card.

ii. If the PPM connector has a latch securing the fiber cable, pull the latch upward to release the cable.

iii. Pull the fiber cable straight out of the connector.

c) Replace the unit with the correct PPM connector:

i. Plug the fiber into a Cisco-supported PPM connector. For more information about supported PPMs, refer to the Installing the GBIC, SFP, SFP+, and XFP Optical Modules in Cisco ONS PlatformsInstalling the GBIC, SFP, SFP+, QSFP, XFP, CXP, CFP and CPAK Optical Modules in Cisco NCS Platforms document.

ii. If the new PPM connector has a latch, close the latch over the cable to secure it.

iii. Plug the cabled PPM connector into the card port until it clicks.

Step 2 To clear the PROV-MISMATCH alarm on GE_XP or 10GE_XP cards, remove Double Add and Translate Add selective modes, CVLAN Ingress CoS, or MAC address learning on SVLAN configuration.

Step 3 To clear the PROV-MISMATCH alarm on TNC/TNCS/TNCE/TNCS-O cards, do the steps that follow:

a) To clear the alarm when the card mode is TNC with OC3/GE ports provisioned and the plugged card is a TNCS-O, do the steps that follow:

1. Login to CTC.
2. In node view (single-shelf mode) or shelf view (multishelf view), double-click the TNCS-O card where you want to clear the alarm.
3. Delete the provisioned OC3/GE ports.
4. Click the **Provisioning** > **Card** > tabs.
5. Set Mode to TNCS-O.
6. Click **Apply**.

b) To clear the alarm when the card mode is TNCO and the plugged card is a TNC/TNCS/TNCE, do the steps that follow:

1. Login to CTC.
2. In node view (single-shelf mode) or shelf view (multishelf view), double-click the TNC/TNCS/TNCE card where you want to clear the alarm.
3. Open TNC/TNCS/TNCE card panel view.
4. Click the **Provisioning** > **Card** > tabs.
5. Set Mode to TNC.
6. Click **Apply**.

Step 4 To clear the PROV-MISMATCH alarm on TNCS card (the alarm that occurs when you replace a TNCS-O card with a TNCS card), do the steps that follow:

a) Remove the TNCS-O card.

b) Delete the TNCS-O card, refer to DLP-G351 Deleting a Card in CTC .

c) Insert the TNCS card.

Step 5 To clear the PROV-MISMATCH alarm on TNCS-O card (the alarm that occurs when you replace a TNCS card with a TNCS-O card), do the steps that follow:

a) Remove the TNCS card.
b) Delete the TNCS card, refer to DLP-G351 Deleting a Card in CTC .
c) Insert the TNCS-O card.

Note On MR-MXP and 400G-XP-LC cards, when the reach distance of one of the QSFP 10G lanes or ports is configured to **Autoprovision** or the correct reach, the PROV-MISMATCH alarm clears on the QSFP port. The alarm clears irrespective of the reach distances configured on the remaining QSFP 10G lanes or ports.

If the troubleshooting procedure does not clear the alarm, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html or call the Cisco Technical Assistance Center (1 800 553-2447) to report the problem.

PTIM

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: TRUNK, EQPT

The Payload Type Identifier Mismatch (PTIM) alarm occurs when there is a mismatch between the way the ITU-T G.709 encapsulation option is configured on the line card at each end of the optical span.

Clear the PTIM Alarm

Procedure

Step 1 In node view (single-shelf mode) or shelf view (multishelf mode), double-click the alarmed line 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**.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

PWR-CON-LMT

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: EQPT

The Power Consumption Limit Has Crossed (PWR-CON-LMT) condition is raised at the shelf level when the total power consumption of the shelf equals or exceeds the maximum power. This alarm is applicable for all the following AC and DC power supply modules.

- NCS2006-DC20
- NCS2006-AC
- NCS2006-DC
- NCS2006-DC40
- 15454-M6-DC20
- 15454-M6-AC2
- 15454-M6-AC
- 15454-M6-DC
- 15454-M6-DC40

Clear the PWR-CON-LMT Alarm

Procedure

Step 1 Remove the card that caused the alarm from the shelf.

Step 2 Remove the card provisioning through the user interface.

Step 3 Place the card in another chassis which supports the required power.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

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.

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

Procedure

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, 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 Protection Switching, Lock Initiation, and Clearing, on page 387 section for commonly used traffic-switching procedures.

Step 2 If the alarm does not clear, complete the Remove and Reinsert (Reseat) Any Card , on page 393 procedure.

Step 3 If the alarm does not clear, complete the Physically Replace a Card, on page 394 procedure 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 Configuration guide for procedures.

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.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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.

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

Procedure

Complete the Clear the PWR-FAIL-A Alarm, on page 325 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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.

Clear the PWR-FAIL-RET-A Alarm

Procedure

Complete the Clear the PWR-FAIL-A Alarm, on page 325 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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 the control card.

Clear the PWR-FAIL-RET-B Alarm

Procedure

Complete the Clear the PWR-FAIL-A Alarm, on page 325 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

PWR-PROT-ON

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Objects: OTS

The Raman Power Protection On alarm occurs when the Raman amplifier is used on fiber span that is too short for Raman power.

Clear the PWR-PROT-ON Alarm

Procedure

Step 1 To clear the alarm, check if the Raman amplifier is connected to the wrong span. If it is, check the patch cords setup and fix it.

Step 2 Alternatively, review the network configuration to see if the Raman amplifier has been wrongly used. If it is, remove it.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

RAMAN-CALIBRATION-FAILED

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: OTS

The RAMAN-CALIBRATION-FAILED alarm is raised on the EDRA-1-xx, EDRA-2-xx, and RAMAN-CTP cards when automatic Raman pump calibration is failed and will not run again. The alarm indicates insufficient Raman Amplification by customer fibre. The Raman calibration can also fail due to the setup issues that include:

- Wrong patch-cords or cabling
- Incorrect ANS
- Missing communication channel between nodes.

Clear the RAMAN-CALIBRATION-FAILED Alarm

Procedure

Step 1 Use optical time domain reflectometer (OTDR) to identity any excess loss between the Raman card LINE-RX port and the customer fibre. After the inspection, a new Raman Calibration is triggered and if the physical problem is fixed, the alarm will clear.

Step 2 If the alarm is caused by a set-up problem, re-verify all node installation steps and manually trigger a Raman Calibration.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

RAMAN-CALIBRATION-PENDING

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: OTS

The RAMAN-CALIBRATION-PENDING condition is raised on the EDRA-1-xx, EDRA-2-xx, and RAMAN-CTP cards when automatic Raman pump calibration is scheduled to run repeatedly after the first installation or fiber cut. The condition is cleared when the Raman pump calibration succeeds or fails for 30 attempts.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

RAMAN-CALIBRATION-RUNNING

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: OTS

The RAMAN-CALIBRATION-RUNNING alarm is raised on the EDRA-1-xx, EDRA-2-xx, and RAMAN-CTP cards when the Raman pump calibration is running. The alarm is cleared when the Raman pump calibration succeeds or fails.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

RAMAN-G-NOT-REACHED

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: OTS

The RAMAN-G-NOT-REACHED alarm is raised on the OPT-RAMP-C cards when the Raman gain value is lower than the ANS target. The alarm also occurs after a cut restoration procedure fails to restore the expected Raman gain set point.

Clear the RAMAN-G-NOT-REACHED Alarm

Procedure

Do the steps that follow to clear the alarm on the OPT-RAMP-C card:

a) Repair the span.
b) Clean the fiber connectors at both ends according to site practice.
c) Check for patch panel connections and fiber splices, if any.
d) Reconnect the fibers according to site practice.
e) Perform the Raman Wizard day-0 procedure to recalibrate the Raman gain setpoint.

REMOTE-FAULT

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Objects: ETH

- when there is a loss of signal synchronization on the port.
- when a remote fault character sequence is received in the incoming MAC stream as defined in IEEE 802.3ae, 10 Gigabit Ethernet fault signaling scheme.

Clear the REMOTE-FAULT Alarm

Procedure

Step 1 Verify and resolve the client port fault and remote fault errors on the remote or upstream node.

Step 2 Verify and resolve loss of signal synchronization error on the remote or upstream node.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

REP-LINK-FLAPPING

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Objects: ETH

The REP-LINK-FLAPPING alarm is raised on GE_XP and 10GE_XP cards when a link flap is detected, and is raised against the REP ports (and switches) facing the link flap.

Clear the REP-LINK-FLAPPING

Procedure

The alarm is cleared when the link flapping is over.

REP-NEIHB-ADJ-FAIL

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Objects: ETH

The REP-NEIHB-ADJ-FAIL (REP-NEIHB-ADJ-FAIL) alarm is raised on GE_XP and 10GE_XP cards when a link flap is detected, and is raised against the REP ports (and switches) facing the link flapping. The alarm is raised till adjacency cannot be established. The alarm is raised in the following scenarios:

- The link between the two REP peer ports is down.
- The switch within the REP segment is down.

The alarm is raised against the REP port facing the immediate loss of adjacency. The alarm is raised on the REP peer port and two peer REP ports impacted by the loss of adjacency based on the two scenarios listed.

Note This alarm does not apply to EdgeNN ports.

Clear the REP-NEIHB-ADJ-FAIL Alarm

Procedure

The alarm is cleared as soon as adjacency is established.

REP-SEGMENT-FAULT

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Objects: ETH, GE

The REP-SEGMENT-FAULT alarm is raised when a segment failure is detected in the following possible scenarios:

- The link between two REP peer ports is down.
- The switch within the REP segment is down.
- REP protocol failure is present on the switch within the REP segment.

The alarm is raised at all REP ports across all switches participating in the impacted REP segment.

Clear the REP-SEGMENT-FAULT Condition

Procedure

The REP-SEGMENT-FAULT alarm is cleared once the segment is complete.

REROUTE-IN-PROG

Default Severities: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Objects: OTS

The Reroute in Progress alarm is raised when a control plane service undergoes a reroute operation.

Clear the REROUTE-IN-PROG Alarm

Procedure

This alarm is cleared automatically when the reroute operation is complete.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

REVERT-IN-PROG

Default Severities: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Objects: OTS

The Revert in Progress alarm is raised when a control plane service undergoes a revert operation.

Clear the REVERT-IN-PROG Alarm

Procedure

This alarm is cleared automatically when the revert operation is complete.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

RFI

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

Logical Object: TRUNK

The Remote Failure Indication condition is raised against . 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.

Clear the RFI Condition

Procedure

Complete the Delete a Circuit, on page 395 procedure and then recreate the circuit.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

RFI-L

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

Logical Object: TRUNK

A RFI Line condition occurs when the system detects an RFI in OC-N card SONET overhead because of a fault in another node. Resolving the fault in the adjoining node clears the RFI-L condition in the reporting node. RFI-L indicates that the condition is occurring at the line level.

Clear the RFI-L Condition

Procedure

Step 1 Log into the node at the far-end node of the reporting system.

Step 2 Identify and clear any alarms, particularly the LOS (OCN) alarm.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

RFI-P

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

Logical Object: STSMON, STSTRM

The RFI Path condition occurs when the system detects an RFI in the an STS-1 signal SONET overhead because of a fault in another node. Resolving the fault in the adjoining node clears the RFI-P condition in the reporting node. RFI-P occurs in the terminating node in that path segment.

Clear the RFI-P Condition

Procedure

Step 1 Verify that the ports are enabled and in service (IS-NR) on the reporting system:

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 OC-N 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.

e) If the Admin State column lists the port as OOS,MT or OOS,DSBLD , click the column and choose **IS**. Click **Apply**.

Note If ports managed into IS admin state are not receiving signals, the LOS alarm is either raised or remains, and the port service state transitions to OOS-AU,FLT.

Step 2 To find the path and node failure, verify the integrity of the SONET STS circuit path at each of the intermediate SONET nodes.

Step 3 Clear alarms in the node with the failure, especially the UNEQ-P , on page 370 alarm.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

RLS

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: OTS

Clear the RLS Condition

ROUTE-OVERFLOW

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: NE regardless of MSTP or MSPP

The ROUTE-OVERFLOW indicates the condition when the OSPF routing table exceeds 700 routes. The symptoms for this condition are loss of visibility to a node or network, inability to access a node , CTM, Telnet, Ping, and so on.

Clear the ROUTE-OVERFLOW Condition

Procedure

Reconfigure the OSPF network to less than 700 routes.

RS-EOC

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: TRUNK

The SONET Data Communications Channel (DCC) Termination Failure alarm occurs when the system loses its data communications channel. Although this alarm is primarily SONET, it can apply to DWDM. For example, the OSCM card can raise this alarm on its STM-1 section overhead.

The RS-DCC consists of three bytes, D1 through D3, in the SONET overhead. The bytes convey information about operation, administration, maintenance, and provisioning (OAM&P). The system uses the DCC on the SONET section overhead to communicate network management information.

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

Warning **Class 1M laser radiation when open. Do not view directly with optical instruments.** Statement 1053

Warning **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 an incomplete 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.

Clear the RS-EOC Alarm

Procedure

Step 1 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 RS-DCC traffic. If they are not, correct them.

Caution Always use the supplied electrostatic discharge wristband when working with a powered system. Plug the wristband cable into the ESD jack located lower-right edge of the shelf assembly.

If the physical connections are correct and configured to carry DCC traffic, ensure that both ends of the fiber span have unlocked ports. Verify that the ACT/SBY LED on each card is green.

Step 2 When the LEDs on the cards are correctly illuminated, complete the Verify or Create Node RS-DCC Terminations, on page 396 procedure to verify that the DCC is provisioned for the ports at both ends of the fiber span.

Step 3 Repeat Step 2, on page 336 procedure at the adjacent nodes.

Step 4 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.

Step 5 If no signal failures exist on terminations, measure power levels to verify that the budget loss is within the parameters of the receiver.

Step 6 If budget loss is within parameters, ensure that fiber connectors are securely fastened and properly terminated.

Step 7 Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card.

Resetting the active control card switches control to the standby control card. If the alarm clears when the node switches to the standby control card, the user can assume that the previously active card is the cause of the alarm.

Step 8 If the control card reset does not clear the alarm, delete the problematic RS-DCC termination by completing the following steps:

a) From card view, click **View** > **Go to Previous View** if you have not already done so.
b) Click the **Provisioning** > **Comm Channels** > **RS-DCC** tabs.
c) Highlight the problematic DCC termination.
d) Click **Delete**.
e) Click **Yes** in the Confirmation Dialog box.

Step 9 Recreate the RS-DCC termination. Refer to the Turn Up Network chapter in the Configuration guide for procedures.

Step 10 Verify that both ends of the DCC have been recreated at the optical ports.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

If the Technical Support technician tells you to reseat the card, complete the Remove and Reinsert (Reseat) Any Card , on page 393 procedure. If the Technical Support technician tells you to remove the card and reinstall a new one, follow the Physically Replace a Card, on page 394 procedure.

RS-TIM

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: STMN

The Regenerator Section TIM alarm occurs when the expected J0 path trace string does not match the received string.

If the alarm occurs on a port that has been operating with no alarms, the circuit path has changed or someone entered a new incorrect value into the Current Transmit String field. Follow the procedure below to clear either instance.

Clear the RS-TIM Alarm

Procedure

Complete the Clear the TIM Alarm, on page 363 procedure for the J0 byte.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

SBYTCC-NEINTCLK

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SDH Logical Object: EQPT

The "Standby TCC - NE Clock Is Internal Clock" condition occurs when the standby TCC NE clock switches to the internal oscillator (clock). This alarm occurs when NE is forced to use internal clock or if all the external clocks fails so that the NE automatically switches to internal clock. This also occurs when the sandby TCC fails and starts using internal NE clock instead of tracking the provisioned external clock.

Clear the SBYTCC-NEINTCLK Alarm

Procedure

Step 1 Clear the following alarms that relate to timing:

- FRNGSYNC , on page 182
- FSTSYNC , on page 182
- LOF (BITS) , on page 232
- LOS (BITS) , on page 240
- HLDOVRSYNC , on page 198
- MANSWTOINT, on page 264
- MANSWTOPRI , on page 264
- MANSWTOSEC , on page 264
- MANSWTOTHIRD , on page 264
- SWTOPRI , on page 356
- SWTOSEC , on page 357

- SWTOTHIRD , on page 357
- SYNC-FREQ , on page 358
- SYNCPRI , on page 359
- SYNCSEC , on page 360
- SYSBOOT , on page 361

Step 2 Reestablish a primary and secondary timing source according to local site practice. If none exists, refer to the Change Node Settings chapter in the Configuration guide.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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 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 system is user-provisionable and has a range for SD from 1E9 dBm to 1E5 dBm.

Clear the SD (TRUNK) Condition

Procedure

Step 1 Ensure that the fiber connector for the card is completely plugged in.

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.

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 Physical Card Reseating, Resetting, and Replacement, on page 392 section.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

SD-L

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: STMN

An SD Line condition is similar to the SD (TRUNK) , on page 338 condition. It applies to the line level of the SONET signal and travels on the B2 byte of the SONET overhead.

An SD-L on an Ethernet or OC-N card does not cause a protection switch. If the alarm is reported on a card that has also undergone a protection switch, the SD BER count continues to accumulate. The condition is superseded by higher-priority alarms such as the LOF and LOS alarms.

Clear the SD-L Condition

Procedure

Complete the Clear the SD (TRUNK) Condition, on page 338 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

SD-L (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, TXP_MR_10E_C, TXP_MR_10E_L, TXPP_MR_2.5G, GE-XP, 10GE-XP, and ADM-10G card has bit error rate (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.

Clear the SD-L (TRUNK) Condition

Procedure

Complete the Clear the SD (TRUNK) Condition, on page 338 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

SD-P

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: STSMON, STSTRM

An SD Path condition is similar to the SD (TRUNK) , on page 338 condition, but it applies to the path (STS) layer of the SONET overhead. A path or STS-level SD alarm travels on the B3 byte of the SONET overhead.

For path protection protected circuits, the BER threshold is user-provisionable and has a range for SD from 1E–9 dBm to 1E–5 dBm. For BLSR 1+1 and unprotected circuits, the BER threshold value is not user-provisionable and the error rate is hard-coded to 1E–6 dBm.

On path protection configurations, an SD-P condition causes a switch from the working card to the protect card at the path (STS) level. On BLSR, 1+1, and on unprotected circuits, an SD-P condition does not cause switching.

The BER increase that causes the condition is sometimes caused by a physical fiber problem such as a poor fiber connection, a bend in the fiber that exceeds the permitted bend radius, or a bad fiber splice.

The SD clears when the BER level falls to one-tenth of the threshold level that triggered the alarm.

Clear the SD-P Condition

Procedure

Complete the Clear the SD (TRUNK) Condition, on page 338 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

SDBER-EXCEED-HO

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: VCMON-HP, VCTRM-HP

The Signal Degrade Threshold Exceeded for High Order condition indicates that the signal degrade BER threshold has been exceeded for a high-order (VC-4) path on optical (traffic) cards. SDBER-EXCEED-HO occurs when the signal BER falls within the degrade threshold (typically 1E-7 dBm) set on the node.

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

Warning **Class 1M laser radiation when open. Do not view directly with optical instruments.** Statement 1053

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

Clear the SDBER-EXCEED-HO Condition

Procedure

Step 1 Determine the BER threshold. Complete the Clear an MXP, TXP, GE-XP, 10GE-XP, and ADM-10G Card Loopback Circuit, on page 396 procedure.

Step 2 If adjustment is acceptable in site practices, adjust the threshold.

Using an optical test set, measure the input power level of the line and ensure that the level is within the guidelines. For specific procedures to use the test set equipment, consult the manufacturer.

Step 3 Verify the input fiber cable connections to the reporting card.

Step 4 Clean the input fiber cable ends according to site practice. If no site practice exists, complete the procedure in the Maintain the Node chapter of the Configuration guide.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

SEQ-MISMATCH-COUNT

Default Severity: Minor (MN)

Logical Object: TRUNK (OTU)

The Sequence Mismatch Count alarm is raised on the OTU trunk port in the WSE card. This alarm is a Threshold Crossing Alert (TCA). This alarm is raised when the sequence mismatch count crosses the provisioned threshold. The TCA is present for a duration of 15 minutes.

Clearing the SEQ-MISMATCH-COUNT Alarm

The alarm is cleared when the polling starts for the following 15 minutes interval, and the sequence mismatch count for that interval is within the threshold value.

If the troubleshooting procedure does not clear the alarm, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html or call the Cisco Technical Assistance Center (1 800 553-2447) to report the problem.

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 TXP or MXP 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

Clear the SF (TRUNK) Condition

Procedure

Complete the Clear the SD (TRUNK) Condition, on page 338 procedure.

Caution Always use the supplied electrostatic discharge wristband when working with a powered NCS system. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

SF-L

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: EQPT

An SF Line condition is similar to the SD (TRUNK) , on page 338 condition, but it applies to the line layer B2 overhead byte of the SONET signal. It can trigger a protection switch.

The SF-L condition clears when the BER level falls to one-tenth of the threshold level that triggered the condition. A BER increase is sometimes caused by a physical fiber problem, including a poor fiber connection, a bend in the fiber that exceeds the permitted bend radius, or a bad fiber splice.

The condition is superseded by higher-priority alarms such as the LOF and LOS alarms.

Clear the SF-L Condition

Procedure

Complete the Clear the SD (TRUNK) Condition, on page 338 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

SF-L (TRUNK)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: TRUNK

A Signal Fail (SF) condition is raised on the trunk when the quality of an incoming optical signal to the MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, TXP_MR_10E, TXP_MR_10E_C, TXP_MR_10E_L, TXPP_MR_2.5G, or ADM-10G card has high BER due to bent or degraded fiber connected to the trunk, 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.

The SF-L condition monitors the incoming BER and is triggered when the BER surpasses the default range.

Clear the SF-L (TRUNK) Condition

Procedure

Complete the Clear the SD (TRUNK) Condition, on page 338 procedure.

Caution Always use the supplied electrostatic discharge wristband when working with a powered NCS system. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly. For detailed instructions on how to wear the ESD wristband, refer to the Electrostatic Discharge and Grounding Guide.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

SF-P

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: STSMON, STSTRM

An SF Path condition is similar to the SF (TRUNK) , on page 342 condition, but it applies to the path (STS) layer B3 byte of the SONET overhead. It can trigger a protection switch.

The SF-P condition clears when the BER level falls to one-tenth of the threshold level that triggered the condition. A BER increase is sometimes caused by a physical fiber problem, including a poor fiber connection, a bend in the fiber that exceeds the permitted bend radius, or a bad fiber splice.

Clear the SF-P Condition

Procedure

Complete the Clear the SF (TRUNK) Condition, on page 342 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

SFTWDOWN

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: EQPT

A Software Download in Progress alarm occurs when the control card is downloading or transferring software.

If the active and standby control cards have the same versions of software, it takes approximately three minutes for software to be updated on a standby control card.

If the active and standby control cards 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 control card 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 condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

Note SFTWDOWN is an informational alarm.

SFTWDOWN-FAIL

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: EQPT

The Software Download Failed (SFTDOWN-FAIL) alarm occurs when the software package download fails on the control card of the system in a multishelf configuration.

An incorrect input that points to the wrong place or file, network issues, or a bad (corrupt) software package can cause this failure. If the software package is corrupt, contact the Cisco Technical Assistance Center (TAC) (1 800 553-2447) for assistance.

Clear the SFTWDOWN-FAIL Alarm

Procedure

Step 1 Verify the network connectivity by pinging the system that is reporting the alarm .

Step 2 Reboot the working (active) control card.

Step 3 Download the software package on the working (active) control card.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

SHELF-COMM-FAIL

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: SHELF

The Shelf Communication Failure alarm applies to optical equipment when an NC shelf is unable to communicate with an SS shelf. Typically this occurs when there is a fiber disconnection. But the alarm can also occur if an SS shelf is resetting.

Clear the SHELF-COMM-FAIL Alarm

Procedure

Step 1 Determine whether an SS shelf controller is being reset. If it is being reset, you must wait for the shelf to reset for this alarm to clear.

Step 2 If the alarm does not clear or if no shelf is being reset, perform the following:

a) NCS 2006 as NC shelf—Check the cabling between the MSM ports of NC shelf and SS shelf controller. Correct it if necessary. Check if the External Connection Unit in the NC and SS shelf is installed correctly.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

SH-IL-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.

Clear the SH-IL-VAR-DEG-HIGH Alarm

Procedure

For the alarmed card, complete the Physically Replace a Card, on page 394 procedure as appropriate.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

SH-IL-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.

Clear the SH-IL-VAR-DEG-LOW Alarm

Procedure

For the alarmed card, complete the Physically Replace a Card, on page 394 procedure as appropriate.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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) , on page 243 alarm 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

Procedure

Step 1 Complete the Clear the LOS (OTS) Alarm, on page 243 procedure.

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, on page 394 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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 cards 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

Procedure

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.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

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 NCS system serving as an IP proxy for the other NCS 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 NCS system proxy node is experiencing problems, or the NCS system proxy node itself is not functioning properly.

Clear the SNTP-HOST Alarm

Procedure

Step 1 Ping the SNTP host from a workstation in the same subnet to ensure that communication is possible within the subnet.

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 system.

SOFT-VERIF-FAIL

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: EQPT

The Software Signature Verification Failed (SOFT-VERIF-FAIL) alarm occurs under the following conditions:

- The software running on any line card in the system is tampered with or the software running on the system did not originate from Cisco.
- Problem present in the software stored in the line cards.

Clear the SOFT-VERIF-FAIL Alarm

Procedure

To clear the alarm, log into the Technical Support Website at http://www.cisco.com/cisco/web/support/index.html for more information or call Cisco TAC (1 800 553-2447).

SPANLEN-OUT-OF-RANGE

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: OTS

The SPANLEN-OUT-OF-RANGE alarm is raised when span loss measured is higher than the maximum expected span loss (or lower than the minimum expected span loss).

The control card automatically measures span loss every hour, or it calculates it when you perform the Calculate Span Loss operation.

