Cisco ONS 15454 SDH Troubleshooting Guide

Product and Documentation Release 6.0
Last Updated: September 2010

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

Text Part Number: 78-16895-01

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

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

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

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

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

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

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

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

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

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.

Cisco ONS 15454 SDH Troubleshooting Guide, Release 6.0

CONTENTS

FIGURES

About this Guide

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:

Revision History

Date	Notes
March 2007	Revision History Table added for the first time.
August 2007	Replaced TX Power High column name with OPT-HIGH in the HI-TX Power section of the Alarm Troubleshooting chapter.
October 2007	• Updated the section Side Switch the Active and Standby Cross-Connect Cards, in the chapter Alarm Troubleshooting. Added a note, caution, and rules for removing an Active Cross Connect Card. • Updated About this Guide chapter.
June 2008	Updated FAILTOSW alarm in Chapter 2, Alarm Troubleshooting.
February 2009	Updated PORT-MISMATCH alarm details in Chapter 2, Alarm Troubleshooting.
June 2009	Updated PWR-FAIL-A, PWR-FAIL-B, PWR-FAIL-RET-A, and PWR-FAIL-RET-B alarm details in Chapter 2, Alarm Troubleshooting.
July 2009	• Updated the COMIOXC alarm details in Chapter 2, Alarm Troubleshooting. • Updated the description of GFP-LFD alarm in Chapter 2, Alarm Troubleshooting.
August 2009	• Updated the shelf assembly part number in Chapter 2, Alarm Troubleshooting. • Updated MEM-GONE alarm description in Chapter 2, Alarm Troubleshooting.
October 2009	• Updated the description and procedure in BKUPMEMP alarm section in Chapter 2, Alarm Troubleshooting. • Added a new procedure to reset a standby TCC2/TCC2P card.
November 2009	• Removed AUTOSW-PDI-SNCP, INCOMPATIBLE-SEND-PDIP, and PDI alarms from the chapter Alarm Troubleshooting. • Updated the card details for LCAS alarms in Chapter 2, Alarm Troubleshooting.
February 2010	Changed the BIEC parameter to BIT-EC in Chapter 5, “Performance Monitoring”.
July 2010	Updated table in Chapter Error Messages.
September 2010	Updated the “Clear the COMIOXC Alarm” procedure in the chapter, “Alarm Troubleshooting”.

Document Objectives

This guide gives general troubleshooting instructions, alarm troubleshooting instructions, equipment replacement instructions, and a list of error messages that apply to the ONS equipment. This information is contained in four chapters. Use this guide in conjunction with the appropriate publications listed in the Related Documentation section.

Audience

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

Document Organization

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

- Chapter 1, "General Troubleshooting," provides methods to discover hardware errors, such as failed ports, that adversely affect signal traffic; it also gives typical software problems that occur and their solutions.
- Chapter 2, "Alarm Troubleshooting," provides indexes, descriptions, and troubleshooting methods for all alarms and conditions generated by the ONS system.
- Chapter 3, "Transients Conditions," describes transient (temporary) conditions.
- Chapter 4, "Error Messages," provides a comprehensive list of all ONS system error messages and their identification numbers.
- Chapter 5, "Performance Monitoring," provides performance monitoring definitions for all Cisco ONS 15454 SDH cards.
- Chapter 6, "SNMP," describes Simple Network Management Protocol as implemented by the ONS 15454 SDH.

Related Documentation

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

- *Cisco ONS 15454 SDH Procedure Guide*
  Provides procedures to install, turn up, test, and maintain an ONS 15454 SDH node and network.
- *Cisco ONS 15454 SDH Reference Manual*
  Provides detailed card specifications, hardware and software feature descriptions, network topology information, and network element defaults.
- *Cisco ONS 15454 SDH TL1 Command Guide*
  Provides a full TL1 command and autonomous message set including parameters, AIDs, conditions and modifiers for the Cisco ONS 15454 SDH.
- *Cisco ONS 15454 SDH TL1 Reference Guide*
  Provides TL1 general information, procedures, and errors for the Cisco ONS 15454 SDH.

- *Ethernet Card Software Feature and Configuration G uide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*
  Provides software features for all Ethernet cards and configuration information for Cisco IOS on ML-Series cards.
- *Release Notes for the Cisco ONS 15454 SDH Release 6.0*
  Provides caveats, closed issues, and new features and functionality information.

Document Conventions

This publication uses the following conventions:

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

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

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

Warning **IMPORTANT SAFETY INSTRUCTIONS**

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

SAVE THESE INSTRUCTIONS

Waarschuwing **BELANGRIJKE VEILIGHEIDSINSTRUCTIES**

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

BEWAAR DEZE INSTRUCTIES

Varoitus **TÄRKEITÄ TURVALLISUUSOHJEITA**

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

SÄILYTÄ NÄMÄ OHJEET

Attention **IMPORTANTES INFORMATIONS DE SÉCURITÉ**

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

CONSERVEZ CES INFORMATIONS

Warnung **WICHTIGE SICHERHEITSHINWEISE**

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

BEWAHREN SIE DIESE HINWEISE GUT AUF.

Avvertenza **IMPORTANTI ISTRUZIONI SULLA SICUREZZA**

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

CONSERVARE QUESTE ISTRUZIONI

Advarsel **VIKTIGE SIKKERHETSINSTRUKSJONER**

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

TA VARE PÅ DISSE INSTRUKSJONENE

Aviso **INSTRUÇÕES IMPORTANTES DE SEGURANÇA**

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

GUARDE ESTAS INSTRUÇÕES

¡Advertencia! **INSTRUCCIONES IMPORTANTES DE SEGURIDAD**

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

GUARDE ESTAS INSTRUCCIONES

Varning! **VIKTIGA SÄKERHETSANVISNINGAR**

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

SPARA DESSA ANVISNINGAR

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 중요 안전 지침

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

이 지시 사항을 보관하십시오.

Aviso **INSTRUÇÕES IMPORTANTES DE SEGURANÇA**

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

GUARDE ESTAS INSTRUÇÕES

Advarsel **VIGTIGE SIKKERHEDSANVISNINGER**

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

GEM DISSE ANVISNINGER

تحذير **إرشادات الأمان الهامة**

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

قم بحفظ هذه الإرشادات

Upozorenje **VAŽNE SIGURNOSNE NAPOMENE**

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

SAČUVAJTE OVE UPUTE

Upozornění **DŮLEŽITÉ BEZPEČNOSTNÍ POKYNY**

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

USCHOVEJTE TYTO POKYNY

Προειδοποίηση

ΣΗΜΑΝΤΙΚΕΣ ΟΔΗΓΙΕΣ ΑΣΦΑΛΕΙΑΣ

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

ΦΥΛΑΞΤΕ ΑΥΤΕΣ ΤΙΣ ΟΔΗΓΙΕΣ

אזהרה

הוראות בטיחות חשובות

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

שמור הוראות אלה

Opomena

ВАЖНИ БЕЗБЕДНОСНИ НАПАТСТВИЈА

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

ЧУВАЈТЕ ГИ ОВИЕ НАПАТСТВИЈА

Ostrzeżenie

WAŻNE INSTRUKCJE DOTYCZĄCE BEZPIECZEŃSTWA

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

NINIEJSZE INSTRUKCJE NALEŻY ZACHOWAĆ

Upozornenie

DÔLEŽITÉ BEZPEČNOSTNÉ POKYNY

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

USCHOVAJTE SI TENTO NÁVOD

Obtaining Optical Networking Information

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

Where to Find Safety and Warning Information

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

Cisco Optical Networking Product Documentation CD-ROM

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

Obtaining Documentation and Submitting a Service Request

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

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

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

CHAPTER 1

General Troubleshooting

This chapter provides procedures for troubleshooting the most common problems encountered when operating a Cisco ONS 15454 SDH. To troubleshoot specific ONS 15454 SDH alarms, see Chapter 2, "Alarm Troubleshooting." If you cannot find what you are looking for, contact Cisco Technical Support.

This chapter includes the following sections on network problems:

- 1.1 Troubleshooting Non-DWDM Circuit Paths with Loopbacks, page 1-2—Describes loopbacks and hairpin circuits, which you can use to test circuit paths through the network or logically isolate faults

Note For dense wavelength-division multiplexing (DWDM) network acceptance tests, refer to the "Perform Network Acceptance Tests" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide.* For SDH network acceptance tests, refer to the "Turn Up Network" chapter in the *Cisco ONS 15454 SDH Procedure Guide.*

- 1.2 Troubleshooting Electrical Circuit Paths With Loopbacks, page 1-9—Explains how to use loopback tests described in "1.1 Troubleshooting Non-DWDM Circuit Paths with Loopbacks" to isolate trouble on electrical circuits.
- 1.3 Troubleshooting Optical Circuit Paths With Loopbacks, page 1-38—Explains how to use loopback tests described in "1.1 Troubleshooting Non-DWDM Circuit Paths with Loopbacks" to isolate trouble on STM-N optical circuits.
- 1.4 Troubleshooting Ethernet Circuit Paths With Loopbacks, page 1-61—Explains how to use loopback tests described in the "1.1 Troubleshooting Non-DWDM Circuit Paths with Loopbacks" to isolate trouble on G-Series or CE-Series Ethernet circuits.
- 1.5 Troubleshooting MXP, TXP, or FC_MR-4 Circuit Paths With Loopbacks, page 1-79—Explains how to use loopbacks tests described in"1.1 Troubleshooting Non-DWDM Circuit Paths with Loopbacks" to isolate trouble on muxponder (MXP), transponder (TXP), or Fibre Channel (FC_MR-4) circuits.
- 1.6 Troubleshooting DWDM Circuit Paths With ITU-T G.709 Monitoring, page 1-93—Explains how to utilize performance monitoring (PM) and threshold crossing alerts (TCA) to locate signal degrades on DWDM circuit paths.

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

- 1.7 Using CTC Diagnostics, page 1-101—Provides procedures and guidelines for checking card LED readiness and downloading a diagnostic file for Cisco Technical Support (TAC).

- 1.8 Restoring the Database and Default Settings, page 1-104—Provides procedures for restoring software data and restoring the node to the default setup.
- 1.9 PC Connectivity Troubleshooting, page 1-104—Provides troubleshooting procedures for PC and network connectivity to the ONS 15454 SDH.
- 1.10 CTC Operation Troubleshooting, page 1-110—Provides troubleshooting procedures for Cisco Transport Controller (CTC) login or operation problems.
- 1.11 Circuits and Timing, page 1-124—Provides troubleshooting procedures for circuit creation and error reporting as well as timing reference errors and alarms.
- 1.12 Fiber and Cabling, page 1-128—Provides troubleshooting procedures for fiber and cabling connectivity errors.
- 1.13 Power Supply Problems, page 1-136—Provides troubleshooting procedures for power supply problems.

1.1 Troubleshooting Non-DWDM Circuit Paths with Loopbacks

Use loopbacks and hairpin circuits to test newly created SDH circuits before running live traffic or to logically locate the source of a network failure. All ONS 15454 SDH electrical cards, STM-N cards, G-Series Ethernet cards, MXP, TXP cards, and FC_MR-4 cards allow loopbacks and hairpin test circuits. Other cards that do not allow loopback include E-Series Ethernet, ML-Series Ethernet, and DWDM cards such as Optical Booster (OPT-BST), Optical Preamplifier (OPT-PRE), Optical Service Channel and Combiner/Splitter Module (OSC-CSM), Band Optical Add/Drop Multiplexing (AD-xB-xx.x), and Channel Optical Add/Drop Multiplexing (AD-xC-xx.x) cards.

To create a loopback on a port, the port must be in the Locked,maintenance Admin State and the Locked-Enabled, loopback & maintenance service state.

Caution Facility (line) 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 the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-230. For detailed information, refer to the "Maintain the Node" chapter in the *Cisco ONS 15454 SDH Procedure Guide*.

Caution On STM-N cards, a facility (line) loopback applies to the entire card and not an individual circuit. Exercise caution when using loopbacks on an STM-N card carrying live traffic.

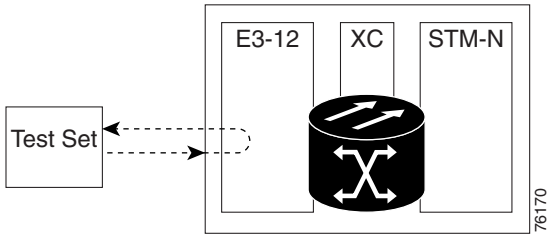
1.1.1 Facility Loopbacks

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

1.1.1.1 General Behavior

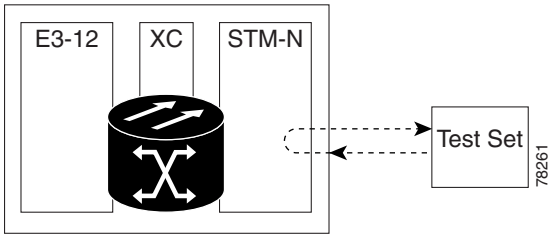
A facility (line) loopback tests the line interface unit (LIU) of a card, the Front Mount Electrical Connection (FMEC) card, and related cabling. After applying a facility loopback on a port, use a test set to run traffic over the loopback. A successful facility loopback isolates the LIU, the Front-Mount Electrical Card (FMEC), or the cabling plant as the potential cause of a network problem. Figure 1-1 shows a facility loopback on an E1-N-14 card.

Figure 1-1 Facility (Line) Loopback Path on a Near-End E1-N-14 Card



To test an optical card LIU, connect an optical test set to the optical port and perform a facility (line) loopback. Or use a loopback or hairpin on a card that is farther along the circuit path. Figure 1-2 shows a facility loopback on an STM-N card.

Figure 1-2 Facility (Line) Loopback Process on a Near-End STM-N Card



In CTC, STM-N cards with facility loopbacks show an icon (Figure 1-3). Loopback icons are not shown on other cards in this release.

Figure 1-3 STM-N Facility Loopback Indicator

Caution Before performing a facility (line) loopback on an optical card, be sure 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 ONS 15454 SDH containing the loopback optical card.

1.1.1.2 ONS 15454 SDH Card Behavior

ONS 15454 SDH port loopbacks either terminate or bridge the loopback signal. All ONS 15454 SDH optical, electrical, Ethernet, MXP, TXP, and FC_MR-4 facility loopbacks are terminated as shown in Table 1-1.

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

Note In Table 1-1, no alarm indication signal (AIS) signal is injected if the signal is bridged. If the signal is terminated, an AIS is injected downstream for all cards except Ethernet cards.

Table 1-1 ONS 15454 SDH Card Facility Loopback Behavior

Card/Port	Facility Loopback Signal
DS3i-N-12	Terminated
E1-N-14	Terminated
G-Series Ethernet	Terminated[1]
MXP, MXPP trunk ports	Bridged
MXP, MXPP client ports	Terminated
TXP, TXPP trunk ports	Bridged
TXP, TXPP client ports	Terminated
STM1-E in STM1-E mode	Terminated
STM1-E ports 9-12 in E4 mode[2]	Terminated

1. G-Series facility loopback is terminated and no AIS is sent downstream. However, the Cisco Link Integrity signal continues to be sent downstream.
2. For the STM1-E card, only Ports 9 through 12 can be placed in E4 mode.

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 will show AS-MT, which means that alarms are suppressed on the facility during loopback.)

In addition to the Conditions window listing, the following behaviors occur:

- If an electrical or optical port is in the Locked-enabled,disabled service state, it injects an AIS signal upstream and downstream.
- When an electrical or optical port is placed in the Locked-enabled,maintenance service state before loopback testing, the port clears the AIS signal upstream and downstream unless there is a service-affecting defect that would also cause an AIS signal to be injected.

MXP and TXP card facility loopbacks behave differently from other ONS 15454 SDH cards. With a client-side MXP or TXP 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 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.

Caution A lock out of protection must be executed before putting a two-fiber or four-fiber BLSR span into a facility loopback state. That is, a span lockout of one side (such as the east side) of a two-fiber BLSR is required before operating a facility loopback on the same (east) side of the ring. A span lockout of one protection side (such as the east protection side) of a four-fiber BLSR is required before operating a facility loopback on the same (east) side working line of the ring. If you do not execute the lockout prior to creating the loopback, the ring can become stuck in an anomalous state after you release the loopback.

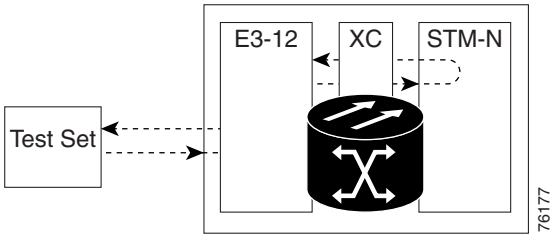
1.1.2 Terminal Loopbacks

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

1.1.2.1 General Behavior

A terminal loopback tests a circuit path as it passes through the XC-VXL cross-connect card loops back from the card with the loopback. Figure 1-4 shows a terminal loopback on an STM-N card. The test-set traffic comes into the electrical card and goes through the cross-connect card to the STM-N card. The terminal loopback on the STM-N card turns the signal around before it reaches the LIU and sends it back through the cross-connect card to the E1-N-14 card. This test verifies that the cross-connect card and terminal circuit paths are valid, but does not test the LIU on the STM-N card.

Figure 1-4 Terminal Loopback Path on an STM-N Card

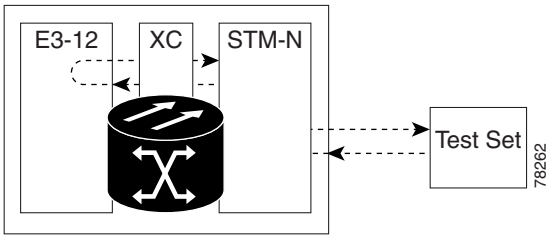


In CTC, STM-N cards with terminal loopbacks show an icon (Figure 1-5). Loopback icons are not shown on other cards in this release.

Figure 1-5 Terminal Loopback Indicator

Figure 1-6 shows a terminal loopback on an E1-N-14 electrical card. The test-set traffic comes in on the STM-N card and goes through the cross-connect card to the E1-N-14 card. The terminal loopback on the E1-N-14 card turns the signal around before it reaches the LIU and sends it back through the cross-connect card to the STM-N card. This test verifies that the cross-connect card and terminal circuit paths are valid, but does not test the LIU on the E1-N-14 card.

Figure 1-6 Terminal Loopback Process on an E1-N-14 Card



1.1.2.2 ONS 15454 SDH Card Behavior

ONS 15454 SDH port loopbacks can either terminate or bridge the loopback signal. In the ONS 15454 SDH system, all optical, electrical, Ethernet, MXP, TXP, and FC_MR-4 facility loopbacks are terminated as shown in Table 1-2. During terminal loopbacks, some ONS 15454 SDH cards bridge the loopback signal while others terminate it.