Clear the SPANLEN-OUT-OF-RANGE Alarm

Procedure

Step 1 Determine the maximum and minimum expected span loss values
a) Log into the SVO web interface.
b) Click the hamburger icon at the top-left of the page, and select **Node Configuration**.
c) Click the **Optical Configuration** > **Span Loss** tabs.
d) Check the maximum and minimum expected span loss values.

Step 2 Determine whether the measured span length falls between these two values.

Step 3 If the value falls outside this range, check the following factors in the fibering:

- Clearance
- Integrity
- Connection

Step 4 Determine whether any site variations are present which conflict with the design and correct them.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

SPAN-NOT-MEASURED

SPAN-NOT-MEASURED is a transient condition.

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 card 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 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.

The local client raises a SQUELCHED condition if the local trunk raises one of the following alarms:

-
-
-
-
-
-
-
- LOF (OCN/STMN) alarm
- LOS (OCN/STMN) alarm
-
-

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

Procedure

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. If it is in loopback, complete the following steps:

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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.

SSM-FAIL

Single Failure Default Severity: 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 NCS system. This alarm indicates that although the NCS system is set up to receive SSM, the timing source is not delivering valid SSM messages.

Clear the SSM-FAIL Alarm

Procedure

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.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

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.

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 ports. 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

Procedure

Complete the Clear the SSM-FAIL Alarm, on page 352 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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 MXP trunk ports is PRC.

Note SSM-PRC is an informational condition and does not require troubleshooting.

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 MXP trunk ports is Stratum 1 Traceable.

Note SSM-PRS is an informational condition and does not require troubleshooting.

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 MXP trunk ports is RES.

Note SSM-RES is an informational condition and does not require troubleshooting.

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 MXP trunk ports 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.

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 MXP trunk ports is ST2.

Note SSM-ST2 is an informational condition and does not require troubleshooting.

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 MXP trunk ports is ST3.

Note SSM-ST3 is an informational condition and does not require troubleshooting.

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 MXP trunk ports 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.

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 MXP trunk ports. The message quality is not used because it is below ST3.

Note SSM-ST4 is an informational condition and does not require troubleshooting.

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 NCS system has SSM support enabled (MXP trunk ports). SSM-STU can also occur if the timing source is sending out SSM messages but SSM is not enabled on the NCS system.

Clear the SSM-STU Condition

Procedure

Step 1 In node view (single-shelf mode) or shelf view (multishelf mode), 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**.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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 MXP trunk ports.

Note SSM-TNC is an informational condition and does not require troubleshooting.

SW-MISMATCH

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: EQPT

The Software Mismatch condition occurs during software upgrade when there is a mismatch between software versions.

Clear the SW-MISMATCH Condition

Procedure

Complete the procedure for the errored card.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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 NCS system switches to the primary timing source (reference 1). The NCS 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.

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 NCS system has switched to a secondary timing source (reference 2).

Clear the SWTOSEC Condition

Procedure

To clear the condition, clear alarms related to failures of the primary source, such as the SYNCPRI , on page 359 alarm.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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 NCS system has switched to a third timing source (reference 3).

Clear the SWTOTHIRD Condition

Procedure

To clear the condition, clear alarms related to failures of the primary source, such as the SYNCPRI , on page 359 alarm or the SYNCSEC , on page 360 alarm.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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

Procedure

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, on page 394 procedure for the control card.

Note It takes up to 30 minutes for the control card to transfer the system software to the newly installed control card. Software transfer occurs in instances where different software versions exist on the two cards. When the transfer completes, the active control card reboots and goes into standby mode after approximately three minutes.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

SYNCLOSS

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Objects: FC, GE, ISC, TRUNK, EQPT

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

Procedure

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.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

SYNCPRI

Default Severity:

Minor (MN), Non-Service-Affecting (NSA) for EXT-SREF; Major (MJ), Service-Affecting (SA) for NE-SREF (For SONET)

Minor (MN), Non-Service-Affecting (NSA) for EXT-SREF; Major (MJ), Non-Service-Affecting (NSA) for NE-SREF (For SDH)

Logical Objects: EXT-SREF, NE-SREF

A Loss of Timing on Primary Reference alarm occurs when the NCS system loses the primary timing source (reference 1). The NCS 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 NCS system should switch to its secondary timing source (reference 2). Switching to the secondary timing source also triggers the SWTOSEC , on page 357 alarm.

Clear the SYNCPRI Alarm

Procedure

Step 1 In node view (single-shelf mode) or shelf view (multishelf mode), 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, on page 240 procedure.

Step 4 If the primary reference clock is an incoming port on the NCS system, complete the Clear the LOS (OCN/STMN) Alarm procedure located in the Alarm Troubleshooting chapter of the Troubleshooting guide.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

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 system loses the secondary timing source (reference 2). If SYNCSEC occurs, the system should switch to a third timing source (reference 3) to obtain valid timing for the system. Switching to a third timing source also triggers the SWTOTHIRD , on page 357 alarm.

Clear the SYNCSEC Alarm

Procedure

Step 1 In node view (single-shelf mode) or shelf view (multishelf mode), 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, on page 240 procedure.

Step 4 Verify that the BITS clock is operating properly.

Step 5 If the secondary timing source is an incoming port on the system, complete the Clear the LOS (OCN/STMN) Alarm procedure located in the Alarm Troubleshooting chapter of the Troubleshooting guide.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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 NCS system loses the third timing source (reference 3). If SYNCTHIRD occurs and the NCS system uses an internal reference for source three, the control card could have failed. The NCS system often reports either the FRNGSYNC , on page 182 condition or the HLDOVRSYNC , on page 198 condition after a SYNCTHIRD alarm.

Clear the SYNCTHIRD Alarm

Procedure

Step 1 In node view (single-shelf mode) or shelf view (multishelf mode), 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 Configuration guide.

Step 3 If the third timing source is a BITS input, complete the Clear the LOS (BITS) Alarm, on page 240 procedure.

Step 4 If the third timing source is an incoming port on the system, complete the Clear the LOS (OCN/STMN) Alarm procedure located in the Alarm Troubleshooting chapter of the Troubleshooting guide.

Caution Always use the supplied electrostatic discharge wristband when working with a powered system. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 5 Wait ten minutes to verify that the control card you reset completely reboots and becomes the standby card.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

SYSBOOT

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: NE

The System Reboot alarm indicates that new software is booting on the control card. No action is required to clear the alarm. The alarm clears when all cards finish rebooting the new software. The reboot takes up to 30 minutes. However, if several line cards are present on the nodes in the network or if the line cards reboot many times, the alarm clears before all the line cards reboot completely.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

Note SYSBOOT is an informational alarm. It only requires troubleshooting if it does not clear.

TEMP-LIC

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: EQPT

The Temporary License (TEMP-LIC) alarm is raised to indicate that a valid temporary license is in use.

Clear the TEMP-LIC Alarm

Procedure

Procure and install a permanent license.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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 control cards 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 control cards, allowing the values to be compared. The temperature of each control card 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

Procedure

Step 1 Complete the Inspect, Clean, and Replace the Air Filter, on page 397 procedure.

Step 2 If the condition does not clear, complete the Remove and Reinsert a Fan-Tray Assembly, on page 398 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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, 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. 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

Procedure

Step 1 Ensure that the physical fibers are correctly configured and attached. To do this, consult site documents.

Step 2 If the alarm does not clear, ensure that the signal has not been incorrectly routed.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

TIM-MON

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: TRUNK

The TIM Section Monitor TIM alarm is similar to the TIM , on page 362 alarm, but it applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, TXP_MR_10E_C, TXP_MR_10E_L, 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.)

Clear the TIM-MON Alarm

Procedure

Complete the Clear the TIM Alarm, on page 363 procedure.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

TIM-P

Default Severity: Critical (CR), Service-Affecting (SA) for STSTRM; Default Severity: Minor (MN), Non-Service-Affecting (NSA) for STSMON

Logical Object: STSMON, STSTRM

The TIM Path alarm occurs when the expected path trace string does not match the received path trace string. Path Trace Mode must be set to Manual or Auto for the TIM-P alarm to occur.

In manual mode at the Path Trace window, the user types the expected string into the Current Expected String field for the receiving port. The string must match the string typed into the Transmit String field for the sending port. If these fields do not match, the login node raises the TIM-P alarm. In Auto mode on the receiving port, the card sets the expected string to the value of the received string. If the alarm occurs on a port that has been operating with no alarms, the circuit path has changed or someone entered a new incorrect value into the Current Transmit String field. Complete the following procedure to clear either instance.

Clear the TIM-P Alarm

Procedure

Complete the Clear the TIM Alarm, on page 363 procedure. (The option will say Edit J1 Path Trace rather than Edit J0 Path Trace.)

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

TIM-S

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: OCN

The TIM for Section Overhead alarm occurs when there is a mismatch between the expected and received J0 section overhead strings in either Manual or Auto mode.

In manual mode at the DS3/EC1-48 card Section Trace window, the user enters the expected string into the Current Expected String field for the receiving port. The string must match the string typed into the Transmit String field for the sending port. If these fields do not match, the login node raises the TIM-S alarm.

In Auto mode on the receiving port, the card sets the expected string to the value of the received string. If the alarm occurs on a port that has been operating with no alarms, the circuit path has changed or someone entered a new incorrect value into the Current Transmit String field. Complete the following procedure to clear either problem.

TIM-S also occurs on a port that has previously been operating without alarms if someone switches the cables or optical fibers that connect the ports. If TIM-S is enabled on the port, the AIS-L , on page 102 alarm can be raised downstream and the RFI-L , on page 333 alarm can be raised upstream.

Note AIS-L and RFI-L are disabled or enabled in the **Provisioning** > **EC1** > **Section Trace** tab **Disable AIS/RDI on TIM-S?** check box.

Clear the TIM-S Alarm

Procedure

Step 1 Double-click the DS3/EC1-48 card to open the card view.

Step 2 Click the **Provisioning** > **EC1** > **Section Trace** tabs.

Step 3 Choose the port from the **Port** pull-down.

Step 4 In the Expected area, enter the correct string into the **Current Expected String** field.

Step 5 Click **Apply**.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

TRAF-AFFECT-RESET-REQUIRED

Default Severity: Minor (MN) and Non-Service affecting (NSA)

Logical Object: CARD

The Traffic Affecting Reset Required alarm is raised when you have to reset the MR-MXP cards. This reset impacts the traffic.

When you downgrade the WSE card from Release 11.12 to older releases such as R11.1.1.2, R11.0, R10 and so on, the Traffic Affecting Reset Required alarm is raised and does not clear.

The Traffic Affecting Reset Required alarm is raised when you have to upgrade the SMR 20 or SMR 20 FS CV cards.

Clear the TRAF-AFFECT-RESET-REQUIRED Alarm

Procedure

Step 1 Display the MR-MXP card in the card view.

Step 2 Click the **Provisioning > Card > Operating Modes** tabs.

Step 3 Click the **FGPA/FIRWAREUpgrade/TrafficAffectingReset** button.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

Clear the TRAF-AFFECT-RESET-REQUIRED Alarm for SMR 20 and SMR 20 FS CV Cards

Procedure

Step 1 Display the SMR 20 or SMR20 FS CV card in the card view.

Step 2 Click the **Maintenance> Firmware** tabs.

Step 3 Click the **FIRMWARE Upgrade** button.

Step 4 Click **Yes**.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

TRAF-AFFECT-SEC-UPG-REQUIRED

Default Severity: Not Reported (NR), Non Service Affecting (NSA)

Logical Object: EQUIPMENT

The TRAF-AFFECT-SEC-UPG-REQUIRED alarm occurs when there is a control FPGA version mismatch and the control FPGA flash partition is not locked.

Clear the TRAF-AFFECT-SEC-UPG-REQUIRED alarm

Procedure

Upgrade the FPGA image and lock the partition of the control FPGA.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

TRAIL-SIGNAL-FAIL

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Objects: OCH, TRUNK

The Trail Signal Fail condition is raised on a DWDM trunk port or OCH port to correlate with the LOS-P (TRUNK) , on page 252 alarm when the trunk port administrative state is set to OOS,DSBLD (or Locked,disabled).

Clear the TRAIL-SIGNAL-FAIL Condition

Procedure

Switch the OCHNC administrative state of the errored OCH or trunk port to **IS** (or **Unlocked**).

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

TRUNK-ODU-AIS

Default Severity: Not Reported (NR)

Logical Object: OCN, OTU, GE, FC

The TRUNK-ODU-AIS condition is raised on the 100G-LC-C or 10x10G-LC card when the node detects the optical data unit (ODU) alarm indication signal (AIS) from the trunk port. This condition is raised to indicate a signal failure.

Clear the TRUNK-ODU-AIS Condition

Procedure

Remove the far-end fault causing the remote ODU-AIS insertion and bring up the traffic between the two ports.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

TRAIL-SIGNAL-FAIL

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Objects: OCH, TRUNK

The Trail Signal Fail condition is raised on a DWDM trunk port or OCH port to correlate with the LOS-P (TRUNK) , on page 252 alarm when the trunk port administrative state is set to OOS,DSBLD (or Locked,disabled).

Clear the TRAIL-SIGNAL-FAIL Condition

Procedure

Switch the OCHNC administrative state of the errored OCH or trunk port to **IS** (or **Unlocked**).

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

OPU-CSF

Default Severity: Not Reported (NR)

Logical Objects: GE

The Optical Payload Unit Client Signal Fail (OPU-CSF) alarm indicates a remote client signal failure on the node.

Clear the OPU-CSF Alarm

Procedure

Clear the remote client signal on the node.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

TRUNK-PAYLOAD-MISM

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: OCN, OTN, GE, FC

The TRUNK-PAYLOAD-MISM alarm is raised on the 10x10G-LC card, which is configured in the 10x10G muxponder mode. This occurs when the payload types configured at the near-end and far-end nodes are different.

Clear the TRUNK-PAYLOAD-MISM Alarm

Configure the same payload type at both near-end and far-end nodes.

Procedure

Step 1 Log in to a node on the network.

Step 2 In node view (single-shelf mode) or shelf view (multishelf mode), double-click the reporting card in CTC to open the card view.

Step 3 Click the **Provisioning** > **Pluggable Port Modules** tabs.

Step 4 In the Pluggable Port Modules area, click **Create**.

Step 5 Choose the same payload type from the Port Type drop-down list and click **OK**.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

TX-OFF-NON-CISCO-PPM

Default Severity: Major (MJ), Non-Service-Affecting (NSA)

Logical Object: PPM

The Laser Off Non Cisco PPM (TX-OFF-NON-CISCO-PPM) alarm occurs when the PPM plugged into a card's port fails the security code check and laser is shutdown. The check fails when the PPM used is not a Cisco PPM.

Clear the TX-OFF-NON-CISCO-PPM Condition

Procedure

Obtain the correct Cisco PPM and replace the existing PPM with the new one.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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.

Clear the UNC-WORD Condition

Procedure

Step 1 Ensure that the fiber connector for the card is completely plugged in.

Step 2 Ensure that the ports on the far end and near end nodes have the same port rates and FEC settings.

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.

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 Physical Card Reseating, Resetting, and Replacement, on page 392 section.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

UNEQ-P

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: STSMON, STSTRM

An SLMF UNEQ Path alarm occurs when the path does not have a valid sender. The UNEQ-P indicator is carried in the C2 signal path byte in the SONET overhead. The source of the problem is the node that is transmitting the signal into the node reporting the UNEQ-P.

The alarm could result from a PARTIAL circuit or an empty VT tunnel. UNEQ-P occurs in the node that terminates a path.

Note If a newly created circuit has no signal, a UNEQ-P alarm is reported on the OC-N cards and the AIS-P condition is reported on the terminating cards. These alarms clear when the circuit carries a signal.

Clear the UNEQ-P Alarm

Procedure

Step 1 In node view, choose **Go to Network View** from the View menu.

Step 2 Right-click the alarm to display the Select Affected Circuits shortcut menu.

Step 3 Click **Select Affected Circuits**.

Step 4 When the affected circuits appear, look in the Type column for VTT, which indicates a VT tunnel circuit. A VT tunnel with no VTs assigned could be the cause of an UNEQ-P alarm.

Step 5 If the Type column does not contain VTT, there are no VT tunnels connected with the alarm. Go to Step 7, on page 371.

Step 6 If the Type column does contain VTT, attempt to delete these rows:

Note The node does not allow you to delete a valid VT tunnel or one with a valid VT circuit inside.

a) Click the VT tunnel circuit row to highlight it. Complete the Delete a Circuit, on page 395 procedure.
b) If an error message dialog box appears, the VT tunnel is valid and not the cause of the alarm.
c) If any other rows contain VTT, repeat Step 6, on page 371.

Step 7 If all nodes in the ring appear in the CTC network view, determine whether the circuits are complete:

a) Click the **Circuits** tab.
b) Verify that PARTIAL is not listed in the Status column of any circuits.

Step 8 If you find circuits listed as PARTIAL, use an optical test set to verify that these circuits are not working circuits that continue to pass traffic. For specific procedures to use the test set equipment, consult the manufacturer.

Step 9 If the PARTIAL circuits are not needed or are not passing traffic, delete the PARTIAL circuits.

Complete the Delete a Circuit, on page 395 procedure.

Step 10 Recreate the circuit with the correct circuit size. Refer to the Create Circuits and VT Tunnels chapter in the Configuration guide.

Step 11 Log back in and verify that all circuits terminating in the reporting card are active:

a) Click the **Circuits** tab.
b) Verify that the **Status** column lists all circuits as active.

Step 12 If the alarm does not clear, clean the far-end optical fiber according to site practice. If no site practice exists, complete the procedure in the Maintain the Node chapter of the Configuration guide.

On the OC-192 card:

Warning **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

Caution Always use the supplied electrostatic discharge wristband when working with a powered system. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 13 If the alarm does not clear, complete the Physically Replace a Card, on page 394 procedure for the OC-N and electrical cards.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

UNIT-HIGH-TEMP

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

Logical Object: EQPT

The UNIT-HIGH-TEMP alarm applies to the 100G-LC-C, 10x10G-LC, or CFP-LC cards. The alarm occurs when the temperature of any one of the internal measurement points exceeds its predefined threshold. It indicates that the card is functioning in abnormal conditions that could jeopardize its reliability in the long term. The alarm is raised because of one of these reasons:

- An improper rack installation
- Abnormally high environmental temperature
- An unclean air filter
- A hardware failure of the card

Clearing the UNIT-HIGH-TEMP Alarm

Procedure

Step 1 Verify that the rack is installed properly. For proper airflow and cooling of the shelf, the shape of the vertical posts of the rack should be such that the airflow vents are not covered. For more information about the installation, refer to the *Hardware Installation Guide*.

Step 2 If the rack installation is proper, verify that the environmental temperature of the room is not abnormally high.

Step 3 If the room temperature is not abnormally high, ensure that nothing prevents the fan-tray assembly from passing air through the system shelf.

Step 4 If the airflow is not blocked, determine whether the air filter needs replacement. Refer to the Inspect, Clean, and Replace the Air Filter, on page 397 procedure.

Step 5 If the air filter is clean, ensure all empty slots are installed with filler cards.

Step 6 If all the slots are installed with cards, check the cooling profile settings for the shelf and ensure it is set to high.

Step 7 If the cooling profile settings are proper, complete the Physically Replace a Card, on page 394 procedure for the 100G-LC-C , 10x10G-LC, or CFP-LC card.

Note When you replace a card an identical card, you do not need to make any changes to the database.

If the troubleshooting procedure does not clear the alarm, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html or call the Cisco Technical Assistance Center (1 800 553-2447) to report the problem.

UNQUAL-PPM

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

Logical Objects: PPM

The Unqualified PPM Inserted condition occurs when a PPM with a nonqualified product ID is plugged into the card port; that is, the PPM passes the security code check as a Cisco PPM but is not qualified for use on the particular card.

Clear the UNQUAL-PPM Condition

Procedure

Obtain the correct Cisco PPM and replace the existing PPM with the new one.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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 Reference Manual*Hardware Specifications document.

Note UNREACHABLE-TARGET-POWER is an informational condition. It only requires troubleshooting if it does not clear.

USB-EMPTY-CODE-VOL

Default Severity: Critital (CR) for M2, M6, and M15 chassis, Minor (MN) for Stand-alone control card, Service-Affecting (SA)

Logical Object: USB MODULE

The USB-EMPTY-CODE-VOL alarm occurs when USB gets formatted during a control card software upgrade.

Clearing the USB-EMPTY-CODE-VOL Alarm

The USB-EMPTY-CODE-VOL alarm clears without user intervention as soon as the USBSYNC operation between the control card and the USB interface is successful.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

USBSYNC

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: USB

The USB Synchronization (USB-SYNC) alarm is raised during the sync operation between the control card and the USB interface.

Clear the USB-SYNC Alarm

Procedure

The USB-SYNC alarm clears without user intervention as soon as synchronization between the control card and the USB interface completes.

USB-MOUNT-FAIL Alarm

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Objects: USB

The USB Mount Fail (USB-MOUNT-FAIL) alarm is raised when the USB flash is not mounted.

Clearing the USB-MOUNT-FAIL Alarm

Procedure

Step 1 Back up the database of the active control card.

Step 2 Remove the standby control card.

Step 3 Reboot the active control card.

Step 4 After the active control card is rebooted, reinsert the standby control card.

If the troubleshooting procedure does not clear the alarm, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html or call the Cisco Technical Assistance Center (1 800 553-2447) to report the problem.

USB PORTS DOWN

Default Severity: Major (MJ), Non-Service-Affecting (NSA)

Logical Object: ECU

The USB Ports Down alarm is raised when the USB enumeration fails to detect the external connection unit (ECU) hubs and passive devices.

Clear the USB PORTS DOWN Alarm

Procedure

Perform soft reset or hard reboot of the controller card.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

USB-WRITE-FAIL

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: USB

The USB Write Fail (USB-WRITE-FAIL) alarm is raised when a write operation on the USB interface fails due to communication disruptions.

Clear the USB-WRITE-FAIL Alarm

Procedure

Step 1 Verify that both the control cards are powered and enabled by confirming lighted ACT/SBY LEDs.

Step 2 If both the control cards are powered and enabled, reset the active control card.

Step 3 Wait ten minutes to verify that the card you reset completely reboots.

Step 4 If the control card you reset does not reboot successfully, or the alarm has not cleared, call Cisco TAC 1 800 553-2447.

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 control card.

Clear the UT-COMM-FAIL Alarm

Procedure

Step 1 In node view (single-shelf mode) or shelf view (multishelf mode), 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.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

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

Procedure

Complete the Physically Replace a Card, on page 394 procedure for the alarmed card.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

VOA-DISABLED

Default Severity: Critical (CR), Service-Affecting (SA)

Logical Object: EQPT

The VOA Disabled alarm indicates that the VOA control loop is disabled due to excessive counter-propagation light. This alarm is raised when there is a mis-cabling of interface cards, that is, when the interface trunk TX port is connected to DMX drop-TX port through the patch-panel.

Clear the VOA-DISABLED Condition

Procedure

To clear the alarm, check and ensure that the patchcords connection to and from the interfaces trunk ports are proper.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

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.

Clear the VOA-HDEG Alarm

Procedure

Complete the Physically Replace a Card, on page 394 procedure for the alarmed card.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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.

Clear the VOA-HFAIL Alarm

Procedure

Complete the Physically Replace a Card, on page 394 procedure for the alarmed card.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

VOA-LMDEG

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.

Clear the VOA-LDEG Alarm

Procedure

Complete the Physically Replace a Card, on page 394 procedure for the alarmed card.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

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.

Clear the VOA-LFAIL Alarm

Procedure

Complete the Physically Replace a Card, on page 394 procedure for the alarmed card.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

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 the control cards are out of range of each other by more than 3V DC.

Clear the VOLT-MISM Condition

Procedure

Step 1 Check the incoming voltage level to the shelf using a voltmeter. Follow site practices.

Step 2 Correct any incoming voltage issues.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

WAITING-TO-START

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: OTS

The WAITING-TO-START condition is raised on the COM-TX and EXP-TX ports of 16-WXC-FS, 17 SMR9 FS, 24 SMR9 FS, 34 SMR9 FS, and SMR20 FS cards by the control cards when a cross-connection is ready to start and/or waiting for other transient conditions to clear. The condition clears when cross-connection is running in In-Service administrative state .

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

WAN-SYNCLOSS

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Objects: STSMON, STSTRM

The WAN-SYNCLOSS condition is raised when GE-Syncloss condition is detected on a STS payloads (STS-192c).

Clear the WAN-SYNCLOSS Condition

Procedure

Set a valid GE frame and payload inside the affected STS.

If the alarm does not get cleared, you need to report a Service-Affecting (SA) problem. Log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or log into http://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html to obtain a directory of toll-free Technical Support numbers for your country.

WKSWPR (2R, EQPT, ESCON, FC, GE, ISC, OTS)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Objects: 2R, EQPT, ESCON, FC, GE, ISC, OTS

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.

This condition is raised when traffic is manually or automatically switched from the working to the protect path on the 200G-CK-LC card. Reset the control card to clear the WKSWPR alarm.

Note For more information about protection schemes, refer to the Manage the Node chapter of the *Cisco ONS 15454 DWDM Procedure Guide*Manage the Node document.

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.

WRK-PATH-RECOVERY-CHECK

Default Severity: Non-Alarming (NA), Non-Service Affecting (NSA)

Logical Objects: OTS

The Working Path Recovery Check (WRK-PATH-RECOVERY-CHECK) alarm is raised against PSM cards when traffic switches to the protection path and that is revertive. This alarm is raised only when the protection path is configured as revertive.

Clear the WRK-PATH-RECOVERY-CHECK Alarm

Procedure

WRK-PATH-RECOVERY-CHECK alarm clears in one of these scenarios:

a) The alarm clears automatically when the Wait To Restore (WTR) timer starts. The traffic reverts to working path at the end of the timer.
b) The alarm clears when traffic switches to the working path.