If a port terminates a terminal or facility 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.

ONS 15454 SDH card terminal loopback bridging and terminating behaviors are listed in Table 1-2.

Note In Table 1-2, no AIS signal is injected if the signal is bridged. If the signal is terminated, an applicable AIS is injected downstream for all cards except Ethernet cards.

Table 1-2 ONS 15454 SDH Card Terminal Loopback Behavior

Card/Port	Terminal Loopback Signal
DS3i-N-12	Bridged
E1-N	Terminated
G-Series Ethernet	Terminated[1]
MXP, MXPP trunk ports	Bridged
MXP, MXPP client ports	Terminated
TXP, TXPP trunk ports	Bridged
TXP, TXPP client ports	Terminated
STM1-E in STM1-E mode	Terminated
STM1-E ports 9-12 in E4 mode[2]	Bridged

1. G-Series Ethernet terminal loopback is terminated and Ethernet transmission is disabled. No AIS is inserted for Ethernet, but a TPTFAIL alarm is raised on the far-end Ethernet port.
2. For the STM1-E card, only Ports 9 through 12 can be placed in E4 mode.

Bridged E1-N-14 and STM-N terminal loopback examples are shown in Figure 1-7 and Figure 1-8.

Figure 1-7 Terminal Loopback on an E1-N-14 Card with Bridged Signal

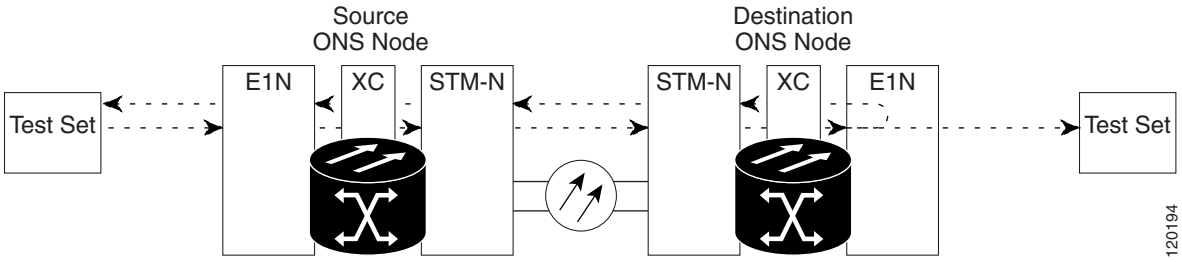
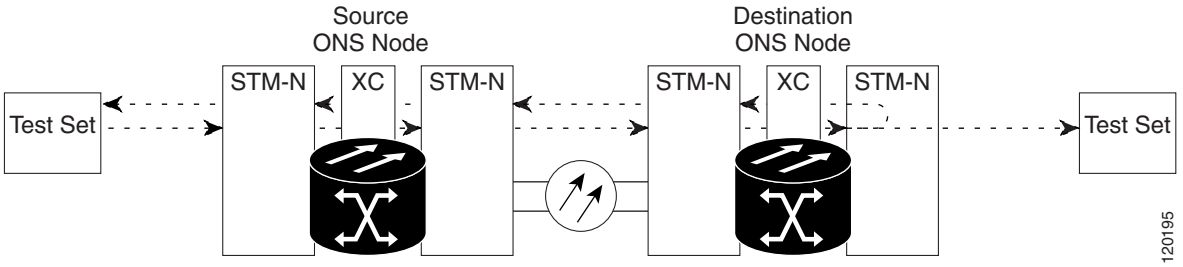


Figure 1-8 Terminal Loopback on an STM-N Card with Bridged Signal



G-Series Ethernet cards placed in terminal loopback have different performance monitoring behavior from other ONS 15454 SDH cards. (For more information about performance monitoring counters, see the Chapter 5, "Performance Monitoring.") Setting a terminal loopback on the G-Series card might not stop the Tx Packets counter or the Rx Packet counters on the CTC card-level view Performance > Statistics page from increasing. The counters can increment even though the loopbacked port has temporarily disabled the transmit laser and is dropping any received packets.

The Tx Packet statistic continues to increment because the statistic is not based on the packets transmitted by the transmit laser but on the transmit signal inside the G-Series card. In normal Unlocked-enabled port operation, the transmit signal being recorded does result in the transmit laser transmitting packets, but in a terminal loopback this signal is being looped back within the G-Series card and does not result in the transmit laser transmitting packets.

The Rx Packet counter might also continue to increment when the G-Series card is in terminal loopback. Receive (Rx) packets from any connected device are dropped and not recorded, but the internally looped back packets follow the G-Series card's normal receive path and register on the Rx Packet counter.

MXP and TXP card facility loopbacks have different service state behaviors and requirements from other ONS 15454 SDH cards. The cards can simultaneously maintain different service states. The following behaviors also occur:

- For TXP and TXPP client-side facility loopback, the client port is in the Locked-enabled,maintenance & loopback service state and the trunk port must be in Unlocked-enabled service state.
- For 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 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 will show AS-MT, which means that alarms are suppressed on the facility during loopback.)

In addition to the Conditions window listing, the following behaviors occur:

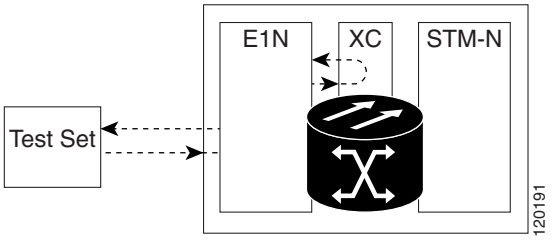
- If an electrical or optical port is in the Locked-enabled,disabled service state, it injects an AIS signal upstream and downstream.
- When an electrical or optical port is placed in the Locked-enabled,maintenance service state before loopback testing, the port clears the AIS signal upstream and downstream unless there is a service-affecting defect that would also cause an AIS signal to be injected.

Caution A lock out of protection must be executed before putting a two-fiber or four-fiber BLSR span into a terminal loopback state. That is, a span lockout of one side (such as the east side) of a two-fiber BLSR is required before operating a facility loopback on the same (east) side of the ring. A span lockout of one protection side (such as the east protection side) of a four-fiber BLSR is required before operating a terminal loopback on the same (east) side working line of the ring. If you do not execute the lockout prior to creating the loopback, the ring can become stuck in an anomalous state after you release the loopback.

1.1.3 Hairpin Circuits

A hairpin circuit brings traffic in and out on an electrical port rather than sending the traffic onto the optical card. A hairpin loops back only the specific VC3 or VC4 circuit and does not cause an entire optical port to loop back, thus preventing a drop of all traffic on the optical port. The hairpin allows you to test a specific VC circuit on nodes running live traffic. Figure 1-9 shows the hairpin circuit path on an E1-N-14 card.

Figure 1-9 Hairpin Circuit Path on an E1-N-14 Card



1.1.4 Cross-Connect Loopbacks

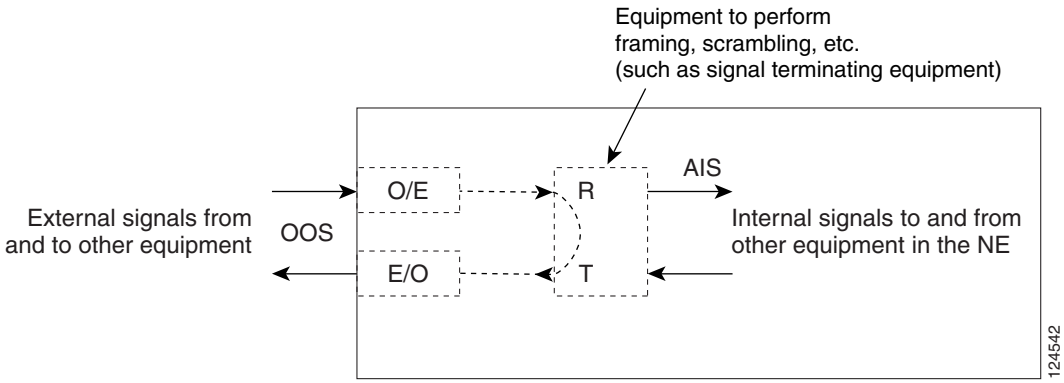
A cross-connect (XC) loopback tests an STM-N circuit path as it passes through the cross-connect card and loops back to the port being tested without affecting other traffic on the optical port. Cross-connect loopbacks are less invasive than terminal or facility loopbacks. Facility and terminal loopback testing and circuit verification often involve taking down the whole line; however, a cross-connect loopback

allows you to create a loopback on any embedded channel at supported payloads of VC3 granularity and higher. For example, you can loop back a single STM-1, STM-4, STM-16, etc. on an optical facility (line) without interrupting the other synchronous transport signal (STS) circuits.

This test can be conducted locally or remotely through the CTC interface without on-site personnel. It takes place only on an STM-N card and tests the traffic path on that VC (or higher) circuit through the port and cross-connect card. The signal path is similar to a facility loopback.

The XC loopback breaks down the existing path and creates a new cross-connect—a hairpin—while the source of the original path is set to inject a line-side "MS-AIS" condition, page 2-173. The loopback signal path and AIS injection are shown in Figure 1-10.

Figure 1-10 NE with SDH Cross-Connect Loopback Function



When creating cross-connect loopbacks, consult the following rules:

- You can create a cross-connect loopback on all working or protect optical ports unless the protect port is used in a 1+1 protection group and is in working mode.
- If a terminal or facility loopback exists on a port, you cannot use the cross-connect loopback.

1.2 Troubleshooting Electrical Circuit Paths With Loopbacks

Facility (line) loopbacks, terminal (inward) loopbacks, and hairpin circuits are often used to test a 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. These procedures apply to DS-3 and E-1 electrical cards.

The example in this section tests an electrical circuit on a two-node multiplex section-shared protection ring (MS-SPRing). Using a series of facility loopbacks, terminal loopbacks, hairpins, and where appropriate cross-connect loopbacks (on optical paths carrying electrical circuits), the path of the circuit is traced and the possible points of failure are tested and eliminated. A logical progression of five network test procedures applies to this sample scenario:

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

West to east direction (left to right):

1. A facility (line) loopback on the source-node electrical card (DS-3 or E-1)
2. A hairpin on the source-node electrical port

3. An XC loopback on the destination-node STM-N virtual concatenation (VC, carrying the electrical circuit)
4. A terminal (inward) loopback on the destination-node electrical port

East to west direction (right to left):

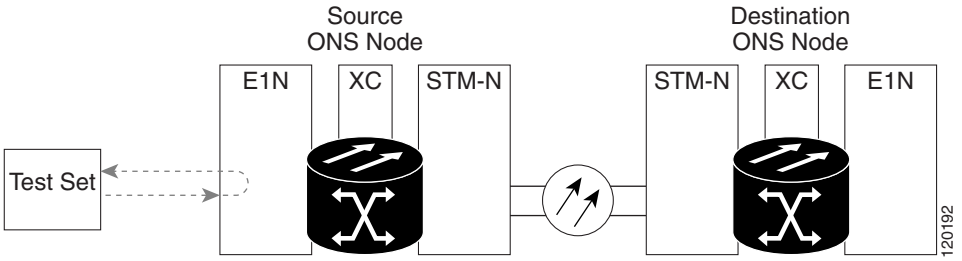
1. A facility (line) loopback on the destination-node electrical port
2. A hairpin on the destination-node electrical port
3. An XC loopback on the source-node STM-N VC (carrying the electrical circuit)
4. A terminal (inward) loopback on the source-node electrical port

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

1.2.1 Perform a Facility (Line) Loopback on a Source Electrical Port (West to East)

The facility (line) loopback test is performed on the node source port in the network circuit; in this example, the E1-N-14 port is the source. Completing a successful facility (line) loopback on this port isolates the cabling, the electrical card, and the FMEC card as possible failure points. Figure 1-11 shows an example of a facility loopback on a source E1-N-14 port.

Figure 1-11 Facility Loopback on a Circuit Source E1-N-14 Port



Caution Performing a loopback on an Unlocked circuit is service-affecting. To protect traffic, apply a lockout or Force switch to the target loopback port. For detailed information, refer to the "Maintain the Node" chapter in the *Cisco ONS 15454 SDH Procedure Guide*.

Note Electrical facility (line) loopbacks do not transmit an AIS condition in the direction away from the loopback. Instead of an AIS, a continuance of the signal transmitted to the loopback is provided.

Complete the "Create the Facility (Line) Loopback on the Source Electrical Port" procedure on page 1-11, then test and clear the loopback as instructed.

Create the Facility (Line) Loopback on the Source Electrical Port

Step 1 Connect an electrical test set to the port you are testing. (For instructions to use the test set, consult the manufacturer.)

Step 2 Use appropriate cabling to attach the transmit and receive terminals of the electrical test set to the FMEC connectors or electrical connection panel for the port you are testing. The transmit and receive terminals connect to the same port.

Step 3 Adjust the test set accordingly.

Step 4 In node view, double-click the card to display the card view.

Step 5 Click the **Maintenance > Loopback** tab.

Step 6 Choose **Unlocked,maintenance** from the Admin State column for the port being tested.

Step 7 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 port being tested.

Step 8 Click **Apply**.

Step 9 Click **Yes** in the confirmation dialog box.

Note It is normal for the "LPBKFACILITY (DS1, DS3)" condition on page 2-152 to appear during loopback setup. The condition clears when you remove the loopback.

Step 10 Complete the "Test and Clear the Electrical Port Facility Loopback Circuit" procedure on page 1-11.

Test and Clear the Electrical Port Facility Loopback Circuit

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

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

Step 3 If the test set indicates a good circuit, no further testing is necessary with the facility loopback. Double-click the card to display the card view.

Step 4 Depending upon the card type, click the **Maintenance > Loopback** tab.

Step 5 Choose **None** from the Loopback Type column for the port being tested.

Step 6 Choose the appropriate state (Unlocked; Locked,disabled; Unlocked,automaticInService) from the Admin State column for the port being tested.

Step 7 Click **Apply**.

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

Step 9 Complete the "Test the Electrical Cabling" procedure on page 1-12.

Test the Electrical Cabling

Step 1 Replace the suspected bad cabling (the cables from the test set to the electrical connection panel or the FMEC card ports) with a known-good cable.

If a known-good cable is not available, test the suspected bad cable with a test set. Remove the suspected bad cable from the electrical connection panel or the FMEC card and connect the cable to the transmit and receive terminals of the test set. Run traffic to determine whether the cable is good or defective.

Step 2 Replace the defective cable.

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

Note The DS-3 Admin State is the basis of the DS-1 Derived State.

Step 4 Choose **None** from the Loopback Type column for the port being tested.

Step 5 Choose the appropriate state (Unlocked; Locked,disabled; Unlocked,automaticInService) from the Admin State column for the port being tested.

Step 6 Click **Apply**.

Step 7 Click **Yes** in the confirmation dialog box.

Step 8 Complete the "Test the Electrical Card" procedure on page 1-12.

Test the Electrical Card

Step 1 Complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the suspected bad card and replace it with a known-good one.

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

Step 3 If the test set indicates a good circuit, the problem was probably the defective card. Return the defective card to Cisco through the RMA process. Log into the Cisco 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 Cisco Technical Assistance Center (TAC) numbers for your country.

Step 4 Complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the faulty card.

Step 5 In card view for the electrical card, double-click the **Maintenance > Loopback** tabs.

Note The DS-3 Admin State is the basis of the DS-1 Derived State.

Step 6 Choose **None** from the Loopback Type column for the port being tested.

Step 7 Choose the appropriate state (Unlocked; Locked,disabled; Unlocked,automaticInService) from the Admin State column for the port being tested.

Step 8 Click **Apply**.

Step 9 Click **Yes** in the confirmation dialog box.

Step 10 Complete the "Test the FMEC" procedure on page 1-13.

Test the FMEC

Step 1 Remove and reinstall the FMEC card to ensure a proper seating:

- **a.** Unscrew the screws on the FMEC cover and pull the cover forward.
- **b.** Loosen the faceplate screws that hold the FMEC card in place.
- **c.** Pull the FMEC card outward by the faceplate to unseat it from the shelf assembly.
- **d.** Push the FMEC card back inward by the faceplate to reseat it in the shelf assembly.

Step 2 Resend test traffic on the loopback circuit with known-good cabling, a known-good card, and the reinstalled FMEC.

Step 3 If the test set indicates a good circuit, the problem is probably an improperly seated FMEC. Click the **Maintenance > Loopback** tabs.

Step 4 Choose **None** from the Loopback Type column for the port being tested.

Step 5 Choose the appropriate state (Unlocked; Locked,disabled; Unlocked,automaticInService) from the Admin State column for the port being tested.

Step 6 Click **Apply**.

Step 7 Click **Yes** in the confirmation dialog box. Continue with Step 17.

Step 8 If the test set indicates a faulty circuit, the problem is probably a defective FMEC card. Return the defective FMEC card to Cisco through the RMA process. Log into the Cisco 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 Cisco TAC numbers for your country.

Step 9 Remove the faulty FMEC and replace it:

- **a.** Unscrew the screws on the FMEC cover and pull the cover forward.
- **b.** Loosen the faceplate screws that hold the FMEC card in place.
- **c.** Pull the FMEC card outward by the faceplate to unseat it from the shelf assembly.
- **d.** Push the FMEC card back inward by the faceplate to reseat it in the shelf assembly.

Step 10 Resend test traffic on the loopback circuit with known-good cabling, a known-good card, and the replacement FMEC card.

Step 11 If the test set indicates a faulty circuit, repeat all of the facility loopback procedures.

Step 12 If the test set indicates a good circuit, the problem is probably the defective FMEC card. Click the **Maintenance > Loopback** tabs.

Step 13 Choose **None** from the Loopback Type column for the port being tested.

Step 14 Choose the appropriate state (Unlocked; Locked,disabled; Unlocked,automaticInService) from the Admin State column for the port being tested.

Step 15 Click **Apply**.

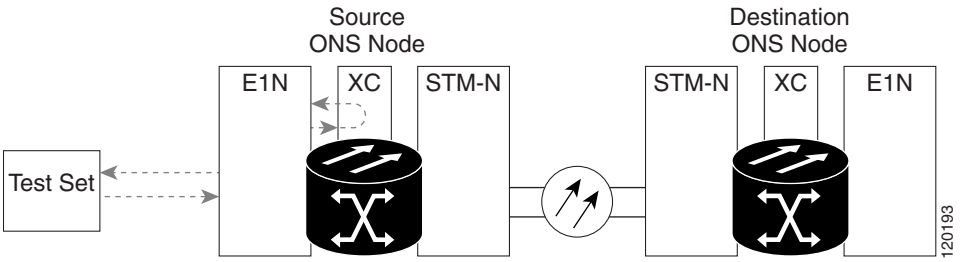
Step 16 Click **Yes** in the confirmation dialog box.