If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

Wait to Restore Condition

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Objects: 2R, ESCON, FC, GE, ISC, PSM

The Wait To Restore condition occurs:

- On the client ports in the 2R, ESCON, FC, GE, and ISC configurations, in a Y-cable protection group when the WKSWPR (TRUNK), on page 381 condition, is raised. The condition occurs when the wait-to-restore time has not expired; this meas 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.
- On PSM cards, when the WTR timer starts. The timer starts before the traffic is switched from the protection path 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.

WTR (TRUNK)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: TRUNK

The Wait To Restore condition occurs when the WKSWPR (TRUNK), on page 381 condition, 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.

WVL-DRIFT-CHAN-OFF

Default Severity: Not Reported (NR), Service-Affecting (SA)

Logical Object: OCH

The Wavelength Channel OFF (WVL_CHAN_OFF) condition occurs in 40-SMR1-C, 40-SMR2-C, 80-WXC-C, 40-WXC-C, or 40-WSS-C cards. The condition detects slow variation in wavelength or optical power of a TXP Trunk-TX port connected to an MSTP multiplexer.

WVL-DRIFT-CHAN-OFF alarm occurs in different ports depending on the type of card:

- In the 80-WXC-C or 40-WXC-C cards, COM-TX port for ADD/DROP and EXP/PT circuits.
- In the 40-SMR1-C or 40-SMR2-C cards, LINE-TX port for ADD/DROP and EXP/PT circuits.
- In the 40-WSS-C card, CHAN-RX port for ADD/DROP circuits and PT port for pass through circuits.

Clear the WVL-DRIFT-CHAN-OFF Condition

Procedure

WVL-DRIFT-CHAN-OFF condition clears in the following scenarios:

- OCH port is forced OOS.
- OCH-circuit associated to the port is deleted or set to OOS state.
- Hardware reset or card removal.
- Software reset of the card.

Note Although the WVL-DRIFT-CHAN-OFF condition is raised in the optical card, make sure that the laser source connected to the MSTP equipment is investigated to isolate the origin of the issue. Laser is likely affected by wavelength instability or wavelength drift causing this condition to occur.

WVL-MISMATCH

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Object: TRUNK

Clear the WVL-MISMATCH alarm

WVL-UNLOCKED Alarm

Default Severity: Major (MJ), Service-Affecting (SA)

Logical Objects: TRUNK

The Wavelength Unlocked (WVL-UNLOCKED) alarm occurs when the laser cannot be tuned at the required wavelength. This is a normal condition during laser frequency requests.

The alarm is cleared when the laser wavelength locker detects a lock condition during which the laser is steadily tuned at the required wavelength.

DWDM Card LED Activity

The following sections list the DWDM card LED sequences during card insertion and reset.

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.

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.

Traffic Card LED Activity

System traffic card LED behavior patterns are listed in the following sections. These sections give behavior for card insertion, reset, and side-switch.

Typical Traffic Card LED Activity After Insertion

When a non-DWDM card is inserted, the following LED activities occur:

1. The red FAIL LED turns on and remains illuminated for 20 to 30 seconds.
2. The red FAIL LED blinks for 35 to 45 seconds.
3. All LEDs blink once and turn off for 5 to 10 seconds.
4. The ACT or ACT/SBY LED turns on. The SF LED can persist until all card ports connect to their far-end counterparts and a signal is present.

Typical Traffic Card LED Activity During Reset

While a non-DWDM card resets, the following LED activities occur:

1. The FAIL LED on the physical card blinks and turns off.
2. The white LED with the letters LDG appears on the reset card in CTC.
3. The green ACT LED appears in CTC.

Typical Card LED State After Successful Reset

When a non-DWDM card successfully resets, the following LED states are present:

- If you are looking at the physical NCS system, the ACT/SBY LED is illuminated.
- If you are looking at node view (single-shelf mode) or shelf view (multishelf mode) of the NCS system, the current standby card has an amber LED depiction with the initials SBY, and this has replaced the white LDG depiction on the card in CTC.
- If you are looking at node view (single-shelf mode) or shelf view (multishelf mode) of the NCS system, the current active card has a green LED depiction with the initials ACT, and this has replaced the white LDG depiction on the card in CTC.

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 system documentation. They are included in this chapter for the user convenience. For further information, please refer to the Configuration guide as appropriate to your purpose

Node and Ring Identification, Change, Visibility, and Termination

The following procedures relate how to identify or change BLSR names and node IDs, and how to verify visibility from other nodes.

Identify a BLSR Ring Name or Node ID Number

Procedure

Step 1 Log into a node on the network.

Step 2 In node view, choose **Go to Network View** from the View menu.

Step 3 Click the **Provisioning** > **BLSR** tabs.

Step 4 From the Ring Name column, record the ring name, or in the Nodes column, record the Node IDs in the BLSR. The Node IDs are the numbers in parentheses next to the node name.

Change a BLSR Ring Name

Procedure

Step 1 Log into a node on the network.
Step 2 In node view, choose **Go to Network View** from the View menu.
Step 3 Click the **Provisioning** > **BLSR** tabs.
Step 4 Highlight the ring and click **Edit.**
Step 5 In the BLSR window, enter the new name in the Ring Name field.
Step 6 Click **Apply.**
Step 7 Click **Yes** in the Changing Ring Name dialog box.

Change a BLSR Node ID Number

Procedure

Step 1 Log into a node on the network.
Step 2 In node view, choose **Go to Network View** from the View menu.
Step 3 Click the **Provisioning** > **BLSR** tabs.
Step 4 Highlight the ring and click **Edit.**
Step 5 In the BLSR window, right-click the node on the ring map.
Step 6 Select **Set Node ID** from the shortcut menu.
Step 7 In the Edit Node ID dialog box, enter the new ID. The Node ID is the number in parentheses after the Node Name.
Step 8 Click **OK.**

Verify Node Visibility for Other Nodes

Procedure

Step 1 Log into a node on the network.
Step 2 In node view, click the **Provisioning** > **BLSR** tabs.
Step 3 Highlight a BLSR.
Step 4 Click **Ring Map**.
Step 5 In the BLSR Ring Map window, verify that each node in the ring appears on the ring map with a node ID and IP address.
Step 6 Click **Close**.

Protection Switching, Lock Initiation, and Clearing

The following sections give instructions for port, ring, and span switching and switch-clearing commands, as well as lock-ons and lockouts.

Initiate a 1+1 Protection Port Force Switch Command

The following sections give instructions for port switching and switch-clearing commands.

Procedure

Step 1 In node view (single-shelf mode) or shelf view (multishelf mode), 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.

Procedure

Step 1 In node view (single-shelf mode) or shelf view (multishelf mode), 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.

Initiate a 1:1 Card Switch Command

Note The Switch command only works on the active card, whether this card is working or protect. It does not work on the standby card.

Procedure

Step 1 In node view, click the **Maintenance** > **Protection** tabs.

Step 2 Click the protection group that contains the card you want to switch.

Step 3 Under Selected Group, click the active card.

Step 4 Next to Switch Commands, click **Switch**.

The working slot should change to Working/Active and the protect slot should change to Protect/Standby.

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.

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.

Procedure

Step 1 In node view (single-shelf mode) or shelf view (multishelf mode), 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.

Procedure

Step 1 In node view (single-shelf mode) or shelf view (multishelf mode), 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.

Procedure

Step 1 In node view (single-shelf mode) or shelf view (multishelf mode), 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

Procedure

Step 1 In node view (single-shelf mode) or shelf view (multishelf mode), 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.

Initiate a Lockout on a BLSR Protect Span

Procedure

Step 1 From the View menu choose **Go to Network View**.
Step 2 Click the **Provisioning** > **BLSR** tabs.
Step 3 Choose the BLSR and click **Edit**.
Step 4 Right-click the BLSR node channel (port) and choose **Set West Protection Operation** (if you chose a west channel) or **Set East Protection Operation** (if you chose an east channel).
Step 5 In the Set West Protection Operation dialog box or the Set East Protection Operation dialog box, choose **Lockout Protect Span** from the drop-down list.
Step 6 Click **OK**.
Step 7 Click **Yes** in the two Confirm BLSR Operation dialog boxes.

Clear a BLSR External Switching Command

Procedure

Step 1 Log into a node on the network.
Step 2 From the View menu, choose **Go to Network View**.
Step 3 Click the **Provisioning** > **BLSR** tabs.
Step 4 Click the BLSR you want to clear.
Step 5 Right-click the west port of the BLSR node where you invoked the switch and choose **Set West Protection Operation**.
Step 6 In the Set West Protection Operation dialog box, choose **Clear** from the drop-down list.
Step 7 Click **OK**.

Step 8 Click **Yes** in the Confirm BLSR Operation dialog box.

Card Resetting and Switching

This section gives instructions for resetting traffic cards and control cards.

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 Configuration 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.

Reset a Card in CTC

Procedure

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2, on page 391.

Step 2 In node view (single-shelf mode) or shelf view (multishelf mode), 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 Control Card and Activate the Standby Card

Note Before you reset the control card, you should wait at least 60 seconds after the last provisioning change you made to avoid losing any changes to the database.

Before you begin

Caution Resetting an active control card can be service-affecting.

Procedure

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 Identify the active control card:

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 In node view (single-shelf mode) or shelf view (multishelf mode), right-click the active control card 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. For LED appearance, see the Typical Card LED State After Successful Reset, on page 385 section.

Step 7 Double-click the node and ensure that the reset control card is in standby mode and that the other control card 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.

Physical Card Reseating, Resetting, and Replacement

This section gives instructions for physically reseating and replacing control cards and line cards.

Caution Do not physically replace a card without first making provisions to switch or move traffic to a different card or circuit..

Remove and Reinsert (Reseat) the Standby Control Card

Note Before you reset the control card, you should wait at least 60 seconds after the last provisioning change you made to avoid losing any changes to the database.

When a standby control card is removed and reinserted (reseated), all three fan lights could momentarily turn on, indicating that the fans have also reset.

Before you begin

Warning **High-performance devices on this card can get hot during operation. To remove the card, hold it by the faceplate and bottom edge. Allow the card to cool before touching any other part of it or before placing it in an antistatic bag.** Statement 201

Caution Always use the supplied electrostatic discharge wristband when working with a powered 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 control card reseat could be service-affecting. Refer to the Protection Switching, Lock Initiation, and Clearing, on page 387 section for traffic-switching procedures.

Procedure

Step 1 Log into a node on the network.

Ensure that the control card you want to reseat is in standby mode. A standby card has an amber ACT/SBY (Active/Standby) LED illuminated.

Step 2 When the control card is in standby mode, unlatch both the top and bottom ejectors on the control card.

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 control card requires several minutes to reboot and display the amber standby LED after rebooting. Refer to the Configuration guide for more information about LED behavior during a card reboot.

Remove and Reinsert (Reseat) Any Card

Before you begin

Warning Warning: High-performance devices on this card can get hot during operation. To remove the card, hold it by the faceplate and bottom edge. Allow the card to cool before touching any other part of it or before placing it in an antistatic bag. Statement 201

Caution Always use the supplied electrostatic discharge wristband when working with a powered NCS system. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Procedure

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

When you replace a card with the identical type of card, you do not need to make any changes to the database.

Before you begin

Warning **High-performance devices on this card can get hot during operation. To remove the card, hold it by the faceplate and bottom edge. Allow the card to cool before touching any other part of it or before placing it in an antistatic bag.** Statement 201

Caution Always use the supplied electrostatic discharge wristband when working with a powered NCS 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 Protection Switching, Lock Initiation, and Clearing, on page 387 section for commonly used traffic-switching procedures.

Procedure

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.

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

This procedure is used for MXP or TXP cards.

Procedure

Step 1 Log into a node on the network.

Step 2 In node view (single-shelf mode) or shelf view (multishelf mode), double-click the card reporting the alarm to open the card view.

Step 3 Click the **Provisioning** > **Line** > **SONET** (or **SDH**) 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

Procedure

Step 1 Log into a node on the network.

Step 2 In node view (single-shelf mode) or shelf view (multishelf mode), 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

Procedure

Step 1 Log into a node on the network.

Step 2 In node view (single-shelf mode) or multishelf view (multishelf mode), click the **Provisioning** > **Comm Channels** > **SDCC** (or **Provisioning** > **Comm Channels** > **MS DCC**) tab.

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 **Set to Unlocked**) radio button.

d) Verify that the Disable OSPF on Link check box is unchecked.
e) Click **OK**.

Clear an MXP, TXP, GE-XP, 10GE-XP, and ADM-10G Card Loopback Circuit

Procedure

Step 1 Log into a node on the network.
Step 2 In node view (single-shelf mode) or shelf view (multishelf mode), 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, for example, OOS,MT.
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.**

Note If ports managed into IS (or Unlocked) administrative state are not receiving signals, the LOS alarm is either raised or remains, and the port service state transitions to OOS-AU,FLT (or Locked-disabled, automaticInService & failed).

Step 8 Click **Apply**.

Verify or Create Node RS-DCC Terminations

Procedure

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.
Step 2 In node view, click the **Provisioning** > **Comm Channels** > **RS-DCC** tab.
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 by completing the following steps:
a) Click **Create**.
b) In the Create RS-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 Unlocked** radio button.
d) Verify that the Disable OSPF on Link check box is unchecked.
e) Click **OK**.

Clear an STM-N Card XC Loopback Circuit

Procedure

Step 1 Log into a node on the network. If you are already logged in, continue with Clear an STM-N Card XC Loopback Circuit, on page 397.

Step 2 Double-click the reporting card in CTC to display the card view.

Step 3 Click the **Maintenance** > **Loopback** > **VC4** tabs.

Step 4 Click **Apply**.

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 Air Filter

Before you begin

To complete this task, you need a replacement air filter, and a pinned hex key.

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

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.

Procedure

Step 1 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 2, on page 398.)

- 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 2 Push the outer side of the handles on the fan-tray assembly to expose the handles.

Step 3 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 4 When the fans have stopped, pull the fan-tray assembly completely out of the shelf assembly.

Step 5 Gently remove the air filter from the shelf assembly. Be careful not to dislodge any dust that could have collected on the filter.

Step 6 Visually inspect the air filter material for dirt and dust.

Step 7 If the air filter has a concentration of dirt and dust, replace the unclean air filter with a clean air filter and reinsert the fan-tray assembly.

Step 8 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 9 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 filter until the fan tray fits correctly.

Note On a powered-up NCS system, the fans start immediately after the fan-tray assembly is correctly inserted.

Step 10 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 11 Rotate the retractable handles back into their compartments.

Step 12 Replace the door and reattach the ground strap.

Remove and Reinsert a Fan-Tray Assembly

Procedure

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 NCS system.

Step 3 Close the retractable handles.

Replace the Fan-Tray Assembly

Before you begin

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 NCS 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.

Procedure

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, on page 399.

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 Air Filter, on page 397 section.

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.

Interface Procedures

This section includes instructions for replacing an AIP.

Replace the Alarm Interface Panel

This procedure replaces an existing AIP with a new AIP on an in-service node without affecting traffic. Ethernet circuits that traverse nodes with a software release prior to R4.0 is affected.

Before you begin

Caution Do not use a 2A AIP with a 5A fan-tray assembly; doing so causes a blown fuse on the AIP.

Caution If any nodes in an Ethernet circuit are not using Software R4.0 or later, there is a risk of Ethernet traffic disruptions. Contact Cisco TAC at 1 800 553-2447 when prompted to do so in the procedure.

Note Perform this procedure during a maintenance window. Resetting the active control card can cause a service disruption of less then 50 ms to OC-N or DS-N traffic. Resetting the active control card can cause a service disruption of 3 to 5 minutes on all Ethernet traffic due to spanning tree reconvergence if any nodes in the Ethernet circuit are not using Software R4.0 or later.

Caution Do not perform this procedure on a node with live traffic. Hot-swapping the AIP can affect traffic and result in a loss of data. For assistance with AIP replacement contact Cisco TAC (1 800 553-2447).

Caution Always use the supplied electrostatic discharge wristband when working with a powered system. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

You need a #2 Phillips screwdriver.

Procedure

Step 1 Ensure that all nodes in the affected network are running the same software version before replacing the AIP and repairing circuits:

a) In network view, click the **Maintenance** > **Software** tabs. The working software version for each node is listed in the Working Version column.

b) If you need to upgrade the software on a node, refer to the release-specific software upgrade document for procedures. No hardware should be changed or circuit repair performed until after the software upgrade is complete. If you do not need to upgrade software or have completed the software upgrade, proceed to Step 2, on page 401.

Step 2 Record the MAC address of the old AIP:

a) Log into the node where you are replacing the AIP. For login procedures, refer to the Connect the PC and Log into the GUI chapter in the Configuration guide.
b) In node view, click the **Provisioning** > **Network** > **General** tabs.
c) Record the MAC address.

Step 3 Call Cisco TAC (1 800 553-2447) for assistance in replacing the AIP and maintaining the original MAC address.

Step 4 Unscrew the five screws that hold the lower backplane cover in place.

Step 5 Grip the lower backplane cover and gently pull it away from the backplane.

Step 6 Unscrew the two screws that hold the AIP cover in place.

Step 7 Grip the cover and gently pull away from the backplane.

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 8 Grip the AIP and gently pull it away from the backplane.

Step 9 Disconnect the fan-tray assembly power cable from the AIP.

Step 10 Set the old AIP aside for return to Cisco.

Caution The type of shelf the AIP resides in determines the version of AIP that should replace the failed AIP. The 15454-SA-ANSI shelf (P/N: 800-19857) and 15454-SA-HD (P/N: 800-24848) currently use the 5A AIP, (P/N: 73-7665-01). The 15454-SA-NEBS3E, 15454-SA-NEBS3, and 15454-SA-R1 (P/N: 800-07149) shelves and earlier use the 2A AIP (P/N: 73-5262-01).

Caution Do not put a 2A AIP (P/N: 73-5262-01) into a 15454-SA-ANSI (P/N: 800-19857) or 15454-SA-HD (P/N: 800-24848) shelf; doing so causes a blown fuse on the AIP.

Step 11 Attach the fan-tray assembly power cable to the new AIP.

Step 12 Place the new AIP on the backplane by plugging the panel into the backplane using the DIN connector.

Step 13 Replace the AIP cover over the AIP and secure the cover with the two screws.

Step 14 Replace the lower backplane cover and secure the cover with the five screws.

Step 15 In node view, click the **Provisioning** > **Network** tabs.

Caution Cisco recommends control card resets be performed in a maintenance window to avoid any potential service disruptions.

Step 16 Reset the standby control card:

a) Right-click the standby control card and choose **Reset Card**.
b) Click **Yes** in the Resetting Card dialog box. As the card resets, a loading (Ldg) indication appears on the card in CTC.The reset takes approximately five minutes. Do not perform any other steps until the reset is complete.

Step 17 Reset the active control card:

a) Right click the active control card and choose **Reset Card**.
b) Click **Yes** in the Resetting Card dialog box. As the card resets, a Ldg indication appears on the card in CTC. The reset takes approximately five minutes and CTC loses its connection with the node.

Step 18 From the **File** drop-down list, choose Exit to exit the CTC session.

Step 19 Log back into the node. At the Login dialog box, choose **(None)** from the Additional Nodes drop-down list.

Step 20 Record the new MAC address:

a) In node view, click the **Provisioning** > **Network** > **General** tabs.

b) Record the MAC address.

Step 21 In node view, click the **Circuits** tab. Note that all circuits listed are PARTIAL.

Step 22 In node view, choose **Repair Circuits** from the **Tools** drop-down list. The Circuit Repair dialog box appears.

Step 23 Read the instructions in the Circuit Repair dialog box. If all the steps in the dialog box have been completed, click **Next**. Ensure that you have the old and new MAC addresses.

Step 24 The Node MAC Addresses dialog box appears. Complete the following steps:

a) From the Node drop-down list, choose the name of the node where you replaced the AIP.

b) In the Old MAC Address field, enter the old MAC address that was recorded in Step 2, on page 401.

c) Click **Next**.

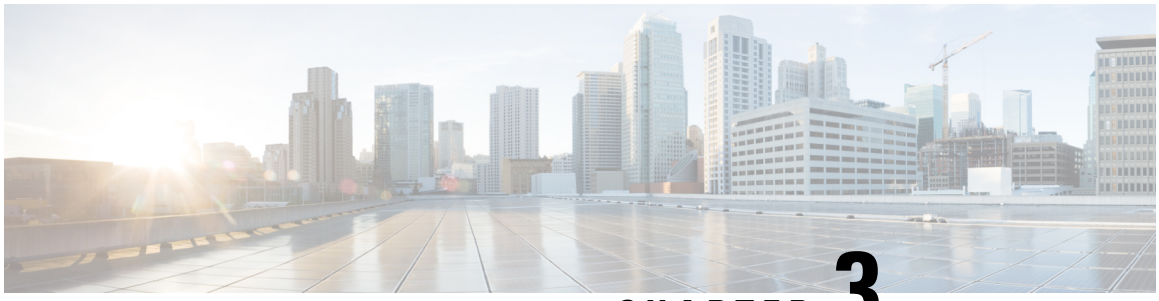
Step 25 The Repair Circuits dialog box appears. Read the information in the dialog box and click **Finish**.

The CTC session freezes until all circuits are repaired. Circuit repair can take up to five minutes or more depending on the number of circuits provisioned on it.

When the circuit repair is complete, the Circuits Repaired dialog box appears.

Step 26 Click **OK**.

Step 27 In the node view of the new node, click the **Circuits** tab. Note that all circuits listed are DISCOVERED. If all circuits listed do not have a DISCOVERED status, call the Cisco TAC (1 800 553-2447) to open a Return Material Authorization (RMA).



CHAPTER 3

Transient Conditions

This chapter gives a description, entity, Simple Network Management Protocol (SNMP) number, and trap for each commonly encountered transient condition.

Alarms can occur even in those cards that are not explicitly mentioned in the Alarm sections. When an alarm is raised, refer to its clearing procedure.

Transients Indexed By Alphabetical Entry

alphabetically lists all transient conditions and their entity, SNMP number, and SNMP trap.

Note The Cisco Transport Controller (CTC) default alarm profile might contain conditions that are not currently implemented but are reserved for future use.

Table 17: Transient Condition Alphabetical Index

Transient Condition	Entity	SNMP Number	SNMP Trap
ADMIN-DISABLE, on page 406	NE	5270	disableInactiveUser
ADMIN-DISABLE-CLR, on page 406	NE	5280	disableInactiveClear
ADMIN-LOCKOUT, on page 406	NE	5040	adminLockoutOfUser
ADMIN-LOCKOUT-CLR, on page 406	NE	5050	adminLockoutClear
ADMIN-LOGOUT, on page 406	NE	5020	adminLogoutOfUser
ADMIN-SUSPEND , on page 406	NE	5340	suspendUser
ADMIN-SUSPEND-CLR, on page 407	NE	5350	suspendUserClear
AUD-ARCHIVE-FAIL, on page 407	EQPT	6350	archiveOfAuditLogFailed
AUTOWDMANS , on page 407	NE	5690	automaticWdmAnsFinished

Transient Condition	Entity	SNMP Number	SNMP Trap
BLSR-RESYNC, on page 407	OCN	2100	blsrMultiNodeTableUpdateCompleted
DBBACKUP-FAIL, on page 407	EQPT	3724	databaseBackupFailed
DBRESTORE-FAIL, on page 407	EQPT	3726	databaseRestoreFailed
EXERCISING-RING , on page 408	OCN	3400	exercisingRingSuccessfully
EXERCISING-SPAN, on page 408	OCN	3410	exercisingSpanSuccessfully
FIREWALL-DIS, on page 408	NE	5230	firewallHasBeenDisabled
FRCDWKSWBK-NO-TRFSW, on page 409	OCN	5560	forceSwitchBackToWorkingResultedInNoTrafficSwitch
FRCDWKSWPR-NO-TRFSW, on page 409	OCN	5550	forceSwitchToProtectResultedInNoTrafficSwitch
INTRUSION , on page 409	NE	5250	securityIntrusionDetUser
INTRUSION-PSWD, on page 409	NE	5240	securityIntrusionDetPwd
IOSCFG-COPY-FAIL, on page 409	—	3660	iosConfigCopyFailed
LOGIN-FAIL-LOCKOUT, on page 410	NE	5080	securityInvalidLoginLockedOutSeeAuditLog
LOGIN-FAIL-ONALRDY, on page 410	NE	5090	securityInvalidLoginAlreadyLoggedOnSeeAuditLog
LOGIN-FAIL-ACL-FAIL, on page 410	NE	10320	securityInvalidLoginAcl
LOGIN-FAILURE-PSWD, on page 410	NE	5070	securityInvalidLoginPasswordSeeAuditLog
LOGIN-FAILURE-USERID, on page 410	NE	3722	securityInvalidLoginUsernameSeeAuditLog
LOGOUT-IDLE-USER, on page 410	—	5110	automaticLogoutOfIdleUser
MASTERKEY-SUCCESS, on page 410	OTU	10045	masterkeySuccess
MANWKSWBK-NO-TRFSW , on page 411	OCN	5540	manualSwitchBackToWorkingResultedInNoTrafficSwitch
MANWKSWPR-NO-TRFSW, on page 411	OCN	5530	manualSwitchToProtectResultedInNoTrafficSwitch
MSSP-RESYNC, on page 411	STMN	4340	msspMultiNodeTableUpdateCompleted
OTDR-HYBRID-SCAN-IN-PROGRESS-RX, on page 296	PPM	9075	otdrHybridScanInProgressRx
OTDR-HYBRID-SCAN-IN-PROGRESS-TX, on page 296	PPM	9070	otdrHybridScanInProgressTx
PM-TCA, on page 411	—	2120	performanceMonitorThresholdCrossingAlert
PS, on page 411	EQPT	2130	protectionSwitch
RMON-ALARM, on page 412	—	2720	rmonThresholdCrossingAlarm
RMON-RESET , on page 412	—	2710	rmonHistoriesAndAlarmsResetReboot
SESSION-TIME-LIMIT, on page 412	NE	6270	sessionTimeLimitExpired

Transient Condition	Entity	SNMP Number	SNMP Trap
SFTWDOWN-FAIL, on page 413	EQPT	3480	softwareDownloadFailed
SPAN-NOT-MEASURED, on page 413	OTS	6440	spanMeasurementCannotBePerformed
SWFTDOWNFAIL, on page 413	EQPT	3480	softwareDownloadFailed
USER-LOCKOUT, on page 413	NE	5030	userLockedOut
USER-LOGIN, on page 413	NE	5100	loginOfUser
USER-LOGOUT, on page 413	NE	5120	logoutOfUser
RESTORE-IN-PROG, on page 412	OCH-TERM	7975	restorationInProg
WKSWBK, on page 413	EQPT, OCN	2640	switchedBackToWorking
WKSWPR, on page 414	2R, TRUNK, EQPT, ESCON, FC, GE, ISC, OCN, STSMON, VT-MON	2650	switchedToProtection
WRMRESTART , on page 414	NE	2660	warmRestart
WTR-SPAN, on page 414	—	3420	spanIsInWaitToRestoreState

Trouble Notifications

The system reports trouble by using standard condition characteristics that follow the rules in Telcordia GR-253 and graphical user interface (GUI) state indicators.