Step 17 Complete the "Perform a Hairpin Test on a Source-Node Electrical Port (West to East)" procedure on page 1-14.

1.2.2 Perform a Hairpin Test on a Source-Node Electrical Port (West to East)

The hairpin test is performed on the XC-VXL cross-connect card in the network circuit. A hairpin circuit uses the same port for both source and destination. Completing a successful hairpin through the card isolates the possibility that the cross-connect card is the cause of the faulty circuit. Figure 1-12 shows an example of a hairpin loopback on a source-node port.

Figure 1-12 Hairpin on a Source-Node Port



Note The ONS 15454 SDH does not support simplex operation on the XC-VXL cross-connect card. Two cross-connect cards of the same type must be installed for each node.

Complete the "Create the Hairpin Circuit on the Source-Node Electrical Port" procedure on page 1-14.

Create the Hairpin Circuit on the Source-Node Electrical Port

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

- **a.** If you just completed the "Perform a Facility (Line) Loopback on a Source Electrical Port (West to East)" procedure on page 1-10, leave the electrical test set hooked up to the source-node electrical port.
- **b.** If you are starting the current procedure without the electrical test set hooked up to the source port, use appropriate cabling to attach the transmit and receive terminals of the electrical test set to the electrical connection panel or the FMEC card connectors for the port you are testing. The transmit and receive terminals connect to the same port.

Step 2 Adjust the test set accordingly.

Step 3 Use CTC to set up the hairpin circuit on the test port:

- **a.** In node view, click the **Circuits** tab and click **Create**.
- **b.** In the Circuit Creation dialog box, choose the type and size, such as VC HO Path Circuit and number of circuits, such as 1.
- **c.** Click **Next**.
- **d.** In the next Circuit Creation dialog box, give the circuit an easily identifiable name such as Hairpin1.

e. Choose the **Size**, such as VC4.

f. Uncheck the **Bidirectional** check box. Leave the default value for State, SD Threshold, and SF Threshold.

g. Click **Next**.

h. In the Circuit Creation source dialog box, select the same **Node**, **Slot**, **Port**, **VC**, and **Tug** where the test set is connected. Leave Use Secondary Source unchecked.

i. Click **Next**.

j. In the Circuit Creation destination dialog box, use the same **Node**, **Slot**, **Port**, **VC**, and **Tug** used for the Circuit Source dialog box. Leave Use Secondary Destination unchecked.

k. In the Circuit Creation circuit routing preferences dialog box, leave all defaults.

l. If the VC Optimization dialog box is displayed, leave all defaults.

m. Click **Finish**.

Step 4 Confirm that the newly created circuit appears on the Circuits tab and that the Dir column describes it as a one-way circuit.

Step 5 Complete the "Test and Delete the Electrical Port Hairpin Circuit" procedure on page 1-15.

Test and Delete the Electrical Port Hairpin Circuit

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

Step 2 Examine the test traffic 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 a good circuit, no further testing is necessary with the hairpin circuit. Clear the hairpin circuit:

a. Click the **Circuits** tab.

b. Choose the hairpin circuit being tested.

c. Click **Delete**.

d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

e. Confirm that the hairpin circuit is deleted form the Circuits tab list.

Step 4 Complete the "Test the Standby XC-VXL Cross-Connect Card" procedure on page 1-15.

Test the Standby XC-VXL Cross-Connect Card

Note Two XC-VXL cross-connect cards (active and standby) must be in use on a node to use this procedure.

Step 1 Perform a reset on the standby cross-connect card to make it the active card:

a. Determine the standby cross-connect card. On both the physical node and the CTC node view window, the standby cross connect ACT/STBY LED is amber and the active card ACT/STBY LED is green.

b. Position the cursor over the standby cross-connect card.

c. Right-click and choose **RESET CARD**.

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

Step 2 Initiate an external switching command (side switch) on the cross-connect cards before you retest the loopback circuit:

Caution Cross-connect side switches are service-affecting. Any live traffic on any card in the node endures a hit of up to 50 ms.

a. Determine the standby cross-connect card. On both the physical node and the CTC node view window, the standby cross-connect ACT/STBY LED is amber and the active card ACT/STBY LED is green.

b. In the node view, select the **Maintenance > Cross Connect > Cards** tabs.

c. In the Cross Connect Cards menu, click **Switch**.

d. Click **Yes** in the Confirm Switch dialog box.

Note After the active cross-connect goes into standby mode, the original standby card becomes active and its ACT/STBY LED turns green. The former active card becomes standby and its ACT/STBY LED turns amber.

Step 3 Resend test traffic on the loopback circuit.

The test traffic now travels through the alternate cross-connect card.

Step 4 If the test set indicates a faulty circuit, assume the cross-connect card is not causing the problem. Clear the hairpin circuit:

a. Click the **Circuits** tab.

b. Choose the hairpin circuit being tested.

c. Click **Delete**.

d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes. Do not check any check boxes.

e. Confirm that the hairpin circuit is deleted form the Circuits tab list.

Step 5 To confirm a defective original cross-connect card, complete the "Retest the Original XC-VXL Cross-Connect Card" procedure on page 1-16.

Retest the Original XC-VXL Cross-Connect Card

Step 1 Initiate an external switching command (side switch) on the cross-connect cards:

a. Determine the standby cross-connect card. On both the physical node and the CTC node view window, the standby cross-connect ACT/STBY LED is amber and the active cross-connect ACT/STBY LED is green.

b. In node view, select the **Maintenance > Cross Connect > Cards** tabs.

c. From the Cross Connect Cards menu, choose **Switch**.

d. Click **Yes** in the Confirm Switch dialog box.

Note After the active cross-connect goes into standby mode, the original standby card becomes active and its ACT/STBY LED turns green. The former active card becomes standby and its ACT/STBY LED turns amber.

Step 2 Resend test traffic on the loopback circuit.

Step 3 If the test set indicates a faulty circuit, the problem is probably the defective card. Return the defective card to Cisco through the RMA process. Log into the Cisco 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 Cisco TAC numbers for your country.

Step 4 Complete the "Physically Replace an In-Service Cross-Connect Card" procedure on page 2-242 for the defective card.

Step 5 Clear the hairpin circuit:

a. Click the **Circuits** tab.

b. Choose the hairpin circuit being tested.

c. Click **Delete**.

d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

e. Confirm that the hairpin circuit is deleted form the Circuits tab list.

Step 6 Complete the "Perform an XC Loopback on a Destination-Node STM-N VC (West to East) Carrying an Electrical Signal" procedure on page 1-17.

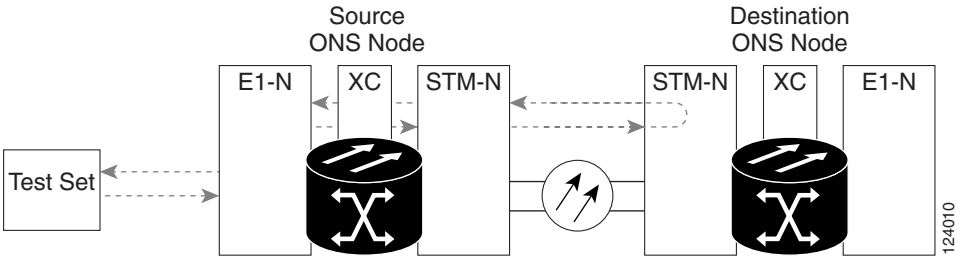
1.2.3 Perform an XC Loopback on a Destination-Node STM-N VC (West to East) Carrying an Electrical Signal

The XC loopback tests whether any problem exists on the circuit's optical span, isolating this span from others present on the card. The loopback occurs on the XC-VXL cross-connect card in a network circuit. Figure 1-13 shows an example of an XC loopback on a destination optical port. The traffic pattern looks similar to a terminal loopback but traffic is only carried on one synchronous transport signal (STS) instead of affecting the entire port.

Note The XC loopback on an optical card does not affect traffic on other circuits.

Note You can perform an XC loopback on either the circuit source working or the protect port of a 1+1 protection group.

Figure 1-13 XC Loopback on a Destination STM-N Port



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

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

a. If you just completed the "Perform a Hairpin Test on a Source-Node Electrical Port (West to East)" procedure on page 1-14, leave the optical test set hooked up to the destination-node port.

b. If you are starting the current procedure without the optical test set hooked up to the destination port, use appropriate cabling to attach the transmit and receive terminals of the optical test set to the port you are testing. The transmit and receive terminals connect to the same port.

Step 2 Adjust the test set accordingly.

Step 3 Use CTC to put the circuit being tested out of service:

a. In node view, click the **Circuits** tab.

b. Click the circuit and then click **Edit**.

c. In the Edit Circuit dialog box, click the **State** tab.

d. Choose Locked,maintenance from the Target Circuit State drop-down list.

e. Click **Apply**.

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

Step 4 Use CTC to set up the XC loopback on the circuit being tested:

a. In node view, double-click the optical card to display the card view.

b. Click the **Maintenance > Loopback > VC4** tabs.

c. Check the check box in the XC Loopback column for the port being tested.

d. Click **Apply**.

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

Step 5 Complete the "Test and Clear the XC Loopback Circuit" procedure on page 1-18.

Test and Clear the XC Loopback Circuit

Note This procedure is performed only on STM-N cards.

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

Step 2 Examine the test 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 a good circuit, no further testing is necessary with the cross-connect. Clear the XC loopback:

a. In card view, click the **Maintenance > Loopback > VC4** tabs.

b. Uncheck the check box in the **XC Loopback** column for the circuit being tested.

c. Click **Apply**.

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

Step 4 Complete the "Test the Standby XC-VXC-10G Cross-Connect Card" procedure on page 1-19.

Test the Standby XC-VXC-10G Cross-Connect Card

Step 1 Perform a reset on the standby cross-connect card:

a. Determine the standby cross-connect card. On both the physical node and the CTC node view window, the standby cross-connect ACT/STBY LED is amber and the active card ACT/STBY LED is green.

b. Position the cursor over the standby cross-connect card.

c. Right-click and choose **RESET CARD**.

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

Step 2 Initiate an external switching command (side switch) on the cross-connect cards before you retest the loopback circuit:

Caution Cross-connect side switches are service-affecting. Any live traffic on any card in the node endures a hit of up to 50 ms.

a. Determine the standby cross-connect card. On both the physical node and the CTC node view window, the standby cross-connect ACT/STBY LED is amber and the active card ACT/STBY LED is green.

b. In the node view, select the **Maintenance > Cross-Connect > Card** tabs.

c. In the Cross-Connect Cards area, click **Switch**.

d. Click **Yes** in the Confirm Switch dialog box.

Note After the active cross-connect goes into standby mode, the original standby card becomes active and its ACT/STBY LED turns green. The former active card becomes standby and its ACT/STBY LED turns amber.

Step 3 Resend test traffic on the loopback circuit.

The test traffic now travels through the alternate cross-connect card.

Step 4 If the test set indicates a faulty circuit, assume the cross-connect card is not causing the problem. Clear the XC loopback circuit:

a. Click the **Circuits** tab.

b. Choose the XC loopback circuit being tested.

c. Click **Delete**.

d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

e. Confirm that the XC loopback circuit is deleted form the Circuits tab list. If the test set indicates a good circuit, the problem might be a defective cross-connect card.

Step 5 To confirm a defective original cross-connect card, complete the "Retest the Original XC-VXC-10G Cross-Connect Card" procedure on page 1-20.

Retest the Original XC-VXC-10G Cross-Connect Card

Note This procedure is performed only on STM-N and XC-VXL cards.

Step 1 Initiate an external switching command (side switch) on the cross-connect cards:

a. Determine the standby cross-connect card. On both the physical node and the CTC node view window, the standby cross-connect ACT/STBY LED is amber and the active card ACT/STBY LED is green.

b. In node view, select the **Maintenance > Cross-Connect > Card** tabs.

c. In the Cross-Connect Cards area, click **Switch**.

d. Click **Yes** in the Confirm Switch dialog box.

Note After the active cross-connect goes into standby mode, the original standby card becomes active and its ACT/STBY LED turns green. The former active card becomes standby and its ACT/STBY LED turns amber.

Step 2 Resend test traffic on the loopback circuit.

Step 3 If the test set indicates a faulty circuit, the problem is probably the defective card. Return the defective card to Cisco through the RMA process. Log into the Cisco 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 Cisco TAC numbers for your country.

Step 4 Proceed to Step 5. If the circuit is not shown to be faulty and the card is not shown to be defective, you are finished with testing.

Step 5 Complete the "Physically Replace an In-Service Cross-Connect Card" procedure on page 2-242 for the defective cross-connect card and perform Step 6.

Step 6 If the test set indicates a good circuit, the cross-connect card might have had a temporary problem that was cleared by the side switch. Clear the XC loopback circuit:

a. Click the **Circuits** tab.

b. Choose the XC loopback circuit being tested.

c. Click **Delete**.

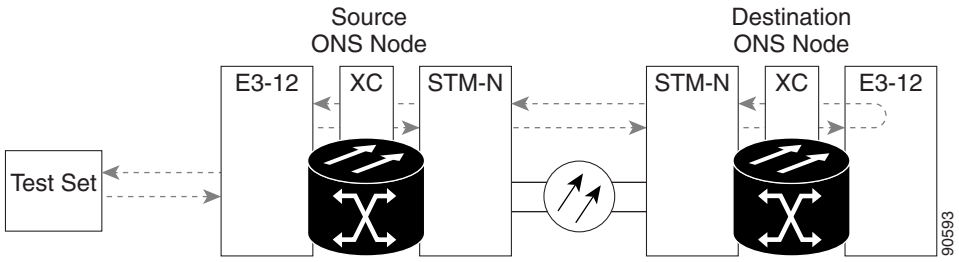
d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

Step 7 If the tests indicate further problems, go to the "Perform a Terminal (Inward) Loopback on a Destination Electrical Port (West to East)" procedure on page 1-21.

1.2.4 Perform a Terminal (Inward) Loopback on a Destination Electrical Port (West to East)

The terminal (inward) loopback test is performed on the node destination port in the circuit, such as a destination-node electrical port. You first create a bidirectional circuit that starts on the source-node port and loops back on the destination-node electrical port. Then you proceed with the terminal loopback test. Completing a successful terminal loopback to a destination-node electrical port verifies that the circuit is good up to the destination port. Figure 1-14 shows an example of a terminal loopback on a destination E3-12 port.

Figure 1-14 Terminal (Inward) Loopback on a Destination E3-12 Port



Caution Performing a loopback on an Unlocked circuit is service-affecting. To protect traffic, apply a lockout or Force switch to the target loopback port. For detailed information, refer to the "Maintain the Node" chapter in the *Cisco ONS 15454 SDH Procedure Guide*.

Note Electrical circuit terminal loopbacks do not transmit an AIS condition in the direction away from the loopback. Instead of an AIS, a continuance of the signal transmitted to the loopback is provided.

Complete the "Create the Terminal (Inward) Loopback on a Destination Electrical Port" procedure on page 1-21, then test and clear the loopback as instructed.

Create the Terminal (Inward) Loopback on a Destination Electrical Port

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

a. If you just completed the "Perform an XC Loopback on a Destination-Node STM-N VC (West to East) Carrying an Electrical Signal" procedure on page 1-17, leave the electrical test set hooked up to the source-node port.

b. If you are starting the current procedure without the electrical test set hooked up to the source port, use appropriate cabling to attach the transmit and receive terminals of the electrical test set to the electrical connection panel or the FMEC card connectors for the port you are testing. Both transmit and receive connect to the same port.

Step 2 Adjust the test set accordingly.

Step 3 In CTC node view, click the **Circuits** tab and click **Create**.

Step 4 In the Circuit Creation dialog box, choose the type and size, such as such as VC HO Path Circuit, and number, such as 1.

Step 5 Click **Next**.

Step 6 In the next Circuit Creation dialog box, give the circuit an easily identifiable name, such as ENtoEN.

Step 7 Leave the **Bidirectional** check box checked. Leave the default value for State.

Step 8 Click **Next**.

Step 9 In the Circuit Creation source dialog box, select the **Node**, **Slot**, **Port**, and **VC4** where the test set is connected.

Step 10 Click **Next**.

Step 11 In the Circuit Creation destination dialog box, fill in the same **Node**, **Slot**, **Port**, and **VC4** (the destination-node port) and click **Finish**.

Step 12 Confirm that the newly created circuit appears in the Circuits tab Dir column as a two-way circuit.

Note It is normal for a "LPBKTERMINAL (DS1, DS3)" condition, page 2-156 to appear during a loopback setup. The condition clears when you remove the loopback.

Note Electrical circuit terminal loopbacks do not transmit an AIS (see the "AIS" condition on page 2-31) in the direction away from the loopback. Instead of an AIS, a continuance of the signal transmitted to the loopback is provided.

Step 13 Create the terminal (inward) loopback on the destination port being tested:

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

b. In node view, double-click the card that requires the loopback, such as an E-1 card in the destination node.

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

d. Select **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 14 Complete the "Test and Clear the Destination Electrical Port Terminal Loopback Circuit" procedure on page 1-23.

Test and Clear the Destination Electrical Port Terminal Loopback Circuit

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

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

Step 3 If the test set indicates a good circuit, no further testing is necessary on the loopback circuit. Double-click the electrical card in the destination node with the terminal loopback.

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

Step 5 Select **None** from the Loopback Type column for the port being tested.

Step 6 Select the appropriate state (Unlocked; Locked,disabled; Unlocked,automaticInService) in the Admin State column for the port being tested.

Step 7 Click **Apply**.

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

Step 9 Clear the terminal loopback circuit:

- **a.** Click the **Circuits** tab.
- **b.** Choose the loopback circuit being tested.
- **c.** Click **Delete**.
- **d.** Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

Step 10 Complete the "Test the Destination Electrical Card" procedure on page 1-23.

Test the Destination Electrical Card

Step 1 Replace the suspected bad card with a known-good card. Complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the suspected bad card and replace it with a known-good one.

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

Step 3 If the test set indicates a good circuit, the problem is probably the defective card.

- **a.** Return the defective card to Cisco through the RMA process. Log into the Cisco 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 Cisco TAC numbers for your country.
- **b.** Complete "Physically Replace a Traffic Card" procedure on page 2-242 for the faulty card.

Step 4 Clear the terminal (inward) loopback state on the port:

- **a.** Double-click the destination-node electrical card.
- **b.** Click the **Maintenance > Loopback** tabs.
- **c.** Select **None** from the Loopback Type column for the port being tested.

d. Select the appropriate state (Unlocked; Locked,disabled; Unlocked,automaticInService) in the Admin State column for the port being tested.

e. Click **Apply**.