The system 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.

Condition Characteristics

Conditions include any problem detected on a 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 Transaction Language One (TL1).

Note Some cleared conditions are found on the History tab.

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.

Transient Conditions

This section lists in alphabetical order all the transient conditions encountered in Software Release 9.1. The description, entity, SNMP number, and SNMP trap accompany each condition.

ADMIN-DISABLE

The Disable Inactive User (ADMIN-DISABLE) condition occurs when the administrator disables a user or when a account is inactive for a specified period.

This transient condition does not result in a standing condition.

ADMIN-DISABLE-CLR

The Disable Inactive Clear (ADMIN-DISABLE-CLR) condition occurs when the administrator clears the disable flag on a user account.

This transient condition does not result in a standing condition.

ADMIN-LOCKOUT

The Admin Lockout of User (ADMIN-LOCKOUT) condition occurs when the administrator locks a user account.

This transient condition does not result in a standing condition.

ADMIN-LOCKOUT-CLR

The Admin Lockout Clear (ADMIN-LOCKOUT-CLR) condition occurs when the administrator unlocks a user account or when the lockout time expires.

This transient condition does not result in a standing condition.

ADMIN-LOGOUT

The Admin Logout of User (ADMIN-LOGOUT) condition occurs when the administrator logs off a user session.

This transient condition does not result in a standing condition.

ADMIN-SUSPEND

The Suspend User (ADMIN-SUSPEND) condition occurs when the password for a user account expires.

This transient condition does not result in a standing condition.

ADMIN-SUSPEND-CLR

The Suspend User Clear (ADMIN-SUSPEND-CLR) condition occurs when the user or administrator changes the password.

This transient condition does not result in a standing condition.

AUD-ARCHIVE-FAIL

The Archive of Audit Log Failed (AUD-ARCHIVE-FAIL) condition occurs when the software fails to archive the audit log. The condition normally occurs when the user refers to an FTP server that does not exist, or uses an invalid login while trying to archive. The user must log in again with correct user name, password, and FTP server details.

This transient condition does not lead to a standing condition.

AUTOWDMANS

The Automatic WDM ANS Finish (AUTOWDMANS) condition indicates that an automatic node setup (ANS) command has been initiated. It normally occurs when you replace dense wavelength division multiplexing (DWDM) cards; the condition is an indication that the system has regulated the card.

This transient condition does not result in a standing condition.

BLSR-RESYNC

The BLSR Multinode Table Update Completed (BLSR-RESYNC) condition might occur when you create or delete circuits on a bidirectional line switched ring (BLSR) or multiplex section-shared protection ring (MS-SPRing), change a ring topology (for example, add or delete a BLSR/MS-SPRing node), or change the BLSR/MS-SPRing circuit state and ring ID.

This transient condition does not result in a standing condition.

DBBACKUP-FAIL

The Database Backup Failed (DBBACKUP-FAIL) 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 the Cisco Technical Assistance Center (TAC) (1 800 553-2447) for assistance.

DBRESTORE-FAIL

The Database Restore Failed (DBRESTORE-FAIL) 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 the Cisco Technical Assistance Center (TAC) (1 800 553-2447) for assistance.

EXERCISING-RING

The Exercising Ring Successfully (EXERCISING-RING) condition occurs whenever you issue an Exercise Ring command from CTC or TL1. This condition indicates that a command is being executed.

EXERCISING-SPAN

The Exercising Span Successfully (EXERCISING-SPAN) condition occurs whenever you issue an Exercise Span command from CTC or TL1. This condition indicates that a command is being executed.

FIREWALL-DIS

The Firewall Has Been Disabled (FIREWALL-DIS) condition occurs when you provision the firewall to Disabled.

This transient condition does not result in a standing condition.

FIRMWARE-DOWNLOAD

The Firmware Download (FIRMWARE-DOWNLOAD) condition occurs when the firmware is being downloaded during the firmware upgrade. The firmware upgrade initiates when the download is complete.

This transient condition does not result in a standing condition.

FIRMWARE-UPG

The Firmware Upgrade (FIRMWARE-UPG) condition occurs when the firmware is being upgraded. This condition reflects the upgrade status.

This transient condition does not result in a standing condition.

FIRMWARE-UPG-COMPLETE

The Firmware Upgrade Complete (FIRMWARE-UPG-COMPLETE) condition occurs when the firmware upgrade is successfully completed.

This transient condition does not result in a standing condition.

FIRMWARE-UPG-FAIL

The Firmware Upgrade Fail (FIRMWARE-UPG-FAIL) condition occurs when the firmware upgrade fails. The user must start the firmware upgrade again.

This transient condition does not result in a standing condition.

FRCDWKSWBK-NO-TRFSW

The Forced Switch Back to Working Resulted in No Traffic Switch (FRCDWKSWBK-NO-TRFSW) condition occurs when you perform a Force Switch to the working port or card and the working port or card is already active.

This transient condition might result in a Force Switch (Ring or Span) standing condition for a BLSR or MS-SPRing.

FRCDWKSWPR-NO-TRFSW

The Forced Switch to Protection Resulted in No Traffic Switch (FRCDWKSWPR-NO-TRFSW) condition occurs when you perform a Force Switch to the protect port or card, and the protect port or card is already active.

This transient condition does not result in a standing condition.

INC-BOOTCODE

The INC-BOOTCODE (Incompatible Boot Code) condition occurs on the Cisco NCS 2015 chassis:

- When the line card with older boot code is inserted on slots 15 and 16
- When the line card with old boot code is inserted into a slot and the slot generates the same IP address of an existing working card
- When the line cards with old boot code are inserted in the adjacent slots.
- When the two line cards are simultaenously inserted in duplicate IP slots.

Insert the line cards with old boot code in any slot between two and seven to update boot codes. This transient condition does not result in a standing condition.

INTRUSION

The Invalid Login Username (INTRUSION) condition occurs when you attempt to log in with an invalid user ID.

This transient condition does not result in a standing condition.

INTRUSION-PSWD

The Security Intrusion Attempt Detected (INTRUSION -PSWD) condition occurs when you attempt to log in with an invalid password.

This transient condition does not result in a standing condition.

IOSCFG-COPY-FAIL

The Cisco IOS Config Copy Failed (IOSCFG-COPY-FAIL) 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, on page 413, but the IOSCFG-COPY-FAIL condition applies to ML-Series Ethernet cards rather than the control card.

LOGIN-FAIL-LOCKOUT

The Invalid LoginLocked Out (LOGIN-FAIL-LOCKOUT) condition occurs when you attempt to log into a locked account.

This transient condition does not result in a standing condition.

LOGIN-FAIL-ONALRDY

The Security: Invalid LoginAlready Logged On (LOGIN-FAIL-ONALRDY) condition occurs when a user attempts to log into a node where the user already has an existing session and a Single-User-Per-Node (SUPN) policy exists.

This transient condition does not result in a standing condition.

LOGIN-FAIL-ACL-FAIL

The Invalid Log in ACL (LOGIN-FAIL-ACL-FAIL) condition occurs when you attempt to log into an ACL-enabled node with a host IP address that is not part of the allowed IP addresses.

This transient condition does not result in a standing condition.

LOGIN-FAILURE-PSWD

The Invalid LoginPassword (LOGIN-FAILURE-PSWD) condition occurs when you attempt to log in with an invalid password.

This transient condition does not result in a standing condition.

LOGIN-FAILURE-USERID

The Invalid LoginUsername (LOGIN-FAILURE-USERID) condition occurs when a user login 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.

LOGOUT-IDLE-USER

The Automatic Logout of Idle User (LOGOUT-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.

MASTERKEY-SUCCESS

The Master Key Exchange Success condition occurs when the primary key is successfully reset and the Threshold Crossing Alert (TCA) has provisioned.

This transient condition does not result in a standing condition.

MANWKSWBK-NO-TRFSW

The Manual Switch Back To Working Resulted in No Traffic Switch (MANWKSWBK-NO-TRFSW) condition occurs when you perform a Manual switch to the working port or card and the working port or card is already active.

This transient condition does not result in a standing condition.

MANWKSWPR-NO-TRFSW

The Manual Switch to Protect Resulted in No Traffic Switch (MANWKSWPR-NO-TRFSW) condition occurs when you perform a Manual switch to the protect port or card and the protect port or card is already active.

This transient condition results in a BLSR or MSSP Manual Switch (Span or Ring) standing condition.

MCAST-MAC-ALIASING

This condition is raised when there are multiple L3 addresses that map to the same L2 address in a VLAN.

MSSP-RESYNC

The MS-SPRing Multi-Node Table Update Completed (MSSP-RESYNC) condition occurs when a node receives all relevant information such as payload, path state, Routing Information Protocol (RIP), cross-connect tables, and cross-connect VT tables from the other nodes in the ring. This condition is raised on all nodes in the ring while a node is added or a circuit is provisioned. This transient condition will not be cleared and is seen in the History tab of CTC.

You must check this condition on all the nodes and then remove the Forced Ring Switch commands.

PM-TCA

The Performance Monitoring Threshold Crossing Alert (PM-TCA) condition occurs when network collisions cross the rising threshold for the first time.

PS

The Protection Switch (PS) condition occurs when traffic switches from a working/active card to a protect/standby card.

REP-PRI-EDGE-ELECTED

The REP-PRI-EDGE-ELECTED condition occurs in GE_XP and 10GE_XP cards when the primary edge port is elected in a segment. The condition is raised on the primary REP port.)

REP-SEC-EDGE-ELECTED

The REP-SEC-EDGE-ELECTED condition occurs in GE_XP and 10GE_XP cards when the secondary edge port is elected in a segment. The condition is raised on the primary REP port.

REP-STCN-GENERATED

The REP-STCN-GENERATED condition occurs in GE_XP and 10GE_XP cards on an edge port with STCN segment or port provisioning after a topology change in the REP segment. The condition is raised on the edge port of the segment.

REP-VLB-ACTIVATED

The REP-VLB-ACTIVATED condition occurs in GE_XP and 10GE_XP cards when VLB is already provisioned on the primary edge, and activation is triggered. The condition is raised on the primary edge port of the segment.

REP-VLB-TRIG-DELAY

The REP-VLB-TRIG-DELAY condition occurs in the GE_XP and 10GE_XP cards when the VLB trigger delay timer is started on the primary edge port. The condition is raised on the primary edge port of the segment.

RESTORE-IN-PROG

The Restoration in Progress (RESTORE-IN-PROG) condition occurs when the WSON initiates a path switch during a restoration of a GMPLS circuit. This condition demotes all outstanding alarms on the path across the entire network. The condition is cleared after a timeout of five minutes.

RMON-ALARM

The Remote Monitoring Threshold Crossing Alarm (RMON-ALARM) condition occurs when the remote monitoring (RMON) variable crosses the threshold.

RMON-RESET

The RMON Histories and Alarms Reset Reboot (RMON-RESET) condition occurs when the time-of-day settings on the control card are increased or decreased by more than five seconds. This invalidates all the history data, and RMON must restart. It can also occur when you reset a card.

SESSION-TIME-LIMIT

The Session Time Limit Expired (SESSION-TIME-LIMIT) condition occurs when a login session exceeds the time limit and you are logged out of the session. You must log in again.

SFTWDOWN-FAIL

The Software Download Failed (SFTDOWN-FAIL) condition occurs when the system fails to download the required software package.

An incorrect input that points to the wrong place or file, network issues, or a bad (corrupt) software package can cause this failure. If the software package is corrupt, contact the Cisco Technical Assistance Center (TAC) (1 800 553-2447) for assistance.

SPAN-NOT-MEASURED

The SPAN-NOT-MEASURED condition is raised when a node cannot perform the span loss verification as it cannot communicate with its peer at the other end of the span.

SWFTDOWNFAIL

The Software Download Failed (SFTDOWN-FAIL) 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 the Cisco Technical Assistance Center (TAC) (1 800 553-2447) for assistance.

USER-LOCKOUT

The User Locked Out (USER-LOCKOUT) 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.

USER-LOGIN

The Login of User (USER-LOGIN) occurs when you begin a new session by verifying your user ID and password.

This transient condition does not result in a standing condition.

USER-LOGOUT

The Logout of User (USER-LOGOUT) condition occurs when you stop a login session by logging out of your account.

This transient condition does not result in a standing condition.

WKSWBK

The Switched Back to Working (WKSWBK) condition occurs when traffic switches back to the working port or card in a nonrevertive protection group.

This transient condition does not result in a standing condition.

WKSWPR

The Switched to Protection (WKSWPR) condition occurs when traffic switches to the protect port or card in a nonrevertive protection group.

This transient condition does not result in a standing condition.

WRMRESTART

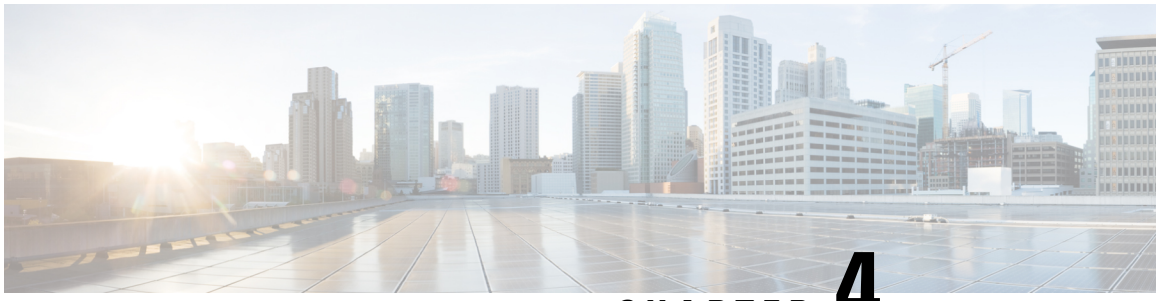
The Warm Restart (WRMRESTART) condition occurs when the node restarts while it is powered up. A restart can be caused by provisioning, such as a database restore or IP changes, or by software defects. A WRMRESTART is normally accompanied by MANRESET or AUTORESET to indicate whether the reset was initiated manually (MAN) or automatically (AUTO).

This is the first condition that appears after a control card is powered up. The condition changes to COLD-START if the control card is restarted from a physical reseat or a power loss.

WTR-SPAN

The Span is in Wait To Restore State (WTR-SPAN) condition occurs when a BLSR or MS-SPRing switches to another span due to a Signal Failure-Span command or a fiber is pulled from a four-fiber BLSR/MS-SPRing configuration. The condition is raised until the WaitToRestore (WTR) period expires.

This transient condition clears when the BLSR/MS-SPRing returns to a normal condition or the IDLE state.

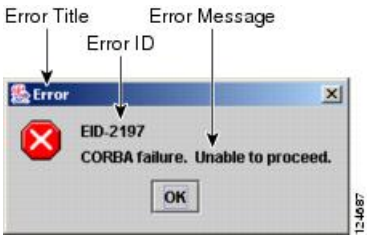


CHAPTER 4

Error Messages

This chapter lists the error messages for the Cisco NCS Platform. The error dialog box in Figure 24: Error Dialog Box, on page 415 consists of three parts: the error title, error ID, and error message.

Figure 24: Error Dialog Box



Error Messages Reference

Table 18: Error Messages, on page 415 gives a list of all error or warning message numbers, the messages, and a brief description of each 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 that 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.

The WSON error messages gives a list of all the WSON error messages and a brief description of each message.

Table 18: Error Messages

Error/Warning ID	Error/Warning Message	Description
EID-0	Invalid error ID.	The error ID is invalid.
EID-1	A null pointer encountered in {0}.	Cisco Transport Controller (CTC) encountered a null pointer in the area described by the specified item.

Error/Warning ID	Error/Warning Message	Description
EID-1000	The host name of the network element cannot be resolved to an address.	Refer to the error 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 the error 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 specified JAR file is incorrect.
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 specified JAR file.
EID-1018	Password shall not contain the associated user-ID.	The password is invalid.
EID-1019	Could not create {0}. Please enter another filename.	CTC could not create the file due to an invalid filename.
EID-1020	Fatal exception occurred, exiting CTC. 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}.	CTC was unable to display the requested view (node or network).
EID-1022	An IOS 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. Please try again later.	Refer to the error message text.

Error/Warning ID	Error/Warning Message	Description
EID-1023	This IOS session has been terminated. Terminations are caused when the session has timed out, the card resets, there is already a session with the slot, or password configuration is required.	Refer to the error message text.
EID-1025	Unable to create Help Broker.	CTC was unable to create the help broker for the online help.
EID-1026	Error found in the Help Set file.	CTC encountered an error in the online help file.
EID-1027	Unable to locate help content for Help ID: "{0}".	CTC was unable to locate the content for the help ID.
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 the 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 the error message text.
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 the 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 the warning message text.
EID-1037	Could not open {0}. Please enter another filename.	Invalid file name. CTC is unable to open the specified file. Ensure that the file exists and the filename was typed correctly.
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 the error message text.
WID-1041	An error occurred while closing the {0} connection.	CTC encountered an error while closing the specified connection.

Error/Warning ID	Error/Warning Message	Description
WID-1042	You have selected Java version {0}. This version is outside of the recommended range and may cause an unpredictable behavior of the software. Do you wish to continue?	Refer to the warning message text.
EID-1043	Error writing to file: {0}. This might be caused by a directory permission, quota or disk volume full issue.	Check for possible causes and try again.
WID-1044	Warning: there is a discrepancy in the build timestamp between the NE cached jar file ({0}) and the NE ({1}). Your CTC jar cache should be emptied.	Refer to the warning message text.
EID-1046	Selected CTC version ({0}) must be greater than or equal{to the login NE version ({1}).	The CTC software version must be greater than or equal to the software version on the node being managed.
EID-1047	No additional Pseudo IOS windows may be opened at this time. The maximum number of Pseudo IOS windows are open.	Refer to the error message text.
EID-1048	This Pseudo IOS connection has been terminated. Terminations are caused when the session has timed out, the node resets, or when the exit command has been invoked. This may also occur when the maximum number of concurrent Pseudo IOS connections has been reached.	Refer to the error message text.
EID-1049	A Pseudo IOS connection cannot be opened right now on this node. Please try again later.	Refer to the error message text.
EID-1050	Connection failed on node {0}	Refer to the error message text.
EID-2001	No rolls were selected. {0}	No rolls were selected for the bridge and roll.
EID-2002	The roll must be completed or canceled before it can be deleted.	You cannot delete the roll unless it has been completed or canceled.
EID-2003	An error occurred while deleting the roll. {0}	There was an error when CTC tried to delete the roll.
EID-2004	No Cisco IOS slot was selected.	You did not select a Cisco IOS slot.
EID-2005	CTC cannot find the online help files for {0}. The files might have been moved, deleted, or not installed. To install online help, run the setup program on the software CD.	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 CD.

Error/Warning ID	Error/Warning Message	Description
EID-2006	An error occurred while editing the circuit(s). {0} {1}.	An error occurred when CTC tried to open the circuit for editing.
EID-2007	The preferences could not be saved.	CTC cannot save the preferences.
EID-2008	The circuit preferences could not be saved: {0}	CTC cannot find the file needed to save the circuit preferences.
EID-2009	CTC was unable to download the package: {0}	Refer to the error message text.
EID-2010	An error occurred while deleting the destination.	CTC could not delete the destination.
EID-2011	The circuit could not be destroyed.	CTC could not destroy the circuit.
EID-2012	The reverse circuit could not be destroyed.	CTC could not reverse the circuit destroy.
EID-2013	The circuit creation failed. The circuit creation cannot proceed due to changes in the network which affected the circuit(s) being created. The dialog box will close. Please try again.	Refer to the error message text.
EID-2014	No circuit(s) were selected. {0}	You must select a circuit to complete this function.
EID-2015	The circuit {0} cannot be deleted because it has one or more rolls.	You must delete the rolls in the circuit before deleting the circuit itself.
EID-2016	The circuit deletion failed.	CTC could not delete the tunnel as there are circuits that use the tunnel.
EID-2017	An error occurred while mapping the circuit. {0}	There was an error mapping the circuit.
EID-2018	The circuit roll failed. The circuit must 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	The circuit roll failed. Bridge and roll is not supported on DWDM circuits.	Refer to the error message text.
EID-2020	The circuit roll failed. The two circuits must have the same direction.	Refer to the error message text.
EID-2021	The circuit roll failed. The two circuits must have the same size.	Refer to the error message text.
EID-2022	The circuit roll failed. A maximum of two circuits can be selected for a bridge and roll operation.	Refer to the error message text.
EID-2023	CTC was unable to create a new user account.	Refer to the error message text.

Error/Warning ID	Error/Warning Message	Description
EID-2024	An error occurred during node selection.	There was an error during node selection.
EID-2025	This feature cannot be used. Verify that each endpoint of this circuit is running software that supports this feature.	Refer to the error or warning message text. For example, this error is generated from the node view Provisioning> WDM-ANS> tabs to indicate that the selected ring type is not supported by the endpoints of the circuit. Another example is the Provisioning> VLAN tabs in card view (Ethernet card only), where it indicates that the back-end spanning tree protocol (STP) disabling is not supported.
EID-2026	The {0} request could not be applied. {1}	Error occurred while attempting to switch a path protection circuit away from a span.
EID-2027	An error occurred while deleting the circuit drop.	CTC could not delete the circuit drop.
EID-2028	An error occurred while removing the 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	An error occurred during provisioning.	There was an error during provisioning.
EID-2031	An error occurred while adding the node.	There was an error while adding a node.
EID-2032	The circuit could not be renamed. {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	Network circuits could not be added: {0}	Refer to the error message text.
EID-2035	The source and destination nodes are not connected.	Refer to the error message text.
EID-2036	The {0} cannot be deleted. 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.

Error/Warning ID	Error/Warning Message	Description
EID-2037	The attribute for {0} cannot be found.	CTC cannot find an attribute for the specified item.
EID-2038	The protection operation is invalid.	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 the 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 the error message text.
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 the error message text.
EID-2047	Please enter a valid value for the slot number.	There was an error due to an invalid slot number.
EID-2048	Please enter a valid value for the port number.	There was an error due to an invalid port number.
EID-2050	The new circuit could not be destroyed.	CTC could not destroy the new circuit.
EID-2051	The circuit cannot be downgraded. {0}	The specified circuit cannot be downgraded.
EID-2052	An error occurred during circuit processing.	There was an error during the circuit processing.
EID-2054	An error occurred while selecting an endpoint.	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 combination boxes.

Error/Warning ID	Error/Warning Message	Description
EID-2056	A communication error occurred: {0}	An internal error occurred in Network Alarm tab while synchronizing alarms with the nodes.
EID-2059	An error occurred while deleting the node. {0}	There was an error during the node deletion.
EID-2060	No PCA circuits were found.	CTC could not find any protection channel access (PCA) circuits for this task.
EID-2061	An error occurred while provisioning the VLAN.	There was an error defining the VLAN.
EID-2062	An error occurred while deleting VLANs. No VLAN(s) were selected. Please select a VLAN.	Refer to the error message text.
EID-2063	The default VLAN cannot be deleted.	The selected VLAN is the default VLAN and cannot be deleted.
EID-2064	An error occurred while deleting VLANs. {0}	There was an error deleting the specified VLAN.
EID-2065	The profile cannot be imported. The profile "{0}" exists in the editor and the maximum number of copies (ten) exists in the editor. The import will be canceled. The profile has already been loaded eleven times.	Cannot import the profile because the profile has reached the maximum number of copies in the editor.
EID-2066	The profile could not be stored. An error occurred while writing to {0}.	CTC encountered an error while trying to store the profile.
EID-2067	An error occurred while writing to the file. {0}	CTC encountered an error while writing the specified file.
EID-2068	The alarm profile could not be loaded from the node.	CTC encountered an error trying to load the alarm profile from the node.
EID-2069	The file could not be found or an I/O exception occurred. {0}	Either the specified file was not found, or there was an input/output exception.
EID-2070	The profile could not be deleted. {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 cannot be removed.	You cannot delete a permanent column.

Error/Warning ID	Error/Warning Message	Description
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 cannot be reset.	A permanent column cannot be reset.
EID-2077	This column is permanent and cannot be renamed.	You cannot rename a permanent column.
EID-2078	At least two columns must be highlighted.	You cannot compare two profiles unless you select two columns.
EID-2079	The alarm types cannot be loaded into table. There are no reachable nodes from which the list of alarm types can be loaded. Please wait until such a node is reachable and try again.	Refer to the error message text.
EID-2080	The node {0} has no profiles.	The specified node does not have any profiles.
EID-2081	An error occurred while removing profile {0} from the node {1}.	There was an error while removing the specified profile from the specified node.
EID-2082	The profile {0} does not exist on the node {1}.	CTC cannot find the specified profile from the specified node.
EID-2083	An error occurred while adding profile {0} to the node {1}.	There was an error adding the specified profile to the specified node.
EID-2085	The profile selection is invalid. No profiles were selected.	You tried to select an invalid profile. Select another profile.
EID-2086	The node selection is invalid. 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 the error message text.
EID-2088	The profile name is invalid.	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 were 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 the node {0}.	CTC is unable to switch to the specified node.
EID-2092	A general exception error occurred.	CTC encountered a general exception error while trying to complete the task.

Error/Warning ID	Error/Warning Message	Description
EID-2093	The name is too short. It does not have enough characters. {0}	The name must have a minimum of six characters.
EID-2094	The password and confirmed password fields do not match.	You must make sure the two fields have the same password.
EID-2095	The password is invalid. {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 was specified.	You did not specify a user name.
EID-2099	An error occurred while ring switching.	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	An error occurred while protection switching.	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	An error occurred while upgrading the span.	There was an error during the span upgrade.
EID-2104	The circuits cannot be switched back because 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	An error occurred while adding {0}. The host is unknown.	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	The extension byte for the ring cannot be set. {0}	CTC cannot set the BLSR/MS-SPRing extension byte.

Error/Warning ID	Error/Warning Message	Description
EID-2114	A card communication failure occurred during the operation.	This error can occur during an attempt to apply a BLSR protection operation to a line.
EID-2115	An error occurred during the operation. {0}	There was an error in applying the specified operation.
EID-2116	The extension byte setting for the ring is invalid. {0}	The extension byte set for the specified ring is invalid.
EID-2118	The ring cannot be deleted. A protection operation is set. All protection operations must be clear for ring to be deleted.	Clear all the protection operations for the ring before deleting it.
EID-2119	{0} cannot be deleted because a protection switch is in effect. Please clear any protection operations, ensure 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 {0} 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	The ring cannot be upgraded. {0}	CTC cannot upgrade the specified ring.
EID-2122	The ring speed for is inadequate for the upgrade procedure. Only {0} (or higher) {1} can be upgraded to four-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 two-fiber {0}. The ports cannot serve as timing references, 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. 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 the 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 the error message text.
EID-2126	An error occurred while provisioning the OSPF area. {0}	There is an Open Shortest Path First (OSPF) area error.

Error/Warning ID	Error/Warning Message	Description
EID-2127	You cannot add this span. It would cause the following circuit(s) to occupy different {0} regions on different spans: {1} 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	The state is invalid.	An internal error occurred while trying to remove a span from a BLSR. This alarm occurs in the network-level BLSR creation dialog box.
EID-2129	You cannot use same slot for east and west protect ports.	Refer to the 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	The reversion cannot be set to INCONSISTENT.	You must select another reversion type.
EID-2135	The overhead circuit preferences could not be stored: {0}	Input/Output error. Unable to store overhead circuit preferences.
EID-2137	An error occurred during the circuit merge. {0}	There was an error while merging the circuits.
EID-2138	Not all destinations could be deleted. Please try again.	Refer to the error message text.
EID-2139	An error occurred while updating the destinations.	There was an error in updating the circuit destinations.
EID-2143	No online help version was selected. The online help book cannot be deleted.	Select the version of online help, and proceed.
EID-2144	An error occurred while deleting the online help book(s). {0}	You cannot delete the specified online help.
EID-2145	No nodes appear to have a Cisco IOS card.	Refer to error message.
EID-2146	This is a security violation. You may only logout of your own account.	You cannot logout of an account other than your own.
EID-2147	This is a security violation. You may only change your own account.	You cannot change an account other than your own.
EID-2148	This is a security violation. You cannot delete the account under which you are currently logged in.	You cannot delete the account you are currently logged in.
WID-2149	There is no exportable content in this view.	Refer to the error message text.

Error/Warning ID	Error/Warning Message	Description
WID-2150	The 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 the warning message text.
WID-2153	Adding this drop will make the circuit a PCA circuit.	Refer to the warning message text.
WID-2154	Monitor circuits cannot be created on a port grouping circuit.	Refer to the warning message text.
WID-2155	Switch counts might not be fully supported on some nodes. {0}	The specified nodes do not support switch counts completely.
WID-2156	The 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 the warning message text.
WID-2157	The roll(s) cannot be completed. {0}	CTC could not complete the roll because the roll is destroyed, in an incomplete state, in a TL1_roll state, is canceled, or is not ready to complete.
EID-2158	The roll mode is invalid. {0}	There are two roll modes: auto and manual. For a one-way circuit source roll, the roll mode must be auto and for a one- way circuit destination roll, the roll mode must be manual.
EID-2159	The roll is not ready for completion. {0}	The roll is not ready for completion.
EID-2160	The roll is not connected. {0}	Refer to error message text.
EID-2161	The sibling roll is not complete. {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 a 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	An error occurred during roll acknowledgment. {0}	Refer to the error message text.
EID-2163	The roll cannot be canceled. {0}	CTC cannot cancel the roll.
EID-2164	An error occurred during the roll. {0}	CTC encountered a roll error.

Error/Warning ID	Error/Warning Message	Description
WID-2165	The MAC address of the 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	The node cannot be inserted into the domain because it is not initialized.	Initialize the node and proceed.
WID-2167	You have insufficient security privileges to perform this action.	You do not have the privilege to perform this action.
WID-2168	The following warnings surfaced while 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 the profile. {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 the 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	The port is unavailable. The desired CTC CORBA ({0}) listener port, {1}, 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	An invalid number was entered. Please check it and try again.	You entered an invalid firewall port number. Try again.
WID-2175	An extension byte mismatch occurred. {0}	There is a mismatch with the extension byte.
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 the warning message text.
WID-2178	Only one edit pane can be opened at a time. The existing pane will be displayed.	Refer to the warning message text.
WID-2179	No update is available because the circuit has been deleted.	Refer to the warning message text.

Error/Warning ID	Error/Warning Message	Description
EID-2180	The CTC initialization failed during step {0}.	CTC initialization has failed in the specified step.
EID-2181	This link cannot be included because 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	The circuit roll failed. Bridge and roll is not supported on VCAT circuits.	Refer to the error message text.
EID-2184	Spanning Tree Protocol cannot be enabled on some ports because the ports have been assigned an incompatible list of VLANs. You can view the VLAN/Spanning Tree table or reassign the Ethernet port VLANs.	Refer to the error message text.
EID-2185	The VLANs on some ports cannot be assigned because they are incompatible with the Spanning Tree Protocol. You can view the VLAN/Spanning Tree table or reassign the VLANs.	Refer to the error message text.
EID-2186	The software download failed on node {0}.	The software could not be downloaded onto the specified node.
EID-2187	The ring name cannot exceed {0} characters. 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	The TL1 keyword "all" cannot be used as the ring name. Please provide another name.	Refer to the 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	The ring name must not be empty.	You must supply a ring name.
EID-2192	A valid route cannot be found for the circuit creation request.	CTC could not complete the circuit creation request either because there are no physical links, or the bandwidth of the available links are already reserved.
EID-2193	A valid route cannot be found for the circuit drop creation request.	Refer to the error message text.

Error/Warning ID	Error/Warning Message	Description
EID-2194	A valid route cannot be found for the roll creation request.	Refer to the 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 the error message text.
EID-2196	CTC cannot be relaunched. {0}	There is an error relaunching CTC.
EID-2197	A CORBA failure occurred. CTC cannot proceed.	There was a CORBA failure, and the task cannot proceed. Verify the Java version.
EID-2198	CTC is 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 the error message text.
EID-2202	An intra-node DRI circuit must have two sources.	Intranode circuit must have two sources to be a dual ring interconnect (DRI).
EID-2203	No member was selected.	You must select a member.
EID-2204	The number of circuits must be a positive integer.	The number of circuits cannot be zero or negative.
EID-2205	The circuit type must be selected.	You must select a circuit type.
EID-2206	The profile cannot be autoselected. Please select profile(s) to store and try again.	Refer to the error message text.
EID-2207	You cannot add this span. Either the ring name is too long (that is, 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 alphanumeric 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 was selected.	You must select a package name.

Error/Warning ID	Error/Warning Message	Description
EID-2211	No node was selected for upgrade.	You must select a node for the upgrade.
EID-2212	A 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 until the node reconnects.	Refer to the error message text.
EID-2215	An error occurred while leaving the {0} page.	There was an error while leaving the specified page.
EID-2216	An error occurred while entering the {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 the error message text.
EID-2218	The bandwidth must be between {0} and {1} percent.	The bandwidth must be within the specified parameters.
EID-2219	The protection operation failed. An XC loopback was applied on the 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 is not able to change it. Please try again later.	Refer to the error message text.
EID-2221	A valid route cannot be found for the unprotected to {0} upgrade request.	Refer to the error message text.
EID-2222	One or more of the following nodes are currently part of a four-fiber {0}. Only a single four-fiber {0} is supported per node. {1}	The nodes, specified by {1}, are already part of a 4-fiber BLSR/MS-SPRing type (specified by {0}).
EID-2223	Only one circuit can be upgraded at a time.	Refer to the error message text.
EID-2224	This link may not be included because it terminates on the source.	Refer to the error message text.
EID-2225	A valid signal could not be detected 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	The circuit roll failed. {0}	Refer to the error message text.

Error/Warning ID	Error/Warning Message	Description
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	An error occurred while deleting member circuits. {0}	Refer to the error message text.
WID-2322	Not all cross-connects from selected circuits could be merged into the current circuit. They might appear as partial circuits.	Refer to the warning message text.
EID-2323	The circuit roll failed. Bridge and roll is not supported on monitor circuits.	A monitor circuit does not support Bridge and Roll.
EID-2324	An error occurred during the circuit upgrade. {0}	Refer to the 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, the selected circuits must be upgraded. Is it OK to upgrade the selected circuits and continue the bridge and roll operation?	Refer to the 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, the selected circuits must be upgraded. Is it OK to upgrade the selected circuits and continue the bridge and roll operation?	Refer to the warning message text.
EID-2328	An error occurred during the circuit reconfiguration. {0}	The attempt to reconfigure the specified circuit has failed.
EID-2329	{0} of {1} circuits could not be successfully created.	A few circuits could not be created.
EID-2330	An error occurred during circuit verification. The selected {0} is invalid! {1}	The selected item, specified by {0}, is invalid as per the details, specified in {1}.
EID-2331	Deleting {0} might be service affecting.	Deleting the item can affect the service of CTC.
EID-2332	A validation error occurred in row {0}. {1} hold-off timer for {2} must be between {3}-10,000 ms, in steps of 100 ms.	Refer to the error message text.
EID-2333	The SSLIOP port cannot have the same port value as IIOP port. Please change it and apply again.	Refer to the 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.

Error/Warning ID	Error/Warning Message	Description
EID-3002	An error occurred while retrieving defaults from the node: {0}	There was an error while retrieving the defaults from the specified node.
EID-3003	The file {0} cannot be loaded.	CTC cannot load the specified file.
EID-3004	Properties cannot be loaded from the node.	Refer to the error message text.
EID-3005	NE update properties cannot be saved to the file {0}.	CTC cannot save the network element (NE) update values to the specified file.
EID-3006	NE update properties cannot be loaded from the node.	Refer to the error message text.
EID-3007	An error occurred while provisioning the {0}.	There was a provisioning error for the specified item.
EID-3008	This is 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} was selected.	Select the specified item, for example, VLAN, port, slot, etc.
EID-3010	A bidirectional optical link could not be created.	Refer to the error message text.
EID-3016	The subnet address is invalid.	Refer to the error message text.
EID-3017	The subnet address already exists.	Refer to the error message text.
EID-3019	The internal subnet address is incomplete.	Enter the complete internal subnet address.
EID-3020	The subnet address cannot be the same for both TSC cards. The requested action is not allowed.	A node internal subnet must be different from one another as each TSC is on separate Ethernet buses, isolated by broadcast domains.
EID-3021	An error occurred while retrieving the diagnostics: {0}	Refer to the error message text.
EID-3022	The requested action is not allowed.	The requested action is not allowed.
EID-3023	The low order cross-connect mode could not be retrieved.	Refer to the error message text.
EID-3024	The {0} cross-connect mode could not be switched. 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.

Error/Warning ID	Error/Warning Message	Description
EID-3025	An error occurred while retrieving thresholds.	There was an error retrieving the thresholds.
EID-3026	The send DoNotUse attribute cannot be modified.	You cannot modify the Send DoNotUse field.
EID-3027	The SyncMsg attribute cannot be modified.	You cannot modify the SyncMsg field.
EID-3028	The port type cannot be changed.	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 the error message text.
EID-3031	An error occurred while hard-resetting the card.	There was an error while resetting card hardware.
EID-3032	An error occurred while resetting the card.	There was an error while resetting the card.
EID-3033	The lamp test is not supported on this shelf.	Refer to the error message text.
EID-3035	The cross-connect diagnostics cannot be performed	Refer to the 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-3039	An error occurred while changing the card type.	There was an error while changing the card.
EID-3040	The card type is invalid.	The selected card type is invalid.
EID-3041	An error occurred while 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.
EID-3042	The flow control low value must be less than the flow control high value for all ports in the card.	Refer to the error message text.
EID-3046	The flow control watermark value must be between {0} and {1}, inclusive.	The flow control watermark value must be between the two specified values.
EID-3047	The file {0} could not be read. Please verify the name and try again.	Refer to the error message text.
EID-3048	There is no Cisco IOS startup configuration file available to download.	CTC could not find the configuration file for IOS startup.
EID-3049	The download cannot be done at this time because an update in progress.	Refer to the error message text.

Error/Warning ID	Error/Warning Message	Description
EID-3050	An error occurred while trying to save the file to your local file system.	Check whether the file already exists and cannot be over written, or there is a space constraint in the file system.
EID-3051	The configuration file has a maximum size of {0} bytes.	The size of the configuration file should not exceed the specified number of bytes.
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	The provisioned input/output ports cannot be removed or another user is updating the card. Please try to remove these ports later.	Another user may be updating the card. You can try again later.
EID-3055	The soak maintenance pane cannot be created.	Refer to the error message text.
EID-3056	Defaults cannot be saved to the file {0}.	CTC cannot save the defaults to the specified file.
EID-3057	Default properties cannot be loaded from the node.	Refer to the error message text.
EID-3058	The file {0} does not exist.	Refer to the error message text.
EID-3059	An error occurred 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	An error occurred while setting values in the table.	Refer to the error message text.
EID-3064	This is not a G1000 card.	This card is not a G1000-4 card.
EID-3065	An error occurred while attempting to create this RMON threshold: {0}	You must wait some time before you try again.
EID-3066	The sample period must be between 10 and {0}.	Refer to the error message text.
EID-3067	The rising threshold must be between 1 and {0}.	This is an invalid rising threshold entry. The valid range is from 1 to the specified value.
EID-3068	The falling threshold must be between 1 and {0}.	This is an invalid falling threshold entry. The valid range is from 1 to the specified value.

Error/Warning ID	Error/Warning Message	Description
EID-3069	The rising threshold must be greater than or equal to the falling threshold.	Refer to the 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	An error occurred while retrieving the learned address list.	Unable to retrieve the learned MAC address from the NE.
EID-3072	An error occurred while clearing the learned address.	Failure attempting to clear the learned MAC address from a specific card or Ether group.
EID-3073	An error occurred while clearing the selected rows.	Failure attempting to clear the learned MAC address from a specific card or Ether group.
EID-3074	An error occurred while clearing the learned address list 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 the parameter column must be selected.	Refer to the error message text.
EID-3076	CTC lost its connection with this node. The NE Setup Wizard will exit.	Refer to the error message text.
EID-3077	No optical link was selected.	Refer to the error message text.
EID-3078	An optical link could not be created.	Refer to the error message text.
EID-3079	Defaults cannot be applied to the node. {0}	CTC cannot apply the defaults to the specified node.
EID-3080	CTC cannot navigate to the target tab. {0}	CTC cannot go to the specified target tab.
EID-3081	The port type cannot be changed.	Refer to the error message text.
EID-3082	The {0} extension byte cannot be changed.	You cannot modify the specified extension byte.
EID-3084	An error occurred while retrieving 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 were selected	Select an OSC termination and proceed.

Error/Warning ID	Error/Warning Message	Description
EID-3086	One or more Osc terminations could not be created.	Refer to the error message text.
EID-3087	The OSC termination could not be edited.	Refer to the error message text.
EID-3088	No {0} card is present to switch.	No card of the specified type is available to switch.
EID-3089	The {0} state cannot be used or changed when the {1} has failed or is missing.	You cannot use or change the specified state when the card is failed or missing.
EID-3090	The operation cannot be performed because the {0} is {1}LOCKED_ON/LOCKED_OUT.	You cannot perform operation.
EID-3091	The operation cannot be performed because the protect card is active.	Refer to the error message text.
EID-3092	The requested action cannot be applied because the service state is invalid.	Select another service state and proceed.
EID-3093	The operation cannot be performed because the duplex pair is {0}locked.	Refer to the error message text.
EID-3094	The operation cannot be performed because no cross-connect redundancy is available.	You cannot perform the requested operation on the cross connect card without having a backup cross connect card.
EID-3095	The deletion failed because the circuit is in use	Refer to the error message text.
WID-3096	An internal communication error was encountered while retrieving 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 the 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 were selected.	Select one of the ring terminations.
EID-3099	The entered key does not match the existing authentication key.	Check the authentication key and reenter.
EID-3100	An error occurred during authentication.	There was an error in authentication. Verify that the key does not exceed the character limit.
EID-3101	The DCC metric must be between 1 and 65535.	The DCC metric should be in the range of 1 to 65535.
EID-3102	The DCC metric is invalid.	There was an invalid DCC metric.

Error/Warning ID	Error/Warning Message	Description
EID-3103	The IP address {0} is invalid}.	The IP address is invalid.
EID-3104	The router priority must be between 0 and 255.	The router priority should be in the range of 0 to 255.
EID-3105	The router priority is invalid.	The router priority is invalid.
EID-3106	The hello interval must be between 1 and 65535.	The hello interval should be in the range of 1 to 65535.
EID-3107	The hello interval is invalid.	The hello interval is invalid.
EID-3109	The dead interval must be between 1 and 2147483647.	The dead interval value must be between 1 and 2147483647.
EID-3110	The dead interval must be larger than the hello interval.	Refer to the error message text.
EID-3111	The LAN transmit delay must be between 1 and 3600 seconds.	The LAN transit delay should be in the range of 1 to 3600 seconds.
EID-3112	The transmit delay is invalid.	The transmit delay is invalid.
EID-3113	The retransmit interval must be between 1 and 3600 seconds.	The retransmit interval should be in the range of 1 to 3600 seconds.
EID-3114	The retransmit interval is invalid.	The retransmit interval is invalid.
EID-3115	The LAN metric must be between 1 and 65535.	The LAN metric should be in the range of 1 to 65535.
EID-3116	The LAN metric is invalid.	The LAN metric is invalid.
EID-3117	If OSPF is active on the 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 the error message text.
EID-3118	If OSPF is active on the LAN, the LAN area ID cannot be the same as the DCC area ID.	LAN must be part of a different OSPF area other than the DCC network.
EID-3119	An error occurred during validation.	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} was selected for deletion.	Choose an object of the specified type to delete.
EID-3121	An error occurred while deleting {0}.	There is an error deleting the item.

Error/Warning ID	Error/Warning Message	Description
EID-3122	No object of type {0} was selected to edit.	Choose an object of the specified type to edit.
EID-3123	An error occurred while editing {0}.	There was an error editing the item.
EID-3124	The {0} termination is in use. Delete the associated OSPF range table entry and try again.	Refer to the error message text.
EID-3125	No {0} terminations were selected.	No specified terminations are selected.
EID-3126	The {0} termination could not be edited.	CTC could not edit the specified termination.
EID-3127	Orderwire cannot be provisioned because the E2 byte is in use by {0}.	Refer to the error message text.
EID-3128	The authentication key cannot exceed {0} characters.	The authentication key cannot exceed the specified number of characters.
EID-3129	The authentication keys do not match!	Refer to the error message text.
EID-3130	An error occurred while creating the OSPF area virtual link.	CTC encountered an error while creating the area virtual link.
EID-3131	An error occurred while creating the OSPF virtual link.	CTC encountered an error creating the virtual link.
EID-3132	An error occurred while setting the OSPF area range: {0}, {1}, false.	CTC encountered an error while setting the area range for the specified values.
EID-3133	The maximum number of OSPF area ranges has been exceeded.	OSPF area ranges exceeded the maximum number.
EID-3134	The area ID is invalid. Use the DCC OSPF area ID, LAN port area ID, or 0.0.0.0.	Refer to the error message text.
EID-3135	The mask is invalid.	Refer to the error message text.
EID-3136	The range address is invalid.	The range address is invalid. Try again.
EID-3137	Your request has been denied because the timing source information was updated while your changes were still pending. Please retry.	Refer to the error message text.
EID-3138	The clock source for switching is invalid.	You have selected an invalid clock source. Choose another clock.
EID-3139	A switch cannot be made to a reference of inferior quality.	Refer to the error message text.

Error/Warning ID	Error/Warning Message	Description
EID-3140	A higher priority switch is already active.	You cannot switch the timing source manually when a higher priority switch is already active.
EID-3141	An attempt was made to access a bad reference.	Refer to the error message text.
EID-3142	No switch is active.	None of the switches are active.
EID-3143	An error occurred while creating the static route entry.	CTC encountered an error while a creating static route entry.
EID-3144	The maximum number of static routes has been exceeded.	The number of static routes has exceeded its limit.
EID-3145	The RIP metric must be between 1 and 15.	The Routing Information Protocol (RIP) metric should be in the range of 1 to 15.
EID-3146	The RIP metric is invalid.	Refer to the error message text.
EID-3147	An error occurred while creating the 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	The MAC addresses could not be retrieved.	Refer to the 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 writable.	The target file is not writable. Specify another file.
EID-3152	An error occurred while creating the protection group.	CTC encountered an error creating Protection Group.
EID-3153	The card cannot be deleted because it is in use.	Refer to the error message text.
EID-3154	An error occurred while provisioning the card: CTC cannot {0} the card.	CTC cannot perform the task on the card.
EID-3155	An error occurred while building the menu.	CTC encountered an error building the menu.
EID-3156	An error occurred while building the menu. Cards were not found for the {0} group.	CTC encountered an error while building the menu, as cards could not be found for the specified group).
EID-3157	The selected model could not be set because of an unexpected model class: {0}.	CTC encountered an unexpected model class while trying to complete the task.

Error/Warning ID	Error/Warning Message	Description
EID-3158	Probable causes: - Unable to switch, because a similar or higher priority condition exists on a peer or far-end card. - A loopback is present on the working port. - Protect port is in OOS disabled admin state	Refer to the error message text.
EID-3159	An error occurred while applying the operation.	CTC encountered an error while applying this operation. 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.
EID-3160	An error occurred while provisioning the {0}.	CTC encountered the specified error.
EID-3161	An error occurred while upgrading the ring.	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 the error message text.
EID-3163	The data in row {0} cannot be validated.	CTC cannot validate the data for the specified row.
EID-3164	The new node ID ({0}) for ring ID {1} duplicates the 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 the error message text.
EID-3166	An error occurred while refreshing the {0} table.	CTC encountered an error while refreshing the specified table.
EID-3167	The slot is already in use.	Refer to the error message text.
EID-3168	An error occurred while provisioning.	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	An error occurred while adding the card.	CTC encountered an error while adding the card.

Error/Warning ID	Error/Warning Message	Description
EID-3170	You cannot delete this card: {0}.	Refer to the error message text.
EID-3171	An error occurred while creating the trap destination.	CTC encountered an error creating the trap destination.
EID-3172	No RMON thresholds were selected.	Select an RMON threshold.
EID-3173	The contact "{0}" cannot exceed {1} characters.	The specified contact exceeds the specified character limit.
EID-3174	The description "{0}" cannot exceed {1} characters.	The specified location exceeds the specified character limit.
EID-3175	The operator identifier "{0}" cannot exceed {1} characters.	The specified operator identifier exceeds the specified character limit.
EID-3176	The operator specific information "{0}" cannot exceed {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 node name "{0}" cannot exceed {1} characters.	The specified name exceeds the specified character limit.
EID-3179	The protect card is in use.	Refer to the error message text.
EID-3180	The 1+1 protection group does not exist.	Create a 1+1 protection group.
EID-3181	The Y-cable protection group does not exist.	Refer to the 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	An error occurred while deleting the protection group.	CTC encountered an error while deleting the protection group.
EID-3184	No {0} was selected.	You must select an item before completing this task.
EID-3185	This ring has an active protection switch operation and cannot be deleted at this time.	Refer to the error message text.
EID-3186	The node is busy: {0} is {1} and cannot be deleted as requested.	The request cannot be completed.
EID-3187	An error occurred while deleting the trap destination.	CTC encountered an error deleting the trap destination.
EID-3188	An error occurred during authentication. The password entered is invalid.	The password you entered is invalid. Enter the password again.

Error/Warning ID	Error/Warning Message	Description
EID-3189	The sum of the {0} must be between {1} and {2}.	Refer to the error message text.
EID-3214	The number of high order circuits for the line could not be retrieved.	The number of High Orders (STS/STM) for the line is not available.
EID-3215	An error occurred while refreshing.	Used frequently in pane classes to indicate a general error condition when trying to refresh from the model.
EID-3216	The proxy port is invalid.	Refer to the error message text.
EID-3217	The statistics could not be refreshed.	CTC could not refresh statistics values.
EID-3218	The automatic node setup could not be launched.	Refer to the error message text.
EID-3219	The automatic node setup information could not be refreshed.	Failure trying to retrieve automatic node setup information.
EID-3220	An error occurred while refreshing row {0}.	Error refreshing the specified row.
EID-3222	The statistics could not be cleared.	Refer to the error message text.
EID-3225	An error occurred while refreshing the pane.	Used frequently in pane classes to indicate a general error condition when trying to refresh from the model.
EID-3226	The {0} termination(s) could not be deleted. {1}	Refer to the error message text.
EID-3227	A baseline could not be recorded. Performance metrics will remain unchanged.	CTC failed to set the baseline values while provisioning NE. Previous values remain unchanged.
EID-3228	The {0} termination(s) could not be created. {1}	Refer to the 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	An error occurred while setting the OPR.	An error was encountered while attempting to provision the optical power received (OPR).
WID-3232	The port state cannot be indirectly transitioned because the port is still providing services. If the port state should be changed, edit it directly through port provisioning.	Edit the port state while provisioning the port.