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

Step 5 Clear the terminal (inward) loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

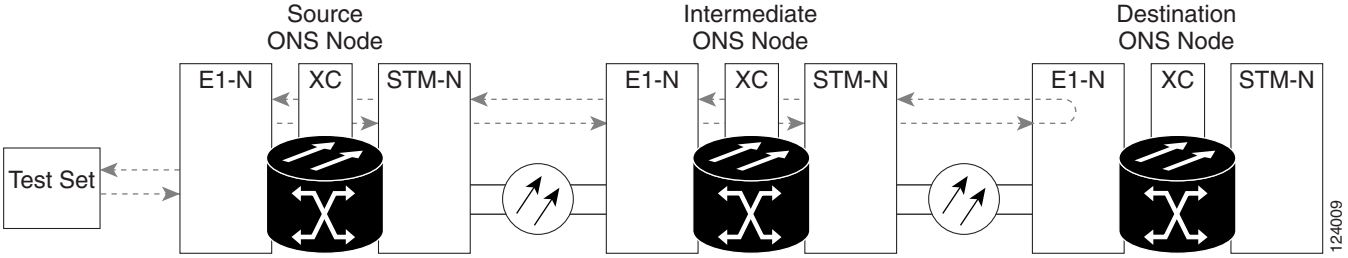
d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

Step 6 Complete the "Perform a Facility (Line) Loopback on a Destination-Node Electrical Port (East to West)" procedure on page 1-24.

1.2.5 Perform a Facility (Line) Loopback on a Destination-Node Electrical Port (East to West)

The facility loopback test is performed on the destination-node electrical port in the network circuit. Completing a successful facility loopback on this port isolates the possibility that the destination-node cabling, electrical card, LIU, or FMEC card is responsible for a faulty circuit. Figure 1-15 shows an example of a facility loopback on a destination E1-N-14 port.

Figure 1-15 Facility Loopback on a Destination E1-N-14 Port



Note Electrical circuit facility (line) loopbacks do not transmit an AIS condition in the direction away from the loopback. Instead of an AIS, a continuance of the signal transmitted to the loopback is provided.

Caution Performing a loopback on an Unlocked circuit is service-affecting. To protect traffic, apply a lockout or Force switch to the target loopback port. For basic instructions, see the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-230. For detailed information, refer to the "Maintain the Node" chapter in the *Cisco ONS 15454 SDH Procedure Guide*.

Complete the "Create a Facility (Line) Loopback Circuit on a Destination Electrical Port" procedure on page 1-25. Then test and clear the loopback as instructed.

Create a Facility (Line) Loopback Circuit on a Destination Electrical Port

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

a. If you just completed the "Perform a Terminal (Inward) Loopback on a Destination Electrical Port (West to East)" procedure on page 1-21, leave the electrical test set hooked up to the destination-node port.

b. If you are starting the current procedure without the electrical test set hooked up to the destination port, use appropriate cabling to attach the transmit and receive terminals of the electrical test set to the electrical connection panel or the FMEC connectors for the port you are testing. Both transmit and receive connect to the same port.

Step 2 Adjust the test set accordingly.

Step 3 In node view, double-click the destination electrical card to display the card view.

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

Step 5 Choose **Locked,maintenance** from the Admin State column.

Step 6 Select **Facility (Line)** from the Loopback Type column for the port being tested. 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.

Note It is normal for a "LPBKFACILITY (DS1, DS3)" condition, page 2-152 or "LPBKFACILITY (E1, E3, E4)" condition, page 2-153 to appear during loopback setup. The condition clears when you remove the loopback.

Step 9 Complete the "Test and Clear the Facility (Line) Loopback Electrical Circuit" procedure on page 1-25.

Test and Clear the Facility (Line) Loopback Electrical Circuit

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

Step 2 Examine the test traffic 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 a good circuit, no further testing is necessary with the loopback circuit. Double-click the card to display the card view.

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

Step 5 Choose **None** from the Loopback Type column for the port being tested.

Step 6 Choose the appropriate state (Unlocked; Locked,disabled; Unlocked,automaticInService) from the Admin State column for the port being tested.

Step 7 Click **Apply**.

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

Step 9 If the test set indicates a faulty circuit, the problem might be a faulty electrical card, faulty cabling from the electrical card to the connection panel or the FMECs. Complete the "Test the Electrical Cabling" procedure on page 1-26.

Test the Electrical Cabling

Step 1 Replace the suspect cabling (the cables from the test set to the electrical connection panel or the FMEC card ports) with a known-good cable.

If a known-good cable is not available, test the suspected bad cable with a test set. Remove the suspected bad cable from the electrical connection panel or the FMEC card and connect the cable to the transmit and receive terminals of the test set. Run traffic to determine whether the cable is good or defective.

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

Step 3 If the test set indicates a good circuit, the problem was probably the defective cable. Replace the defective cable.

Step 4 Double-click the card to display the card view.

Step 5 Click the **Maintenance > Loopback** tabs.

Step 6 Choose **None** from the Loopback Type column for the port being tested.

Step 7 Choose the appropriate state (Unlocked; Locked,disabled; Unlocked,automaticInService) from the Admin State column for the port being tested.

Step 8 Click **Apply**.

Step 9 Click **Yes** in the confirmation dialog box.

Step 10 Complete the "Test the Electrical Card" procedure on page 1-26.

Test the Electrical Card

Step 1 Complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the suspected bad card and replace it with a known-good one.

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

Step 3 If the test set indicates a good circuit, the problem is probably the defective card. Return the defective card to Cisco through the RMA process. Log into the Cisco 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 Cisco TAC numbers for your country.

Step 4 Replace the faulty card. Complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the faulty card.

Step 5 Double-click the card to display the card view.

Step 6 Click the **Maintenance > Loopback** tabs.

Step 7 Choose **None** from the Loopback Type column for the port being tested.

Step 8 Choose the appropriate state (Unlocked; Locked,disabled; Unlocked,automaticInService) from the Admin State column for the port being tested.

Step 9 Click **Apply**.

Step 10 Click **Yes** in the confirmation dialog box.

Step 11 Complete the "Test the FMEC" procedure on page 1-27.

Test the FMEC

Step 1 Remove and reinstall the FMEC card to ensure a proper seating:

- **a.** Unscrew the screws on the FMEC cover and pull the cover forward.
- **b.** Loosen the faceplate screws that hold the FMEC card in place.
- **c.** Pull the FMEC card outward by the faceplate to unseat it from the shelf assembly.
- **d.** Push the FMEC card back inward by the faceplate to reseat it in the shelf assembly.

Step 2 Resend test traffic on the loopback circuit with known-good cabling, a known-good card, and the reinstalled FMEC card. If the test set indicates a good circuit, the problem is probably an improperly seated FMEC card.

Step 3 Clear the facility (line) 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 (Unlocked; Locked,disabled; Unlocked,automaticInService) from the Admin State column for the port being tested.
- **d.** Click **Apply**.
- **e.** Click **Yes** in the confirmation dialog box.

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

Step 4 If the test set indicates a faulty circuit, the problem is probably the defective FMEC card. Return the defective FMEC card to Cisco through the RMA process. Log into the Cisco 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 Cisco TAC numbers for your country.

Step 5 Complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the faulty FMEC card.

Step 6 Resend test traffic on the loopback circuit with known-good cabling, a known-good card, and the replacement FMEC card.

Step 7 If the test set indicates a faulty circuit, repeat all of the facility loopback procedures. If the faulty circuit persists, contact the Cisco Technical Support. Log into the Cisco 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 Cisco TAC numbers for your country.

Step 8 If the test set indicates a good circuit, the problem is probably a defective FMEC card. Clear the facility (line) 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 (Unlocked; Locked,disabled; Unlocked,automaticInService) from the Admin State column for the port being tested.

d. Click **Apply**.

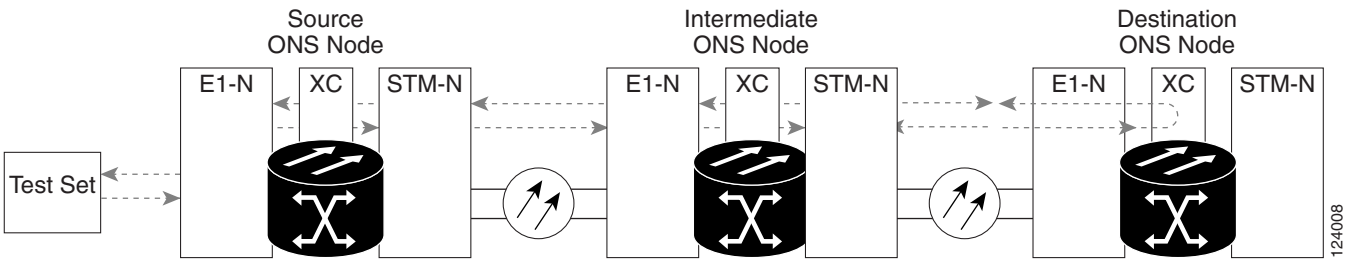
e. Click **Yes** in the confirmation dialog box.

Step 9 Complete the "Perform a Hairpin Test on a Destination-Node Electrical Port (East to West)" procedure on page 1-28.

1.2.6 Perform a Hairpin Test on a Destination-Node Electrical Port (East to West)

The hairpin test is performed on the cross-connect card in the network circuit. A hairpin circuit uses the same port for both source and destination. Completing a successful hairpin through the card isolates the possibility that the cross-connect card is the cause of the faulty circuit. Figure 1-16 shows an example of a hairpin loopback on a destination-node port.