Error/Warning ID	Error/Warning Message	Description
EID-3233	The current loopback provisioning does not allow this state transition.	Refer to the error message text.
EID-3234	The current synchronization provisioning does not allow this state transition.	You cannot transition the port state to the target date while in the current synchronization state.
EID-3235	The requested state transition cannot be performed on this software version.	Refer to the error message text.
EID-3236	The database restore failed. {0}	CTC failed to restore the specified database.
EID-3237	The database backup failed. {0}	CTC failed to backup the specified database.
EID-3238	The send PDIP setting on {0} is inconsistent with the setting on the 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 the 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	An {1} exists on the selected ports. Therefore, you must create the {0}s one by one.	The specified DCC already exists on the selected port. You can create a DCC of another type.
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	An {0} exists on the selected ports. Therefore, you must create the {1}s one by one.	The specified DCC already exists on the selected port. You can 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 the warning message text.
EID-3246	The wizard was not able to validate the data. {0}	CTC encountered an error.

Error/Warning ID	Error/Warning Message	Description
EID-3247	An ordering error occurred. The absolute value should be {0}.	The absolute value entered was wrong.
EID-3248	The value for the parameter {0} is invalid.	CTC changed the incorrect parameter.
EID-3249	The voltage increment value is invalid.	Refer to the error message text.
EID-3250	The power monitor range is invalid.	Refer to the error message text.
EID-3251	The requested action could not be completed. {0}	CTC could not complete the specified action.
EID-3252	No download has been initiated from this CTC session.	Refer to the error message text.
EID-3253	The reboot operation failed. {0}	Refer to the error message text.
EID-3254	An error occurred during validation. {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	You cannot change the timing configuration because a Manual/Force operation is in effect.	Refer to the error message text.
WID-3256	The timing reference(s) could not be assigned because one or more of the timing reference(s): - is already used and/or - has been selected twice and/or - is attempting to use the same slot twice. Please verify the settings.	Refer to the warning message text.
EID-3257	Duplicate DCC numbers are not permitted. {0}.	CTC detected more than one occurrence of the a DCC number. Remove one of them.
EID-3258	A software error occurred while attempting to download the file. Please try again later.	Refer to the error message text.
EID-3259	An error occurred while creating the FC-MR threshold.	You must create a Fibre Channel Multirate (FC_MR) card threshold.
EID-3260	An error occurred while provisioning the internal subnet: {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 the error message text.
EID-3262	The port provisioning cannot be changed when the port status is {0}.	You must provision the ports only when the port is Out of Service.

Error/Warning ID	Error/Warning Message	Description
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-3265	An error occurred while modifying the protection group.	Protection Group could not be modified.
EID-3266	Conditions could not be retrieved from the shelf or card view.	Refer to the error message text.
WID-3267	The XTC protection group cannot be modified.	Refer to the warning message text.
WID-3268	The filter entry is invalid. {0}	The specified entry is invalid.
WID-3269	The {0} operation was successfully initiated for {1} but its completion status could not be obtained from the node. When the node is accessible, check its software version to verify if the {0} succeeded.	Refer to the 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	An entry is 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 result in a node reboot cannot take place during a software upgrade. Please try again after the software upgrade is done.	Refer to the warning message text.
WID-3275	Ensure that the remote interface ID and the local interface ID on the two sides match. (The local interface ID on this node should equal the remote interface ID on the neighbor node and vice-versa).	Refer to the 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 exceed {0} characters. Your input will be truncated.	The input exceeds the character limit. The value will be truncated to the maximum character limit.

Error/Warning ID	Error/Warning Message	Description
WID-3279	This card has been deleted. CTC will return to the shelf view.	CTC returns to node view.
WID-3280	ALS will not engage until both the protected trunk ports detect LOS.	Refer to the warning message text.
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 ONS 15600s are currently unsafe to upgrade...	Refer to the warning message text.
WID-3283	Before activating a new version, ensure that you have a database backup from the current version.	Refer to the 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 might result in traffic loss.	Refer to the 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 the 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 the warning message text.
WID-3288	The status of this ring 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	The specified provisionable patchcord(s) could not be deleted.	Refer to the error message text.
EID-3291	The revertive behavior cannot be changed because a protection switch is active.	Protection switch should not be active to change the revertive behavior.
EID-3292	An error occurred while resetting the shelf.	CTC encountered an error while resetting the node.
EID-3293	No such provisionable patchcords exists.	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.

Error/Warning ID	Error/Warning Message	Description
EID-3294	No RMON thresholds are available for the selected port.	Refer to the error message text.
EID-3295	This card does not support RMON thresholds.	Refer to the error message text.
EID-3296	Buffer-to-buffer credit is only supported for Fibre Channel (FC) and FICON.	Refer to the error message text.
EID-3298	This interfaces does not support ALS auto restart.	Refer to the error message text.
EID-3300	Duplicate OSPF area IDs are not permitted.	OSPF area IDs should be unique.
EID-3301	The LAN metric cannot be zero.	Refer to the error message text.
EID-3302	The standby {0} is not ready.	Standby controller card is not ready.
EID-3303	The DCC area ID and {0} conflict. {1}	DCC Area ID and ring type, specified by {0}, conflict each other due to the details specified by {1}.
EID-3304	The DCC number is out of range.	Enter a DCC number that is within the range
EID-3305	OSPF cannot be active on the LAN interface when the backbone area is 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 the error message text.
EID-3307	An error occurred while creating a connection object at {0}.	CTC encountered an error at the specified connection while creating the connection.
EID-3308	DWDM links can be used only for optical channel circuits.	Refer to the error message text.
EID-3309	The link was excluded because it was in the 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	The DWDM link does not have wavelengths available.	Refer to the error message text.
EID-3311	The laser is already on.	Refer to the error message text.
EID-3312	The power setpoint cannot be changed. {0} {1}	CTC cannot change the power setpoint. The new setpoint would either make the thresholds inconsistent or set the fail threshold outside the range.

Error/Warning ID	Error/Warning Message	Description
EID-3313	The offset cannot be modified because the service state of the port is IS.	Refer to the error message text.
EID-3314	The requested action is not allowed. The state value is invalid.	Refer to the error message text.
EID-3315	This operation cannot be performed.	CTC is unable to perform operation.
EID-3316	The node side is invalid.	This task was applied to the wrong node side.
EID-3317	The ring name is too long.	Reduce the number of characters in the name.
EID-3318	The ring name is invalid.	The name you entered is illegal.
EID-3319	The wrong line was selected.	Select another line
EID-3320	The optical link could not be deleted.	CTC cannot delete the optical link.
EID-3321	This feature is unsupported by this version of software.	Refer to the error message text.
EID-3322	The equipment is not plugged in.	Plug-in the equipment and proceed.
EID-3323	The APC system is busy.	Automatic Power Control (APC) system is busy.
EID-3324	There is no path to regulate.	There is no circuit path to regulate.
EID-3325	The requested action is not allowed.	Generic DWDM provisioning failure message.
EID-3326	The input was invalid.	The input value is incorrect.
EID-3327	An error occurred while retrieving thresholds.	There was an error retrieving the thresholds. This message is displayed only for the OSCM/OSC-CSM line thresholds.
EID-3328	An error occurred while applying changes to row {0}. The value is out of range.	There was an error applying the changes to the specified row. The value is out of range.
EID-3330	Unable to switch to the byte because an overhead channel is present on this byte of the port.	Refer to the error message text.
EID-3331	An error occurred while applying changes to the row.	Refer to the error message text.
EID-3334	Timing parameters on the protect port cannot be changed.	You cannot change timing parameters on protect port.

Error/Warning ID	Error/Warning Message	Description
EID-3335	The port type cannot be changed because the SDH validation check failed. Check if this port is part of a circuit, protection group, SONET DCC, orderwire, or UNI-C interface.	Refer to the error message text.
EID-3336	An error occurred while reading a control mode value.	The Control Mode must be retrieved.
EID-3337	An error occurred while setting a set point gain value.	The Gain Set Point must be set.
EID-3338	An error occurred while reading a set-point gain value.	The Gain Set Point must be retrieved.
EID-3339	An error occurred while setting a tilt calibration value.	The tilt calibration must be set.
EID-3340	An error occurred while setting expected wavelength.	The expected wavelength must be set.
EID-3341	An error occurred while reading expected wavelength.	The expected wavelength must be retrieved.
EID-3342	An error occurred while reading actual wavelength.	The actual wavelength must be retrieved.
EID-3343	An error occurred while reading actual band.	The actual band must be retrieved.
EID-3344	An error occurred while reading expected band.	The expected band must be retrieved.
EID-3345	An error occurred while setting expected band.	The expected band must be set.
EID-3346	An error occurred while retrieving defaults from the node: {0}.	There was an error retrieving defaults from the specified node.
EID-3347	The file {0} cannot be loaded.	CTC cannot load the specified file.
EID-3348	Properties cannot be loaded from the node.	Refer to the error message text.
EID-3349	NE update properties cannot be saved to a file.	Check your file system for space constraint or any other problem.
EID-3350	NE update properties cannot be loaded from the node.	Refer to the error message text.
EID-3351	The file {0} does not exist.	The specified file does not exist.
EID-3352	An error occurred while setting a value at {0}.	There was an error while setting the value at the specified location.
EID-3353	No such interface is available.	The interface specified is not present in CTC.
EID-3354	The specified endpoint is in use.	Select another endpoint that is not in use.
EID-3355	The specified endpoint is incompatible.	Refer to the error message text.
EID-3357	The connections could not be calculated.	Refer to the error message text.

Error/Warning ID	Error/Warning Message	Description
EID-3358	An optical link model does not exist for the specified interface.	Create an optical linkmodel for the interface, and proceed.
EID-3359	Optical parameters could not be set for the node.	Refer to the error message text.
EID-3360	ANS cannot be performed. Please check {0} parameter value.	Refer to the error message text.
EID-3361	The ring termination is in use. An error occurred while deleting the ring termination.	You cannot delete a ring in use.
EID-3362	An error occurred while deleting the ring termination.	There was an error while deleting ring termination.
EID-3363	No ring terminations were selected.	You must select a ring termination.
EID-3364	An error occurred while creating the ring ID.	There was an error while creating the ring ID.
EID-3365	The OSC termination is in use.	Select another optical service channel (OSC) which is not in use.
EID-3366	The OSC termination could not be deleted.	There was an error deleting the OSC termination.
EID-3370	No optical link was selected.	You must select an optical link.
EID-3371	An error occurred while calculating the automatic optical link list.	Refer to the error message text.
EID-3372	CTC attempted to access an OCHNC connection that has been destroyed.	CTC destroyed an external attempt to access an optical channel network connection.
EID-3375	The expected span loss must be set.	Refer to the error message text.
EID-3376	The measured span loss could not be retrieved.	Refer to the error message text.
EID-3377	The wrong interface was used.	The interface used for the card is wrong.
EID-3378	This is a 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	This is a 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	The host cannot be found.	Refer to the error message text.

Error/Warning ID	Error/Warning Message	Description
EID-3381	The 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 increment by the specified value.
EID-3382	The number of credits must be between {0} and {1}.	The number of credits must be between the specified values.
EID-3383	The 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 increment 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. Is it OK to continue?	Refer to the warning message text.
EID-3385	{0}. Delete the circuits and try again.	Refer to the error message text.
EID-3386	The transponder mode could not be provisioned: {0}	The specified transponder mode cannot be provisioned.
EID-3387	You must change port(s) {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	The card mode cannot be changed because the card has circuits.	Refer to the error message text.
EID-3389	An error occurred while changing the card mode.	Refer to the error message text.
EID-3390	The port is in use.	Refer to the error message text.
EID-3391	The port rate cannot be changed because the port has been deleted.	You cannot change the port rate of a card that has been deleted.
WID-3392	The timing reference(s) could not be assigned because with external timing, only a single protected, or two unprotected timing references per BITS Out can be selected. Please use the "Reset" button and verify the settings.	Refer to the warning message text.
WID-3393	The timing reference(s) could not be assigned because with line or mixed timing, only a single unprotected timing reference per BITS Out can be selected. Please use the "Reset" button and verify the settings.	Refer to the warning message text.
EID-3394	An error occurred while refreshing the power monitoring values.	Refer to the error message text.

Error/Warning ID	Error/Warning Message	Description
EID-3395	The configuration is invalid. {0}	CTC encountered an error in IP address, net mask length, or default router, or a restricted IIOP port was selected.
EID-3397	The file {0} is the wrong version.	The specified file is of wrong version.
EID-3398	The PPM cannot be deleted.	Refer to the error message text.
EID-3399	The PPM cannot be deleted because it has port(s) in use.	Remove the ports connected to the Pluggable Port Module before it can be deleted.
EID-3400	Unable to switch. A force to the primary facility is not allowed.	Refer to the 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	The switch request could not be completed. The {0} card is not present or is not responding. Try again after ensuring that the {0} card is present and is not resetting.	Refer to the error message text.
EID-3403	The administrative state transition has not been attempted on the monitored port.	Refer to the error message text.
EID-3404	The far end IP address could not be set on the {0} termination. The IP address cannot be: loopback (127.0.0.0/8) class D (224.0.0.0/4) class E (240.0.0.0/4) broadcast (255.255.255.255/32) internal {1}	Refer to the error message text.
EID-3405	You cannot change card parameters with port {0} in {1} state. Click "Reset" to revert the changes.	Refer to the error message text.
EID-4000	The {0} ring name cannot be changed now because 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} node ID cannot be changed now because a {0} switch is active.	You cannot change the ring ID because a switch of the same ring type is active.

Error/Warning ID	Error/Warning Message	Description
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. If the node was running {0} before, reverting will restore the {0} provisioning, losing any later provisioning. If the node was running some other version, reverting will LOSE ALL PROVISIONING. {1} {2}	Refer to the warning message text.
EID-4003	The Cisco IOS console is disabled for the card in Slot {0}.	The card may not be an IOS-based card or it may be rebooting.
EID-4004	An error occurred while canceling the software upgrade.	CTC encountered an error while canceling the software upgrade.
EID-4005	{0} encountered while performing a database backup.	CTC encountered the specified error during database backup.
EID-4006	The file {0} does not exist or cannot be read.	Refer to error message.
EID-4007	The size of the file {0} is zero.	The size of the file that is being backed up or restored is zero.
WID-4008	A software upgrade is in progress. {0} cannot proceed during a software upgrade. Please try again after the software upgrade has completed.	The specified action cannot be performed during a software upgrade. You must try after the upgrade process is completed.
EID-4009	{0} encountered while restoring the database.	CTC encountered the specified error while restoring the database.
EID-4010	The operation was terminated because: {0}	Refer to the error message text.
EID-4011	An error occurred during provisioning: {0}	Refer to the error message text.
WID-4012	Node management for {0} is not provided.	Refer to the warning message text.
EID-4013	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. If the node was running {0} before, reverting will restore the {0} provisioning, losing any later provisioning. If the node was running some other version, reverting will LOSE ALL PROVISIONING. {1} {2} {3}	Refer to the error message text.
EID-4014	The manual path trace 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.

Error/Warning ID	Error/Warning Message	Description
EID-4015	Software activation is in progress. Provisioning is not allowed.	Refer to the error message text.
EID-4016	Software activation is in progress. {0} is not allowed.	Refer to the error message text.
EID-4017	Path Trace mode cannot be set at this endpoint. The circuit is one-way.	Refer to the error message text.
WID-4018	{0} already exists. Do you want to replace it?	Refer to the warning message text.
EID-4019	Profile cannot be mapped because the UNI Port is not in transparent mode.	Refer to the error message text.
EID-4020	Profile cannot be mapped because the transparent mode UNI Port tagged VLAN is not {0}.	Refer to the error message text.
EID-4021	Profile cannot be mapped because SVLAN {0} is not enabled for the NNI Port.	Refer to the error message text.
EID-4022	The user already exists.	Refer to the error message text.
EID-4023	Access control already exists for the group selected.	Refer to the error message text.
EID-4024	The View already exists.	Refer to the error message text.
EID-4025	Invalid Mask entry, cant be more then {0} the length of OID.	Refer to the error message text.
EID-4026	CTC was unable to create a new view.	Refer to the error message text.
EID-4027	Name and Subtree OID cant be empty.	Refer to the error message text.
EID-4028	Password will be sent as plain text.	Refer to the error message text.
EID-4029	The passwords must be at least {0} characters long.	Refer to the error message text.
EID-4030	The admitted SVLAN values must be in the range [1-4093].	Refer to the error message text.
EID-4031	On {0} interface the Recover from Fiber Cut Fails.	Refer to the error message text.
EID-4032	Link Integrity and L2 1+1 protection cannot operate on the same interface.	Refer to the error message text.
WID-4033	No files were specified. Please enter a valid file name.	Refer to the error message text.
EID-4034	WDMANS parameter already present.	Refer to the error message text.
EID-4035	WDMANS parameter is not valid.	Refer to the error message text.

Error/Warning ID	Error/Warning Message	Description
EID-4036	WDMANS parameter cannot be removed. This may be in use by the system.	Refer to the error message text.
EID-4037	This operation is not supported on the protect entity of a protection group.	Refer to the error message text.
EID-4051	The bandwidth for the configuration modes is allocated once the payload for the PPMs are provisioned. In case of MXP_MR mode the bandwidth is allocated only after a circuit is created.	Refer to the error message text.
EID-4052	ODU Utilization is not supported for this mode. Bandwidth utilization is not valid for Operating mode provisioned on the PPM.	Refer to the error message text.
EID-5000	A valid route cannot be found for the tunnel change request.	Refer to the error message text.
EID-5001	The tunnel could not be changed.	Refer to the error message text.
EID-5002	The tunnel could not be restored and must be recreated manually.	Refer to the error message text.
EID-5003	The circuit roll failed. {0}	Refer to the error message text.
EID-5004	There is already one four-fiber {0} provisioned on the set of nodes involved in {1}. The maximum number of four-fiber {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 the warning message text.
WID-5006	Warning: A 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 the warning message text.
WID-5008	Please ensure that all the protection groups are in proper states after the cancellation.	Refer to the warning message text.
WID-5009	The circuit {0} is not upgradable. No {1} capable {2}s are available at the node {3}.	No VT capable STSs are available at the node.
EID-5010	The domain name already exists.	Refer to the error message text.

Error/Warning ID	Error/Warning Message	Description
EID-5011	The domain name cannot exceed {0} characters.	You may have reached the maximum number of characters.
WID-5012	The software load on {0} does not support the addition of a node to a 1+1 protection group.	Refer to the warning message text.
EID-5013	{0} does not support the 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 before 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 occurred while attempting to provision the {0}. {1}	CTC encountered an error while provisioning the card.
EID-5017	Provisioning could not be rolled back. The {0} might 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 a(n) {1} node and cannot be added to a(n) {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	The manual path trace 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.
EID-5020	Software activation is in progress. Provisioning is not allowed.	Refer to the warning message text.
EID-5021	Software activation is in progress. {0} is not allowed.	Refer to the error message text.
WID-5022	Warning: Ethergroup circuits are stateless (that is, always in service). The current state selection of {0} will be ignored.	Refer to the warning message text.
EID-5023	CTC cannot communicate with the node. The operation failed.	CTC encountered a network communication error. Connectivity between CTC and the NE was disrupted, either transiently or permanently.
EID-5024	The overhead circuit will not be upgraded.	Refer to the error message text.

Error/Warning ID	Error/Warning Message	Description
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 the warning message text.
EID-5026	An ONS 15600 cannot serve as the primary or secondary node in a four-fiber {0} circuit. Please change your ring and/or node selections so that an ONS 15600 is not chosen as the primary or secondary node in this four-fiber {1} circuit.	Refer to the error message text.
WID-5027	The {0} Edit dialog box for the ring {1} has been closed due to significant provisioning changes. These changes might only be transitory, so you can reopen the {0} Edit dialog box to view the updated state.	Re-open the BLSR/MS-SPRing edit window to view the updated state of the ring.
WID-5028	Warning: This operation should only be used to clean up rolls that are stuck. It might also affect completeness of the circuit. Is it OK to continue with the deletion?	Refer to the warning message text.
EID-5029	A software downgrade cannot be performed to the selected version while an 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 the error message text.
EID-5030	A software downgrade cannot be performed at the present time.	Try the software downgrade later.
WID-5031	Canceling a software upgrade during a standby TSC clock acquisition might result in a traffic outage.	Refer to the warning message text.
EID-5032	An error occurred while accepting the load.	Refer to the error message text.
EID-5033	The profile could not be loaded. An error occurred while decoding the characters.	CTC detected an error while decoding characters and could not load the profile.
EID-5034	The profile could not be loaded. An error occurred while trying to recognize the file format.	CTC detected an error and could not load the profile.
EID-5035	The profile could not be loaded. An error occurred while reading the file.	CTC could not read the file and is therefore unable to load the profile.
EID-5036	The GNE hostname {0} is invalid.	The specified host name is invalid. CTC could not resolve the host name to any valid IP address

Error/Warning ID	Error/Warning Message	Description
EID-5037	Provisionable patchcords cannot be created between transponder trunk ports and multiplexer/demultiplexer ports on the same node.	You must create provisionable patchcords between transponder trunk ports and mux/demux ports that are on different nodes.
EID-5038	Provisionable patchcords created between transponder trunk ports and multiplexer/demultiplexer ports must use the same wavelength: {0} is not equal to {1}.	Wavelengths used by provisionable patchcords for transponder trunk ports and mux/demux ports must be the same.
EID-5039	Provisionable patchcords created between transponder trunk ports and multiplexer/demultiplexer ports must use the same wavelength: {0} is not equal to {1}. Please provision the {2} wavelength on {3}.	Transmitter and receiver port wavelengths are not equal. Provision the receiver and transmitter wavelengths on transmitter and receiver ports respectively.
EID-5040	Provisionable patchcords created between OC3/OC12 ports and multiplexer/demultiplexer ports are not supported.	Refer to the error message text.
EID-5041	Provisionable patchcords created between gray OC-N trunk ports and multiplexer/demultiplexer ports are not supported.	Refer to the error message text.
EID-5042	Provisionable patchcords created between OC-N trunk ports and multiplexer/demultiplexer ports must use the same wavelength: {0} is not equal to {1}.	Wavelengths used by provisionable patchcords for OC-N trunk ports and mux/demux ports must be the same.
WID-5043	Warning: Only the line card was provisioned. The wavelength compatibility check was skipped.	Refer to the warning message text.
EID-5044	Virtual links can be used only for OCH-Trail circuits.	Refer to the error message text.
EID-5045	The virtual link does not have wavelengths available.	Set wavelengths for the virtual link and proceed.
WID-5046	Warning: if you select "Use OCHNC Direction," your circuit will be limited to nodes prior to release 07.00.	Refer to the warning message text.
EID-5047	Provisionable patchcords created between OC3/OC12 ports are not supported.	Refer to the error message text.
EID-5048	Provisionable patchcords created between gray OC-N trunk ports are not supported.	Refer to the error message text.
EID-5049	Provisionable patchcords created between gray OC-N trunk ports and multiplexer/demultiplexer ports are not supported.	Refer to the error message text.
EID-5050	The element model could not be found. {0}	The specified Element Model cannot be located.

Error/Warning ID	Error/Warning Message	Description
WID-5051	The port state cannot be indirectly transitioned because the port aggregates OCHCC circuits: if the port state needs to be changed, edit it directly through port provisioning.	Refer to the warning message text.
EID-5052	The operation is not valid for the connection type.	You may have selected the incorrect switch.
EID-5053	The operation cannot be performed because the connection is under test access.	Refer to the error message text.
EID-5054	The TL1 tunnel could not be opened. {0}	Refer to the error message text.
EID-5055	Some patchcords were not deleted. Patchcords cannot be deleted if they are incomplete or support any circuits, or if the nodes supporting them are not connected.	Refer to the error message text.
EID-5056	This PPC cannot be deleted because one or more circuits are provisioned over it.	Remove the circuits provisioned over the provisionable patchcord before trying to delete it.
EID-5057	The addition of the last node has not yet finished. Please wait before trying to add a new node.	Refer to the error message text.
EID-5058	An OCHNC upgrade is applicable only to bidirectional circuits.	Refer to the error message text.
EID-5059	The OCHNC upgrade failed. One or more communication failures occurred during the operation.	CTC encountered a complete failure while upgrading optical channel network connection.
EID-5060	The OCHNC upgrade partially failed. One or more communication failures occurred during the operation. Create the OCHCC manually.	CTC encountered a partial failure while upgrading an optical channel network connection.
EID-5061	The overhead circuit source and destination must reside on the same shelf.	Refer to the error message text.
EID-5062	A four-fiber {0} cannot be created using three cards.	A four-fiber BLSR needs four cards.
WID-5063	The profile "{0}" includes a change to the OPEN-SLOT alarm severity. This change is disallowed for the ONS 15600. "{1}" will continue to use the OPEN-SLOT severity of MN that is included in the default configuration. Other changes from the "{2}" profile were successfully applied to {3}".	Refer to the warning message text.
EID-5064	{0} {1}	This indicates the status of path protection switching.

Error/Warning ID	Error/Warning Message	Description
WID-5065	If you apply routing constraints to more than {0} nodes, performance might be affected and the operation might require more time than expected. Select Yes if you intend to proceed in spite of this risk, or No if you prefer to review your selection.	Refer to the warning message text.
WID-5066	The routing constraints will be lost. Are you sure you want to reset your changes?	Refer to the warning message text.
WID-5067	The routing constraints will be lost. Are you sure you want to leave this panel?	Refer to the warning message text.
EID-5068	The routing constraints could not be applied.	Refer to the error message text.
EID-5069	A source node cannot be added to either of these lists.	Select a node other than the source node to add to the route.
EID-5070	A destination node cannot be added to either of these lists.	Select a node other than the destination node to add to the route.
EID-5071	This node already belongs to one of these lists.	The node is already selected either in include or exclude list in the OCH circuit.
EID-5072	An OCH-Trail tunnel link was found but without any associated circuit.	Create an OCH-Trail circuit associated with the link.
EID-5073	You are creating an unprotected link from a protected port. Do you want to continue?	Refer to the error message.
EID-5074	Deleting OCH DCN circuits will cause a loss of connectivity to nodes in the circuit path that do not have other DCN connections. Do you want to continue?	Refer to the error message.
EID-5075	The VLAN ID must be a number between 1 and 4093.	Enter a number between 1 and 4093.
EID-5076	An error occurred while provisioning the VLAN ID. The VLAN ID is already present in the current profile	Select a VLAN ID that is not present in the current profile.
EID-5077	An error occurred while provisioning the VLAN database profile. {0}	CTC could not save the VLAN profile to the file name mentioned.
EID-5078	The VLAN merge is not complete. You forgot to fill {0} record(s).	Fill in the number of records specified and then proceed.
EID-5079	An error occurred while validating the provisionable patchcord.	Refer to the error message text.
EID-5080	No rolls are available.	You cannot delete a roll without selecting a roll.
EID-5081	An error occurred while tracing the RPR ring: {0}	The circuit reference is invalid.

Error/Warning ID	Error/Warning Message	Description
EID-5082	{0} does not support: - Low-order circuits that have both {1}-protected and {2}-protected spans and that cross a node that does not have low-order cross-connect capability. - High-order circuits that carry low-order circuits with the parameters described above.	Refer to the error message text.
EID-5083	This circuit is not the same size as the existing circuit {0}. This circuit has size {1} and the existing circuit has size {2}.	During an RPR circuit creation ML card, the new circuit size and the existing circuit size must be the same.
EID-5084	The Trunk model could not be found. {0}	The trunk specified is not found.
EID-5085	The maximum number of VLAN DB profiles is {0}.	Refer to the error message.
EID-5086	The circuit roll failed. You cannot bridge and roll the selected circuit because it has a monitor circuit.	Refer to the error message.
EID-5087	You cannot use same slot for east working and west protect ports.	Refer to the error message text.
EID-5088	You cannot use same slot for east working and west protect ports.	Refer to the error message text.
WID-5089	The maximum number of circuits that can be deleted at a time is 200. Do you want to delete the first 200 circuits selected?	Refer to the error message text
EID-5090	This operation cannot be completed. The selected circuits have different state models; please select circuits of the same type.	Refer to the error message text
EID-5091	Some PPC terminations were not repaired.	Refer to the error message text
WID-5092	The TL1 encoding mode for the tunnel is being changed. Do you want to modify the encoding?	Confirm if you really want to modify TL1 tunnel encoding.
EID-5094	Currently, CTC does not support bridge and roll on circuits having multiple cross-connects on a single node.	Refer to the error message text.
EID-5095	No path were selected. Please select at least one path starting from the {0} NE.	Refer to the error message text.
EID-5096	The first path must starts from the {0} NE.	Refer to the error message text.
EID-5097	The selected path should be linked with the last selected and keep the same direction.	Refer to the error message text.
EID-5098	The node is not selectable. Only the Span between the nodes are selectable.	Refer to the error message text.
EID-5099	Raman Command Error on {0}. {1}.	Refer to the error message text.

Error/Warning ID	Error/Warning Message	Description
EID-5100	Raman Command in TimeOut. {0}.	Refer to the error message text.
EID-5101	Failed to get trunk ports for client. {0}.	Refer to the error message text.
EID-5102	Protected cards must have 2 trunk ports. (found {0}).	Refer to the error message text.
EID-5103	Failed to get colocated OCH ports for trunk: {0}.	Refer to the error message text.
EID-5104	Both OCHCC and OCHNC Protected are not allowed.	Refer to the error message text.
EID-5105	Cannot find entity model for endpoint: {0}.	Refer to the error message text.
EID-5106	Cannot find Out OTS line for selected endpoint: {0}.	Refer to the error message text.
EID-5107	Cannot find Protected Out OTS line for selected endpoint: {0}.	Refer to the error message text.
EID-5108	The demultiplexer associated with the selected endpoint :{0} is missing or not connected.	Refer to the error message text.
EID-5109	The demultiplexer associated with the protect path for the selected endpoint: {0} is missing or not connected.	Refer to the error message text.
EID-5110	The card selection is invalid. No cards were selected.	Refer to the error message text.
EID-5111	An error was occurred while configuring SNMPv3 proxy server.	Refer to the error message text.
EID-5112	No source of trap was selected.	Refer to the error message text.
EID-5113	Specify a valid value for target tag.	Refer to the error message text.
EID-5114	Specify a valid value for context engine ID.	Refer to the error message text.
EID-5115	No value was selected for proxy type.	Refer to the error message text.
EID-5116	No value was selected for local user.	Refer to the error message text.
EID-5117	No value was selected for proxy destination.	Refer to the error message text.
EID-5118	Specify a valid value for target IP.	Refer to the error message text.
EID-5119	The password for authentication should be at least 8 characters long.	Refer to the error message text.
EID-5120	The user name should be at least 6 characters long.	Refer to the error message text.
EID-5122	The node ({0}) does not support ML-MR POS port protection.	Refer to the error message text.
EID-5123	Primary ({0}) and secondary ({1}) nodes have to be the same for ML-MR POS port protection.	Refer to the error message text.

Error/Warning ID	Error/Warning Message	Description
EID-5124	No nodes appear to support a Pseudo IOS connection.	Refer to the error message text.
EID-5125	No node was selected.	Refer to the error message text.
EID-5126	The Pseudo IOS console is disabled for the selected node.	Refer to the error message text.
EID-5127	The password for encryption should be at least 8 characters long.	Refer to the error message text.
EID-5128	{0} configuration already exists for the {1} {2} with the specified parameters.	Refer to the error message text.
WID-5129	Failed to retrieve the complete OSPF database as it is very large. Please contact Cisco Technical Support (http://www.cisco.com/techsupport) if you want to retrieve the complete OSPF database.	Refer to the warning message text.
EID-5130	Connection failed on node {0}	Refer to the error message text.
EID-5131	An error occurred while deleting the circuit end point.	Refer to the error message text.
WID-5132	Failed to retrieve the status of Proxy server on the node. Please contact Cisco Technical Support (http://www.cisco.com/techsupport) if you want to retrieve the Proxy status.	Refer to the warning message text.
EID-5133	SNMPv3 Proxy configuration already exists for the specified parameters.	Refer to the error message text.
EID-5134	On node {0} the calculated gain is much greater than expected. The wizard cannot operate under this condition. Please call TAC for support.	Refer to the error message text.
EID-5135	Added {0} network circuits to {1}. Circuits using the following wavelength(s) could not be updated as there is not a unique path through the added node: {2}	Refer to the error message text.
WID-5136	This operation will be applied to all drops of this circuit.	Refer to the error message text.
EID-5137	Please specify a valid SRLG value. SRLG value should be numeric.	Refer to the error message text.
EID-5138	Please specify a unique SRLG value. SRLG value already exists.	Refer to the error message text.

Error/Warning ID	Error/Warning Message	Description
EID-5139	Unable to retrieve the node info.	The node name/node IP address could not be retrieved.
EID-5140	Unable to retrieve the link info.	The link source/link destination information could not be retrieved.
EID-5141	Error while initializing some instances.	Error in the backend process.
EID-5142	Unable to generate the SRLG Report.	The node name/node IP address or link source/link destination information could not be retrieved.
WID-5143	Are you sure you want to reset the unique SRLG for {0}	Refer to the error message text.
EID-5144	Unable to set the SRLG for {0}	Refer to the error message text.
EID-5145	Unable to launch view for {0}	The node/link is down.
EID-5146	Unknown Error occurred while updating the SRLG value on the Node/Link. {0}	Refer to the error message text.
WID-5147	Are you sure you want to reset the additional SRLG for {0}	Refer to the error message text.
EID-5148	Unable to set the SRLG for Router {0}	• Cisco router connectivity is down. • XML interface on the Cisco router is not reachable. • Not enough memory on the Cisco router
EID-5149	Unable to get the node model	Complete node information could not be retrieved.
EID-5150	Unable to get the side model	Complete side information could not be retrieved.
EID-5151	Unable to delete the SRLG for CRS node {0}	Refer to the error message text.
WID-5152	Some SRLGs cannot be synchronized. Network operation might be inconsistent.	Refer to the error message text.

Error/Warning ID	Error/Warning Message	Description
EID-5153	Unable to perform SRLG synchronization operation.	• The node name/node IP address or link source/link destination information could not be retrieved. • Cisco CRS node connectivity is down. • XML interface on the Cisco CRS is not reachable. • Not enough memory on the Cisco CRS.
EID-5154	Specified value is out of range for SRLG. SRLG value should be specified between {0}-{1}	Refer to the error message text.
WID-5155	No. of SRLGs for circuit {0} are exceeding the limit. One circuit can have maximum {1} SRLGs defined. Trimming SRLG list to defined maximum size.	Refer to the error message text.
EID-5156	Maximum limit for defining additional SRLGs for Node/Link is reached. Maximum SRLGs that can be defined are {0}	Refer to the error message text.
WID-5157	No CRS based OCH Trail circuits detected	There are no Cisco CRS nodes associated with the circuit.
WID-5158	Some SRLGs cannot be deleted from CRS. Please use Synchronize IPoDWDM to synchronize SRLGs.	• Cisco CRS node connectivity is down. • XML interface on the Cisco CRS is not reachable. • Not enough memory on the Cisco CRS.
WID-5159	Some SRLGs cannot be set on CRS. Please use Synchronize IPoDWDM to synchronize.	• Cisco CRS node connectivity is down. • XML interface on the Cisco CRS is not reachable. • Not enough memory on the Cisco CRS.

Error/Warning ID	Error/Warning Message	Description
EID-5160	Maintenance state cannot be set on CRS. Please use Synchronize IPoDWDM to synchronize.	• Cisco CRS node connectivity is down. • XML interface on the Cisco CRS is not reachable. • Not enough memory on the Cisco CRS.
EID-5161	Some of the effected routers could not be brought back into IS.	• Cisco CRS node connectivity is down. • XML interface on the Cisco CRS is not reachable. • Not enough memory on the Cisco CRS.
EID-5162	The circuit must be in the DISCOVERED state in order to start a PPT.	Refer to the error message text.
EID-5163	Unable to retrieve the Shelf info.	Complete node information could not be retrieved.
EID-5164	Requested operation cannot be completed.	Refer to the error message text.
EID-5165	Unable to perform Maintenance synchronization operation.	• The node name/node IP address or link source/link destination information could not be retrieved. • Cisco CRS node connectivity is down. • XML interface on the Cisco CRS is not reachable. • Not enough memory on the Cisco CRS.
EID-5166	Source is not fully specified.	The node, shelf, or slot is not selected.
EID-5167	Unable to set the Transport Admin State on the CRS {0}	• Cisco CRS node connectivity is down. • XML interface on the Cisco CRS is not reachable. • Not enough memory on the Cisco CRS.

Error/Warning ID	Error/Warning Message	Description
EID-5168	Unable to set the Maintenance state for {0}	Complete node information could not be retrieved.
WID-5169	Some routers have responded not to start maintenance. Do you still want to go ahead with the maintenance activity?	Refer to the error message text.
WID-5170	Some Transport Admin States cannot be synchronized. Network operation might be inconsistent.	Refer to the error message text.
WID-5171	Some routers have not responded with Embargo status. Continuing maintenance activity may be traffic affecting. Are you sure you want to continue?	Refer to the error message text.
EID-5172	Provisionable patchcords can not be created between incompatible ports.	Refer to the error message text.
EID-5173	Some Server Trail terminations were not repaired.	Refer to the error message text.
WID-5174	Routing constraints has been specified only for protected path. Can be evaluated to move some constraints on working path since these are treated with priority. Please consider that some good constraint on protected part may not be evaluated correctly since that constraint may be already applied to working path by auto-routing. Do you want to continue anyway?	Refer to the error message text.
EID-5175	Unknown Error occurred while updating the SRLG value on the CRS node(s). {0}	Refer to the error message text.
WID-5176	One or more SVLANs are invalid. Please remove them before continuing.	Refer to the error message text.
EID-5190	Unable to trace Layer 2 topology. The root link may have been deleted.	Refer to the error message text.
WID-5206	Unable to clear proactive protection on the router. Do it manually.	Clear the proactive protection on the router manually.
EID-5217	Error in trunk configuration on {0}.	Refer to the error message text.
EID-5218	Gmpls circuits can not be reconfigured.	Refer to the error message text.

Error/Warning ID	Error/Warning Message	Description
EID-5220	The time slot selected does not match the payload.	Select the correct payload.
EID-5221	The ODU-1 selected does not match the payload.	Select the correct payload.
WID-5221	Deleting the following OCH TRAIL circuit(s) will cause the Layer2 services (SVLAN, EVC and MPLS TP Tunnel) provisioned on them to go PARTIAL.	Refer to the error message text.
EID-6000	This platform does not support power monitoring thresholds.	Refer to the 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 working.
EID-6002	One of the XC cards is locked.	Unlock the cross-connect card.
EID-6003	The OSC termination could not be created. This ring ID is already assigned.	Enter a new ID for the ring.
EID-6004	A system reset cannot be performed while a BLSR ring is provisioned on the node.	Remove the BLSR from the node and continue with the reset procedure.
EID-6005	The timing references could not be assigned. - Only two DS1 or BITS interfaces can be specified. - DS1 interfaces cannot be retimed and used as a reference. - BITS-2 is not supported on this platform.	Refer to the error message text.
EID-6006	The timing references could not be assigned. - An NE reference can only be used if the timing mode is LINE. - A BITS reference can only be used if the timing mode is not LINE. - A Line reference can only be used if the timing mode is not EXTERNAL.	Refer to the error message text.
EID-6008	SF BER and SD BER are not provisionable on the protect line of a protection group.	Refer to the error message text.
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 endpoints.	Refer to the 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 endpoint.	Refer to the warning message text.
WID-6011	Ingress idle filtering should be turned off only when required to operate with non-Cisco Fibre Channel/FICON-over-SONET equipment.	Refer to the warning message text.
EID-6012	The retiming configuration could not be changed because there are circuits on this port.	You cannot change the timing configuration on this port unless the circuits on this port are deleted.

Error/Warning ID	Error/Warning Message	Description
EID-6013	The NTP/SNTP server could not be changed. {1}	Refer to the error message text.
EID-6014	The operation failed because the reference state is OOS.	Change the Out-of-service state to Active.
EID-6015	The distance extension cannot be disabled if the port media type is FICON 1Gbps ISL or FICON 2Gbps ISL.	Refer to the error message text.
EID-6016	The 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 the 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 the 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 the 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 the 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.
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.

Error/Warning ID	Error/Warning Message	Description
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 the error message text.
EID-6033	A previous operation is still in progress.	Another operation is in progress. You must try after sometime.
EID-6035	The parent entity does not exist.	Refer to the error message text.
EID-6036	The parent PPM entity does not exist.	Create a parent entity for the PPM.
EID-6037	This equipment type is not supported.	CTC does not support this equipment.
EID-6038	The PPM port is invalid.	Refer to the error message text.
EID-6039	The card is part of a regeneration group.	Select another card.
EID-6040	Out of memory.	Refer to the error message text.
EID-6041	The port is already present.	Refer to the error message text.
EID-6042	The port is used as timing source.	Choose another port because the selected port is being used as a timing source.
EID-6043	A DCC or GCC is present.	Refer to the error message text.
EID-6044	The card or port is part of protection group.	Refer to the error message text.
EID-6045	The port has overhead circuit(s).	Refer to the error message text.
EID-6046	The ITU-T G.709 configuration is not compatible with the data rate.	Refer to the error message text.
EID-6047	The 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}.	The trunk port is in the wrong state to carry out the action.
EID-6049	The card operating mode of {0} is not supported.	CTC does not support the mode of operation requested on the card.

Error/Warning ID	Error/Warning Message	Description
EID-6050	Some {0} terminations were not {1}d. {2}	Refer to the error message text.
WID-6051	All {0} terminations were {1}d successfully. {2}	Refer to the warning message text.
EID-6052	The authentication key can not be blank.	Enter an authentication key.
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 not a valid receiver of SNMP traps.
EID-6055	The IP address is already in use.	Refer to the error message text.
EID-6056	The SNMP trap destination is invalid. {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 the warning message text.
EID-6058	The maximum number of IP-over-CLNS tunnels has been exceeded.	Refer to the error message text.
EID-6059	The specified IP-over-CLNS tunnel already exists!	Specify another IP Over CLNS tunnel.
EID-6060	An error occurred while trying to {0} an IP-over-CLNS tunnel entry: {1}.	Refer to the error message text.
EID-6061	An error occurred while deleting the IP-over-CLNS tunnel entry.	CTC encountered an error while deleting the IP Over CLNS tunnel entry.
EID-6062	The selected IP-over-CLNS tunnel does not exist.	Create a IP Over CLNS tunnel.
EID-6063	The selected router does not exist.	Create a router.
EID-6064	The MAA address list is full.	Refer to the error message text.
EID-6065	The selected area address is duplicated.	Enter another area address.
EID-6066	The primary area address cannot be removed.	Refer to the error message text.
EID-6067	The selected area address does not exist.	Choose another area address.
EID-6068	The IP-over-CLNS NSEL cannot be modified while there are IP-over-CLNS tunnel routes provisioned.	You cannot change the NSEL address if tunnels are provisioned.
EID-6069	The node is currently in ES mode. Only Router 1 can be provisioned.	An End System needs only one provisioned router.
EID-6070	No router was selected.	Select a router.

Error/Warning ID	Error/Warning Message	Description
EID-6071	The TARP data cache cannot be flushed.	You cannot flush the cache in the Tunnel identifier Address Resolution Protocol (TARP) state.
EID-6072	The TARP data cache entry cannot be added: {0}	You cannot add the specified cache entry.
WID-6073	A TARP request has been initiated. Try refreshing the TARP data cache later.	Refer to the warning message text.
EID-6074	End system mode only supports one subnet.	Refer to the error message text.
EID-6075	An error occurred while trying to remove a MAT entry. The entry does not exist.	CTC is removing the MAT entry.
EID-6076	An error occurred while trying to {0} a TARP manual adjacency entry: {1}	CTC cannot add the specified adjacency entry for reasons unknown.
EID-6077	The area address must be between 1 and 13 bytes long, inclusive.	The area address should not be more than 13 characters.
EID-6078	A TDC entry with this TID {0} does not exist in the table.	The specified Tunnel Identifier does not exist.
EID-6079	A TDC entry with this TID {0} could not be removed. Please verify that TARP is enabled.	You must enable TARP 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 the 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 another user. The changes cannot be committed.	Refer to the 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 vxWorks shell to assist users.	Refer to the warning message text.
EID-6086	The card cannot be changed because card resources are in use.	The card you are trying to remove is being used. Cannot change the card.
EID-6087	The card cannot be changed because the card type is invalid or incompatible.	Refer to the error message text.

Error/Warning ID	Error/Warning Message	Description
EID-6088	This line cannot be put into loopback while it is in use as a timing source.	Refer to the error message text.
EID-6089	The interface was not found. {0}	CTC cannot find the specified interface.
EID-6090	The interface type is not valid for this operation. {0}	Choose another interface.
EID-6091	The current state of the interface prohibits this operation. {0}	The port is in an invalid state to set a loopback.
EID-6092	This operation is prohibited for this interface. {0}	CTC does not allow this operation for the specified interface.
EID-6093	The maximum number of TARP data cache entries has been exceeded.	You have exceeded the number of characters permitted.
EID-6094	The maximum number of manual adjacency table entries has been exceeded.	Refer to the error message text.
EID-6095	The AIS/Squelch mode is invalid.	Refer to the error message text.
EID-6096	A default IP-over-CLNS tunnel route is only allowed on a node without a default static route and a default router of 0.0.0.0.	Refer to the error message text.
EID-6097	The authorization key does not comply with Cisco IOS password restrictions. {0}	Specify another authorization key.
EID-6098	A default static route is not allowed when a default IP-over-CLNS tunnel exists.	Refer to the error message text.
EID-6099	You cannot create a subnet on a disabled router.	Create the subnet on an active router.
WID-6100	Disabling a router that has a provisioned subnet is not recommended.	Refer to the warning message text.
EID-6101	The MAT entry already exists.	Refer to the error message text.
WID-6102	The new card has less bandwidth than the current card. Circuits of size VT15 and larger will be deleted.	Refer to the 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 canceled.
EID-6105	The 'Change Card' command is valid for MRC cards only when Port 1 is the sole provisioned port.	Refer to the error message text.
EID-6106	To delete all RADIUS server entries, RADIUS authentication must be disabled.	Disable Radius authentication and proceed.

Error/Warning ID	Error/Warning Message	Description
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: 23, 1001-9999 (with the exception of 1080, 2001-2017, 2361, 3081-3083, 4001-4017, 4022, 4081, 4083, 5000, 5001, 7200, 9100, 9300, 9401).	Refer to the error message text.
EID-6108	That port is already in use.	Restart a TELNET session.
EID-6109	A section trace is active on the trunk port. The action cannot be completed.	Actions such as putting the port in an incomplete state are not permitted while a section trace is active.
EID-6110	The maximum number of TARP requests has been reached.	You have exceeded the maximum number of TARP requests.
EID-6111	The card in Slot {0} cannot be removed from the protection group while its traffic is switched.	Refer to the error message text.
EID-6112	An error occurred while adding a shelf: {0}	The shelf ID specified is invalid or already exists, the equipment does not support multishelf, the specified shelf position is out of range, or the specified shelf position is already in use.
EID-6113	An error occurred while deleting a shelf: {0}	One or more of the equipment modules (provisioned virtual links, provisioned server trails, provisioned protection groups, or provisioned DCCs) in the shelf is currently in use. Delete cards from all the slots and try again.
EID-6114	The maximum number of supported shelves has already been provisioned.	Refer to the error message text.
EID-6115	There are bad or duplicate shelf positions. Valid rack numbers are {0} to {1}. Valid rack positions are {2} to {3}.	Refer to the error message text.
EID-6116	CTC attempted to access an OCH-Trail connection that has been destroyed.	Software has prevented an attempt to access an OCH trail.
EID-6117	CTC attempted to access an OCH-Trail audit that has been destroyed.	The resource cannot be accessed because it is released or fully utilized.
WID-6118	The following slots are provisioned but do not have cards installed: {0} CTC will assume they are ITU-T interfaces.	Refer to the warning message text.

Error/Warning ID	Error/Warning Message	Description
EID-6119	The shelves could not be rearranged. {0}	One of the following conditions is present: duplicate shelf positions, invalid shelf positions, or concurrent movement (two CTC sessions are attempting to rearrange the shelves at the same time.)
EID-6120	This equipment does not support multishelf.	Refer to the error message text.
WID-6121	This internal patchcord cannot be provisioned because the endpoints have no compatible wavelengths.	The end points of an internal patchcord should have compatible wavelengths.
EID-6122	The wizard could not be started. {0}	CTC was unable to initiate the wizard due to the specified reason.
EID-6123	The OSI request can not be completed successfully.	A communication failure occurred.
EID-6124	The ALS recovery pulse interval is invalid.	Refer to the error message text.
EID-6125	The ALS recovery pulse duration is invalid.	Refer to the error message text.
EID-6126	The current setting does not support the specified ALS mode.	Refer to the error message text.
EID-6127	All enabled routers are required to have the same area.	Refer to the error message text.
EID-6128	A software download is in progress. Configuration changes that result in a card reboot cannot take place during a software download. Please try again after the software download is done.	Refer to the error message text.
EID-6129	The payload configuration and card mode are incompatible.	Refer to the error message text.
EID-6135	A DCC is present.	A data communication channel (DCC) already exists.
EID-6136	An error occurred during provisioning: {0}	CTC was not able to provision the specified port or card.
EID-6137	Multishelf cannot be disabled. {0}	Multishelf is not supported on equipment, is already disabled, or modules on the shelf are currently in use.
EID-6138	The LAN configuration is invalid.	Verify the LAN configuration.
EID-6139	Invalid card(s) are present. Please remove all non-MSTP cards and try again.	Non-DWDM cards cannot be added to an a DWDM node. Remove the cards.

Error/Warning ID	Error/Warning Message	Description
EID-6140	The shelf identifier for a subtended shelf cannot be provisioned through CTC. It must be changed using the LCD.	Refer to the error message text.
EID-6143	The DHCP server could not be changed.	Refer to the error message text.
EID-6144	The port provisioning cannot be changed when the port media is Undefined.	If the port is not pre-provisioned with the type of media that is going to be inserted, you cannot access any of the existing values for the port.
WID-6145	OSPF on LAN should only be enabled when the LAN routers run OSPF. Otherwise, the node will not be reachable from outside its subnet. RIP implementation only advertise routes in one direction to connected routers. It does not learn or distribute routes advertised by other routers. Also note that enabling OSPF on the LAN will temporarily cause the current list of static routes to stop being advertised to remote nodes and only be used locally.	Refer to the warning message text.
WID-6146	Deleting the protection group while in a switched state might cause a loss of traffic. It is recommended that you verify switch states before proceeding.	Refer to the warning message text.
EID-6149	The LAPD MTU size must be greater than or equal to the {0} LSP buffer size {1}. Alternatively, you can decrease the {0} LSP buffer size to {2}.	Refer to the error message text.
EID-6150	The value is out of range.	Enter a value that is within the range.
EID-6151	The minimum span loss must be less than the maximum span loss.	Refer to the error message text.
EID-6152	The "Use NTP/SNTP Server" field is checked. Enter the NTP/SNTP server IP address or server name.	Enter the NTP/SNTP server name. To leave this field empty, uncheck the Use NTP/SNTP Server" and proceed.
EID-6153	The maximum frame size is invalid.	Refer to the error message text.
EID-6154	To combine unidirectional two-port provisioning and autonegotiation on the same port, autonegotiation must be set first.	Refer to the error message text.
EID-6155	Transponder mode cannot be provisioned with circuits on the card.	Refer to the error message text.
EID-6156	The transponder configuration is invalid.	The transponder is not configured properly.

Error/Warning ID	Error/Warning Message	Description
EID-6157	The watermark values are either out of range or inconsistent.	Enter valid watermark values.
EID-6179	The 1+1 protection group is not optimized.	Refer to the error message text.
EID-6196	The equipment has failed or is missing.	Operation is requested on a failed or missing equipment.
EID-6197	Attributes cannot be changed when the port administrative state is {0}.	You cannot change the attributes when the port is in the specified administrative state.
WID-6204	This action will cause the node to reboot. When provisioning in single-shelf mode, Shelf {0} of the node that you connect to must be properly preprovisioned or you will lose traffic. Use the LCD to return to single-shelf mode. CTC cannot be used for this. Changing from subtended shelf mode to single-shelf mode could be traffic-affecting.	Refer to the warning message text.
EID-6205	The interlink port is not provisioned.	The user creates an ADM peer group without interlink ports.
EID-6206	The ADM peer group has already been created on the peer card.	The user creates an ADM peer group involving an ADM card inserted in a peer group.
EID-6207	This card is not in the ADM peer group.	The selected ADM card is not involved in an ADM peer group.
EID-6208	The payload is not OTU2.	Refer to the error message text.
EID-6209	The side is already defined by the node.	During the creation of a side on node, a side is already defined.
EID-6210	No side was selected.	The user requests an operation on a side, but no side is selected.
EID-6211	The side was not deleted.	CTC could not delete the selected side successfully.
EID-6212	One of the ports is connected to a patchcord or virtual link.	An operation on a port was not performed because the port is connected to a patchcord or a virtual link.
EID-6213	It is not possible to associate the side to the two ports.	During the creation of a side it is not possible to associate the selected ports to the new side.

Error/Warning ID	Error/Warning Message	Description
EID-6214	The port is already assigned to a side.	The selected port is already assigned to a side.
EID-6215	Error provisioning the CVLAN ID. Enter a valid number or range between 0 and 4094.	The entered CVLAN ID was out of the admitted range.
EID-6216	Changing card will reset the optical thresholds to the default setting and may affect the optical connection. The optical connection will work only if the optical performance is compatible with {0} card. Please check the network design.	Refer to the error message text.
EID-6217	You cannot delete the {0} {1}.	You cannot delete {0} {1} because it is part of an ADM peer group or one or more circuits are provisioned on it.
EID-6218	Invalid Ethernet duplex value	the Ethernet duplex value is invalid. Enter again.
EID-6219	Invalid committed info rate	The committed info rate value is invalid. Enter again.
EID-6220	Invalid Ethernet speed value	The Ethernet speed value is invalid. Enter again.
EID-6221	Invalid mtu value	The MTU value is invalid. Enter again.
EID-6222	Invalid flow control value	The flow control value is invalid. Enter again.
EID-6223	Invalid Network Interface Mode	The network interface mode value is invalid. Enter again.
EID-6224	Invalid ingress COS value	The ingress COS value is invalid. Enter again.
EID-6225	Invalid ethertype value	The Ethertype value is invalid. Enter again.
EID-6226	Invalid buffer size value	The Buffer size value is invalid. Enter again.
EID-6227	Invalid egress QOS value	The egress QOS value is invalid. Enter again.
EID-6228	Invalid QinQ working Mode	The QinQ working mode is invalid. Enter again.
EID-6229	Configured protection status Not Supported	The protection status is not supported
EID-6230	The number of provisioned entries exceeds the limit	Refer to the error message text.

Error/Warning ID	Error/Warning Message	Description
EID-6231	This is not a valid VLAN ID.	Entered VLAN ID is not present in the database file.
EID-6232	The VLAN remapping ID is not allowed.	Refer to the error message text.
EID-6233	The CVLAN is duplicated.	You cannot have identical CVLAN IDs.
EID-6234	The VLAN ID is out of range.	The VLAN ID entered is out of range.
EID-6235	This is not a valid VLAN name.	The entered VLAN name exceeds the number of characters (32) allowed.
EID-6236	The protected VLAN number exceeds the maximum allowed.	The user enters more than 256 protected VLAN in the VLAN database.
EID-6237	The port is not in OOS disabled admin state	Refer to the error message text.
EID-6238	The VLAN ID is in use.	The entered VLAN ID is in use by a node.
EID-6239	APC wrong node side.	Refer to the error message text.
EID-6240	You cannot change the Admin State for an interlink port when it is part of an ADM peer group. This operation is not supported.	Refer to the error message text.
EID-6242	The protection slot is invalid.	You must select a valid protection slot.
EID-6243	The {0} address of {1} is invalid.	Refer to the error message text.
EID-6244	The mask of {0} is invalid.	The mask of the specified value is not valid.
EID-6245	The cost must be between 1 and 32767.	Refer to the error message text.
EID-6246	The {0} address cannot be {1}.	Refer to the error message text.
EID-6247	The authentication type is invalid.	Enter a valid authentication type.
EID-6248	The cost must between 1 and 15.	Refer to the error message text.
EID-6249	The port has a cross-connect.	Refer to the error message text.
EID-6250	The reversion time is invalid.	The reversion time is invalid. Enter again.
EID-6251	Invalid Margin For Span Aging. Value is not in the range 0 - 10.	Enter a value between 0 and 10.

Error/Warning ID	Error/Warning Message	Description
EID-6252	The data cannot be retrieved because ANS parameters cannot be calculated on the node in its current configuration.	Refer to the error message text.
EID-6253	Invalid Margin For Span Aging.	Refer to the error message text.
EID-6254	SDH mode does not support timing references.	Timing reference is not supported by SDH mode.
EID-6255	Only DS1 interfaces with ESF line types support timing references.	Refer to the error message text.
EID-6256	sendDoNotUse and sendDoNotUseFF are mutually exclusive.	Refer to the error message text.
EID-6257	The termination is already in use.	Refer to the error message text.
EID-6258	The side is carrying services or traffic.	Refer to the error message text.
EID-6259	A pluggable module on Port 22 remains unmanaged.	Refer to the error message text.
EID-6260	You cannot delete this port. There was a severe architectural error related to the index of the pluggable trunk port object. Please contact technical support for assistance.	Refer to the error message text.
EID-6261	This is not a valid VLAN ID. The VLAN database is empty.	The user adds a row without a valid VLAN database loaded.
EID-6263	The equipment requires two slots.	The user provisions a double footprint card in a single slot.
EID-6264	The patchcord is duplicated.	Refer to the error message text.
EID-6265	The wavelength is in use by an OCH trail, a virtual link, or an internal patchcord.	Refer to the error message text.
EID-6266	The card cannot be changed because the port has not been provisioned.	Refer to the error message text.
EID-6267	Each port can have a maximum of 8 MAC addresses.	Refer to the error message text.
EID-6268	This server trail does not have a valid start or end.	Refer to the error message text.
EID-6269	The maximum number of server trails is 3743.	Refer to the error message text.
EID-6270	A unique server trail ID could not be allocated.	Refer to the error message text.
EID-6271	The server trail already exists.	Refer to the error message text.
EID-6272	The server trail size must not exceed the port bandwidth.	Refer to the error message text.

Error/Warning ID	Error/Warning Message	Description
EID-6273	An OCH Trail circuit is active on the trunk port. To modify the ITU-T G.709 parameter, the circuit must be out of service.	Refer to the error message text.
EID-6274	Unable to restore this database: The software version cannot be obtained from the node. Please try again.	The user tries to restore a database on a node, but its not possible to get the software version from it.
EID-6275	You cannot change this parameter. The port is part of an active circuit.	Certain parameters like Port Rate and Admin State cannot be changed when the port is part is part of an active circuit. Delete all the circuits on the port before changing admin state of the port.
EID-6276	APC is disabled. APC Correction Skipped. Override cannot be performed.	Refer to the error message text.
EID-6277	There are no alarm conditions available to run APC Correction Skipped Override.	Refer to the error message text.
EID-6278	APC Correction Skipped Override is not supported for this card.	Refer to the error message text.
EID-6279	Protection cannot be disabled when the FPAS alarm is active.	Refer to the error message text.
WID-6280	Any configuration change will be lost and the operation is traffic affecting.	Refer to the error message text.
EID-6281	The port is involved in a protection group. The protected port is not in the {0} administrative state	Change the port state to administrative.
WID-6282	Forcing FPGA update will be traffic-affecting.	Refer to the error message text.
WID-6283	Enabling ALS on a DWDM trunk port that is connected to a channel filter will result in a conflict with the ALS on the amplifier card or with the VOA startup process. Is it OK to continue?	Refer to the error message text.
WID-6284	Changing the timing standard will re-initialize the shelf timing and might affect traffic. OK to continue?	Refer to the error message text.
WID-6285	Since you are changing the IP address of one node containing some PPC terminations, you are also requested to run the PPC Repair tool in order to fix the IP addresses stored in the nodes connected by these PPCs	Refer to the error message text.
EID-6286	The port type cannot be changed because the port has been deleted.	Refer to the error message text.

Error/Warning ID	Error/Warning Message	Description
EID-6287	You cannot edit the {0} {1}.	Port rate of Optical and Electrical ports cannot be changed while circuits are provisioned on them.
EID-6288	The BERT configuration is invalid.	Refer to the error message text.
EID-6289	The BERT mode is not yet configured	Refer to the error message text.
WID-6290	The BERT mode is configured in unframed format	Refer to the error message text.
WID-6291	Port has circuits; configuring the BERT mode will disrupt normal traffic.	Refer to the error message text.
EID-6292	The alarm type name cannot exceed 20 characters	Refer to the error message text.
EID-6294	The alarm type name contains invalid characters. Only the following characters are valid: 0-9, A-z, a-z and "-".	Refer to the error message text.
EID-6295	The alarm type is in use and cannot be deleted.	Refer to the error message text.
EID-6296	Maximum number of alarm types that can be added cannot exceed 50.	Refer to the error message text.
EID-6297	Hard coded alarm types cannot be deleted.	Refer to the error message text.
EID-6298	The alarm type already exists.	Refer to the error message text.
EID-6299	The alarm type does not exist.	Refer to the error message text.
EID-6300	Selective auto negotiation is allowed only when selected speed and duplex modes are non-auto. Click "Reset" to revert the changes.	Refer to the error message text.
WID-6301	Selective auto negotiation applies only to copper SFPs.	Refer to the error message text.
EID-6302	Users are not allowed to perform this operation.	When logged in as a maintenance user provisioning operation is not allowed.
EID-6303	The ITU-T G.709 configuration cannot be disabled when Fast Protection is enabled.	Refer to the error message text.
EID-6304	Users are not allowed to perform this operation.	Refer to the error message text.
EID-6305	The view could not be deleted.	Refer to the error message text.
EID-6306	The ITU-T G.709 configuration cannot be disabled when Fast Protection is enabled.	Refer to the error message text.
WID-6307	You have only selected one trunk-to-trunk patchcord. For complete deletion, you must select both patchcords that are attached to the 10GE_XP/GE_XP cards. Do you want to continue?	Refer to the warning message text.

Error/Warning ID	Error/Warning Message	Description
WID-6308	You have only selected one trunk-to-OCH patchcord. For complete deletion, you must select both patchcords that are attached to the TXP/MXP card. Do you want to continue?	Refer to the warning message text.
EID-6309	OCHNC circuits, OSC terminations, synchronization sources and protection groups must be removed before you can remove this patchcord.	Refer to the error message text.
EID-6310	The Committed Info Rate value must be in range [0-100].	Refer to the error message text.
EID-6311	The MTU value must be in range [64-9700].	Refer to the error message text.
EID-6312	The multicast IP address must be in range [224.0.0.0 - 239.255.255.255] Excluding the following IP address subranges [(224-239).(0/128).0.(0-255)]	Refer to the error message text.
EID-6313	The multicast IP address count must be in range [1-256]	Refer to the error message text.
EID-6314	Could not retrieve TTY session for the chosen CRS.	Refer to the error message text.
EID-6315	CRS provisioning failed. {0}	Refer to the error message text.
EID-6316	The chosen node is not a CRS-1.	Refer to the error message text.
EID-6317	The value specified for IPv6 Address or IPv6 Default Router is invalid.	Refer to the error message text.
EID-6318	The value specified for Prefix Length is invalid. Valid range of values is 0 to 128.	Refer to the error message text.
EID-6319	IPv6 mode can be enabled only if SOCKS and firewall are enabled on the node.	Refer to the error message text.
EID-6320	IPv6 mode cannot be enabled on a node if RIP is enabled.	Refer to the error message text.
EID-6321	IPv6 mode cannot be enabled on a node if 'OSPF on LAN' is enabled.	Refer to the error message text.
EID-6322	IPv6 Address cannot be specified for {0} when IPv6 mode is not enabled on the node.	Refer to the error message text.
EID-6323	CTC was unable to delete SnmpV3 Target.	Refer to the error message text.
EID-6324	The card mode is invalid in this configuration.	Refer to the error message text.
EID-6325	SW version mismatch on node {0}: found {1}, expected {2}.	Refer to the error message text.

Error/Warning ID	Error/Warning Message	Description
EID-6326	The CRS node {0} version[{1}] is greater than the supported version[{2}]. The creation of ochtrail circuits between CRS nodes will not be disabled, but there could be unexpected behaviors.	Refer to the error message text.
EID-6327	The end point of patchcord have an incompatible wavelength.	Refer to the error message text.
EID-6329	Protection/AIS action cannot be both set to squelch.	Refer to the error message text.
EID-6330	The node failed to restart the Pseudo IOS CLI service on the selected port. Try using another unreserved port that is not being used within the 1024 - 65535 range.	Refer to the error message text.
EID-6331	That port is already in use. Also note that the Pseudo IOS port may not be changed if any Pseudo IOS connections are currently open.	Refer to the error message text.
WID-6332	All previously configured IPv6 destinations will become unreachable if IPv6 mode is disabled. It is recommended that you remove all IPv6 related provisioning before disabling IPv6 mode. Do you want to continue?	Refer to the warning message text.
WID-6333	The NE default {0} not available in the selected NE Defaults Tree.	Refer to the warning message text.
WID-6334	Could not find the NE default {0}.	Refer to the warning message text.
WID-6335	CTC was unable to create a new Target account.	Refer to the warning message text.
WID-6336	Changing the card to EFEC mode will cause the ports 1 and 2 to be disabled. Do you want to continue?	Refer to the warning message text.
WID-6337	CE-MR-10/CE-MR-6 card does not validate the Ethernet FCS when traffic is received from optical side. This can result in errored frames from optical side being forwarded to the peer device via front ports. It would be left to the peer device to detect the errors and discard the frames. It is suggested to enable the FCS option on both ends of the circuit. The GFP FCS will be used to discard errored frames. The discarded frames will be accounted under the performance pane for the POS port.	Refer to the warning message text.
WID-6338	Ingress COS setting is not compatible with QinQ mode.	Refer to the warning message text.
WID-6339	Some circuits may become partial as part of this upgrade and would need to be reconfigured.	Refer to the warning message text.

Error/Warning ID	Error/Warning Message	Description
WID-6340	One or more QinQ rules have not been deleted because they are not related to the current circuit.	Refer to the warning message text.
WID-6341	The Functional view on {0} is disabled.	Refer to the warning message text.
WID-6342	Changing the {0} settings might be traffic affecting. Do you want to continue?	Refer to the warning message text.
WID-6343	The selected file name is too long. File names (including the full path) must be less than 254 characters. Please enter a valid file name.	Refer to the warning message text.
EID-6344	It is detected a shelf mismatch condition.	Refer to the error message text.
EID-6345	The line termination is invalid.	Refer to the error message text.
EID-6346	The overhead is not supported.	Refer to the error message text.
EID-6347	A patchcord was expected for a successful operation.	Refer to the error message text.
EID-6348	A Virtual link already exists on the same path.	Refer to the error message text.
EID-6349	The overhead creation has failed.	Refer to the error message text.
EID-6350	The unprotected line is not present	Refer to the error message text.
EID-6351	The port status is active.	Refer to the error message text.
EID-6352	IPv4 access cannot be disabled when IPv6 mode is not enabled on the node.	Refer to the error message text.
EID-6353	IPv4 access cannot be disabled when the node is in Multishelf configuration.	Refer to the error message text.
EID-6354	Disabling IPv4 access may lead to loss of communication with the node. Make the change anyway?	Refer to the error message text.
EID-6355	IPv6 access cannot b disabled when IPv4 Access is disabled on the node.	Refer to the error message text.
EID-6356	Multishelf configuration cannot be enabled when IPv4 Access is disabled on the node.	Refer to the error message text.
EID-6357	The Multicast SVLAN field can be modified only when the MVR feature is disabled.	Refer to the error message text.
EID-6358	Too many TRANSLATE QinQ rules per port with MVR feature enabled.	Refer to the error message text.
EID-6359	The PLIM {0} is part of an OCH Trail circuit and its configuration cannot be changed.	Refer to the error message text.

Error/Warning ID	Error/Warning Message	Description
EID-6360	The fiber cut restore operation did not succeed on {1}. {0}	Refer to the error message text.
EID-6361	The resource is already in use, please retry later.	Refer to the error message text.
EID-6362	Request timed out, please retry.	Refer to the error message text.
EID-6363	An internal communication error was encountered while retrieving values. Please retry.	Refer to the error message text.
EID-6364	Could not perform the requested operation because of a CRS communication error.	Refer to the error message text.
EID-6365	Could not perform the requested operation on PLIM {0} because that port is already in an LMP data link with neighbor {1}.	Refer to the error message text.
EID-6366	The IP address {0} was not found in the CRS ARP table.	Refer to the error message text.
WID-6367	This operation will also change the CRS configuration. Is it OK to continue?	Refer to the error message text.
WID-6368	This operation will also change the Router configuration. Moreover, it requires the PLIM shutdown and may be SERVICE AFFECTING. Is it OK to continue?	Refer to the error message text.
EID-6369	The rollback operation has failed.	Refer to the error message text.
EID-6370	The requested operation is not authorized on {0}. Please check task privileges.	Refer to the error message text.
WID-6371	Since you have changed the IP address of one node containing Server Trail terminations, you should also fix the IP addresses stored in the nodes connected by these Server Trails. Run the Server Trail Repair tool to fix these IP addresses.	Refer to the error message text.
EID-6372	A Server Trail with the requested ID and old peer IP Address does not exist.	Refer to the error message text.
WID-6373	AIS Squelch action(a link Integrity attribute) should not be simultaneously set	Refer to the error message text.
EID-6374	The selected SVLAN is already used for MVR.	Refer to the error message text.

Error/Warning ID	Error/Warning Message	Description
EID-6375	Missing L2 internal patchcords between XP cards.	Refer to the error message text.
EID-6376	Profile cannot be mapped because the SVLAN is not enabled on the port.	Refer to the error message text.
EID-6377	The configuration must be applied on the working interface in case of protection group.	Refer to the error message text.
EID-6378	Squelch protection action and Auto mode are not compatible in case of L2 1+1.	Refer to the error message text.
EID-6379	The NTP/SNTP server and the Backup NTP/SNTP servers cannot be the same.	Refer to the error message text.
EID-6380	Multishelf VLAN range must be in range of {0} to {1}.	Refer to the error message text.
WID-6381	Changing the OTU2_XP card mode to 10GE LAN to WAN will reboot the card. Do you want to continue?	Refer to the error message text.
WID-6382	Changing the OTU2_XP card mode from 10GE LAN to WAN will reboot the card and delete the pluggable ports 1 and 3. Do you want to continue?	Refer to the error message text.
EID-6383	The board is busy. Please retry later.	Refer to the error message text.
EID-6384	The value "{0}" must be between {1} and {2}.	Refer to the error message text.
EID-6385	The value "{0}" has too many decimal points [xx.0 .. xx.9].	Refer to the error message text.
EID-6386	The value "{0}" must be a float between {1} and {2}.	Refer to the error message text.
EID-6387	The value "{0}" must be a integer between {1} and {2}.	Refer to the error message text.
EID-6388	"{0}" is not a valid enumerated value.	Refer to the error message text.
EID-6389	Power fail low TCA is greater than high TCA.	Refer to the error message text.
EID-6390	Error while setting DISABLE FEC on {0}.	Refer to the error message text.
EID-6391	Error while setting STANDARD FEC on {0}.	Refer to the error message text.
EID-6392	Error while setting ENHANCED FEC on {0}.	Refer to the error message text.
EID-6393	Error while setting SD BER on {0}.	Refer to the error message text.

Error/Warning ID	Error/Warning Message	Description
EID-6394	The maximum number of CVLAN ranges cannot exceed 48 in selective QinQ mode.	Refer to the error message text.
EID-6397	Unable to update the FPGA as the STANBY CTX is not ready.	Retry later.
EID-6398	Unable to update the FPGA as the database is busy saving recent modifications.	Retry later.
EID-6482	The storm control threshold value must be in range [{0}-{1}].	Refer to the error message text.
EID-6487	Error while setting DISABLE FEC on {0}.	Refer to the error message text.
EID-6488	Error while setting ENHANCED FEC on {0}.	Refer to the error message text.
EID-6489	Error while setting STANDARD FEC on {0}.	Refer to the error message text.
EID-6490	Error while setting SD BER on {0}.	Refer to the error message text.
EID-6545	An error occurred while reading actual channels.	Refer to the error message text.
EID-6546	An error occurred while setting actual channels.	Refer to the error message text.
EID-6547	Valid License is not available on this card.	Retry after installing a permanent license.
EID-6548	License Operation Error.	Refer to the error message text.
EID-6549	License is not supported.	The license you are installing is not supported on the card.
EID-6550	The Product ID of the card does not support Licensing.	Licensing is not supported on the card.
EID-6551	The card is not in provisioned state, hence this license data cannot be fetched currently	Retry after the card is provisioned.
EID-6552	License operation failed due to Communication failure with the line card.	Check if the line card is installed correctly.
EID-6553	License file size has exceeded the limit	Refer to the error message text.
EID-6590	Unsupported operation	Refer to the error message in the text. This error occurs when the desired operation is not supported or an invalid operation for the desired feature is performed.
EID-6601	The client ports are provisioning on the ports before deleting.	Refer to the error message text.

Error/Warning ID	Error/Warning Message	Description
EID-6602	Incompatible Operating Mode is provisioned. The Following Operating Modes are not Compatible: Transponder (4GFC TXP) with 8GFC Transponder (8GFC TXP).	Refer to the error message text.
EID-6626	UNI Wrong Configuration.\n {0}	Interface is already created or wrong parameters configured.
EID-6627	The operation is not supported	Performing an unsupported operation.
EID-6628	LAN WAN Enabled on the Port.	LAN WAN is enabled on the Port.
EID-6629	Operating mode is not provisioned on the PPM.	The PPM does not have any mode provisioned. Create a card mode for the ports before creating the payload.
EID-6630	The FEC settings are incompatible.	FEC mode is not configured correctly for the protection mode being provisioned during circuit creation.
EID-6631	Operation is not Supported. Valid License is not available on Card/Peer Combination.	Valid license is not installed on the peer card for the operation mode being provisioned.

The following table lists the error messages for RAMAN-CTP, RAMAN-COP, EDRA-1-xx, and EDRA-2-xx cards.

Error	Error Message	Cause/Solution
Error RC01	Unexpected internal Error	If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).
Error RC02	Raman card is not plugged or not ACTIVE	Ensure the Raman card is properly plugged in and is active.
Error RC03	Raman pumps are not ON (either OFF or APR)	Check for fiber continuity and connectors.
Error RC04	Target Raman Gain/Tilt not set by ANS	Ensure ANS parameters are properly set by ANS.
Error RC05	No reply received from facing node (nodes communication error)	The OSC PPP is down or there is no communication between nodes.

Error	Error Message	Cause/Solution
Error RC06	Cards in facing node are missing or busy - in use by another calibration or OTDR scan running	Check if an OTDR scan is running from either end of span or a Raman calibration is under progress
Error RC07	Raman Card is busy - in use by another calibration (another side in this node) or OTDR scan running	
Error RC08	Failed turning on/off probe output power in facing node	Depending on the Raman card that is installed on the facing node, the card that actually generates the probe signal is : EDRA-1-xx to EDRA-1-xx in the other side EDRA-2-xx to EDRA-2 -xx itself RAMAN-CTP - to the booster card launching power into the fiber. Verify that there are no ports in disabled state. Ensure all patchcords from the Raman card to the other card are generating the probe signal.
Error RC09	Failed enabling/disabling probe power into fibre in facing node	If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).
Error RC10	Failed setting Raman Pumps to calibration power	
Error RC11	Failed setting Raman Pumps to stand-by power	
Error RC12	Failed setting Raman Pumps to ANS target power	
Error RC13	Measured probe input power level on Line-RX is below measurable level	The Raman card did not detect any probe signal from the other node indicating a failure in the LINE-RX photodiode. The Raman card needs to be replaced.
Error RC14	Measured input Raman ASE on Line-RX is below measurable level (no Raman amplification!)	After turning on the Raman pumps, no input ASE is detected. There may be a problem with the transmission fiber. Inspect all connectors and verify losses between Raman card LINE-RX connector and the transmission fiber input.

Error	Error Message	Cause/Solution
Error RC15	Cards in facing node are not suitable for Raman calibration	The probe signal contains channels that do not cover the entire optical band (for example, all channels at one end of the spectrum). Add more channels to the probe signal or disable the channels so that Raman calibration can run using ASE.
Error RC16	Probe signal used for calibration has changed (e.g. channels count has changed)	This is a transient condition. The number of active channels in the span has changed during the calibration. The calibration will be automatically retried later.
Error RC17	Raman gain is lower than managed minimum	The measured Raman gain is outside the range managed by the Raman calibration. Fiber may need to be replaced. Check the connectors and losses between Raman card LINE-RX connector and transmission fiber input.
Error RC18	Raman gain is higher than managed maximum	
Error RC19	Force APR is set on Raman Card	Check if APR is forced on the Raman card.