Figure 1-16 Hairpin on a Destination-Node Port



Note The ONS 15454 SDH does not support simplex operation on the XC-VXL cross-connect card. Two cross-connect cards of the same type must be installed for each node.

Complete the "Create the Hairpin Circuit on the Destination-Node Port" procedure on page 1-28.

Create the Hairpin Circuit on the Destination-Node Port

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

a. If you just completed the "Perform a Facility (Line) Loopback on a Destination-Node Electrical Port (East to West)" procedure on page 1-24, leave the electrical test set hooked up to the electrical port in the destination node.

b. If you are starting the current procedure without the electrical test set hooked up to the electrical port, use appropriate cabling to attach the transmit and receive terminals of the electrical test set to the electrical connection panel or the FMEC connectors for the port you are testing. The transmit and receive terminals connect to the same port.

Step 2 Adjust the test set accordingly.

Step 3 Use CTC to set up the hairpin circuit on the test port:

a. In node view, click the **Circuits** tab and click **Create**.

b. In the Circuit Creation dialog box, choose the type and size, such as VC HO Path Circuit, and number, such as 1.

c. Click **Next**.

d. In the next Circuit Creation dialog box, give the circuit an easily identifiable name such as Hairpin1.

e. Uncheck the **Bidirectional** check box. Leave the default value for State, SD Threshold, and SF Threshold.

f. Click **Next**.

g. In the Circuit Creation source dialog box, select the same **Node**, **Slot**, **Port**, **VC,** and **Tug** where the test set is connected. Leave Use Secondary Source unchecked.

h. Click **Next**.

i. In the Circuit Creation destination dialog box, use the same **Node**, **Slot**, **Port**, **VC,** and **Tug** used for the source dialog box. Leave Use Secondary Destination unchecked.

j. Click **Next**.

k. In the Circuit Creation circuit routing preferences dialog box, leave all defaults.

l. If the VC Optimization dialog box appears, leave all defaults.

m. Click **Finish**.

Step 4 Confirm that the newly created circuit appears on the Circuits tab and that the Dir column describes it as a one-way circuit.

Step 5 Complete the "Test and Delete the Electrical Hairpin Circuit" procedure on page 1-29.

Test and Delete the Electrical Hairpin Circuit

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

Step 2 Examine the test traffic 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 a good circuit, no further testing is necessary with the hairpin circuit. Clear the hairpin circuit:

a. Click the **Circuits** tab.

b. Choose the hairpin circuit being tested.

c. Click **Delete**.

d. Click **Yes** in the Delete Circuits box.

e. Confirm that the hairpin circuit is deleted form the Circuits tab list.

Step 4 Complete the "Test the Standby XC-VXL Cross-Connect Card" procedure on page 1-30.

Test the Standby XC-VXL Cross-Connect Card

Note Two XC-VXL cross-connect cards (active and standby) must be in use on a node to use this procedure.

Step 1 Perform a reset on the standby XC-VXL cross-connect card to make it the active card:

a. Determine the standby cross-connect card. On both the physical node and the CTC node view window, the standby cross-connect ACT/STBY LED is amber and the active card ACT/STBY LED is green.

b. Position the cursor over the standby cross-connect card.

c. Right-click and choose **RESET CARD**.

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

Step 2 Initiate an external switching command (side switch) on the cross-connect cards before you retest the loopback circuit:

Caution Cross-connect side switches are service-affecting. Any live traffic on any card in the node endures a hit of up to 50 ms.

a. Determine the standby XC-VXL cross-connect card. On both the physical node and the CTC node view window, the standby cross-connect ACT/STBY LED is amber and the active card ACT/STBY LED is green.

b. In the node view, select the **Maintenance > Cross-Connect > Card** tabs.

c. In the Cross-Connect Cards area, click **Switch**.

d. Click **Yes** in the Confirm Switch dialog box.

Note After the active XC-VXL cross-connect goes into standby mode, the original standby card becomes active and its ACT/STBY LED turns green. The former active card becomes standby and its ACT/STBY LED turns amber.

Step 3 Resend test traffic on the loopback circuit.

The test traffic now travels through the alternate cross-connect card.

Step 4 If the test set indicates a faulty circuit, assume the cross-connect card is not causing the problem. Clear the hairpin circuit:

a. Click the **Circuits** tab.

b. Choose the hairpin circuit being tested.

c. Click **Delete**.

d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

e. Confirm that the hairpin circuit is deleted form the Circuits tab list.

Step 5 To confirm a defective original cross-connect card, complete the "Retest the Original XC-VXL Cross-Connect Card" procedure on page 1-31.

Retest the Original XC-VXL Cross-Connect Card

Step 1 Initiate an external switching command (side switch) on the XC-VXL cross-connect cards:

a. Determine the standby cross-connect card. On both the physical node and the CTC node view window, the standby cross-connect ACT/STBY LED is amber and the active card ACT/STBY LED is green.

b. In node view, select the **Maintenance > Cross-Connect > Card** tabs.

c. From the Cross-Connect Cards menu, choose **Switch**.

d. Click **Yes** in the Confirm Switch dialog box.

Note After the active cross-connect goes into standby mode, the original standby card becomes active and its ACT/STBY LED turns green. The former active card becomes standby and its ACT/STBY LED turns amber.

Step 2 Resend test traffic on the loopback circuit.

Step 3 If the test set indicates a faulty circuit, the problem is probably the defective card. Return the defective card to Cisco through the RMA process. Log into the Cisco 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 Cisco TAC numbers for your country.

Step 4 Proceed to Step 5. If the test does not indicate a faulty circuit, proceed to Step 6.

Step 5 Complete the "Physically Replace an In-Service Cross-Connect Card" procedure on page 2-242 for the defective cross-connect card.

Step 6 If the test set indicates a good circuit, the cross-connect card might have had a temporary problem that was cleared by the side switch. Clear the hairpin circuit:

a. Click the **Circuits** tab.

b. Choose the hairpin circuit being tested.

c. Click **Delete**.

d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

e. Confirm that the hairpin circuit is deleted form the Circuits tab list.

Step 7 Complete the "Perform an XC Loopback on a Source-Node STM-N VC (East to West) Carrying an Electrical Circuit" procedure on page 1-31.

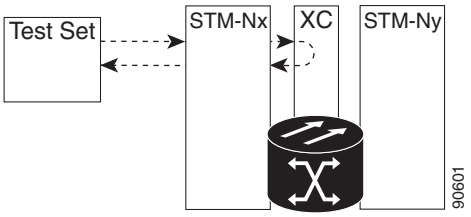
1.2.7 Perform an XC Loopback on a Source-Node STM-N VC (East to West) Carrying an Electrical Circuit

The XC loopback tests whether any problem exists on the circuit's optical span, isolating this span from others present on the card. It also eliminates the cross-connect card as the source of trouble for a faulty circuit. The loopback occurs on the XC-VXL cross-connect card in a network circuit. Figure 1-17 shows an example of an XC loopback on a source STM-N port.

Note The XC loopback on an STM-N card does not affect traffic on other circuits.

Note You can perform an XC loopback on either the circuit source working or the protect port of a 1+1 protection group.

Figure 1-17 XC Loopback on a Source STM-N Port



Complete the "Create the XC Loopback on the Source Optical Port Carrying an Electrical Circuit" procedure on page 1-32.

Create the XC Loopback on the Source Optical Port Carrying an Electrical Circuit

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 Hairpin Test on a Destination-Node Electrical Port (East to West)" procedure on page 1-28, 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 transmit and receive terminals of the optical test set to the port you are testing. The transmit and receive terminals connect to the same port.

Step 2 Adjust the test set accordingly.

Step 3 Use CTC to put the circuit being tested out of service:

a. In node view, click the **Circuits** tab.

b. Click the circuit and then click **Edit**.

c. In the Edit Circuit dialog box, click the **State** tab.

d. Choose **Locked,maintenance** from the Target Circuit State drop-down list.

e. Click **Apply**.

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

Step 4 Use CTC to set up the XC loopback on the circuit being tested:

a. In node view, double-click the optical card to display the card view.

b. Click the **Maintenance > Loopback > VC4** tabs.

c. Click the **XC Loopback** column check box for the port being tested.

d. Click **Apply**.

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

Step 5 Complete the "Test and Clear the XC Loopback Circuit" procedure on page 1-33.

Test and Clear the XC Loopback Circuit

Note This procedure is performed only on STM-N cards.

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

Step 2 Examine the test 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 a good circuit, no further testing is necessary with the cross-connect. Clear the XC loopback:

a. In card view, click the **Maintenance > Loopback > VC4** tabs.

b. Uncheck the check box in the XC Loopback column for the circuit being tested.

c. Click **Apply**.

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

Step 4 Complete the "Test the Standby XC-VXL Cross-Connect Card" procedure on page 1-33.

Test the Standby XC-VXL Cross-Connect Card

Step 1 Perform a reset on the standby cross-connect card:

a. Determine the standby cross-connect card. On both the physical node and the CTC node view window, the standby cross-connect ACT/STBY LED is amber and the active card ACT/STBY LED is green.

b. Position the cursor over the standby cross-connect card.

c. Right-click and choose **RESET CARD**.

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

Step 2 Initiate an external switching command (side switch) on the cross-connect cards before you retest the loopback circuit:

Caution Cross-connect side switches are service-affecting. Any live traffic on any card in the node endures a hit of up to 50 ms.

a. Determine the standby cross-connect card. On both the physical node and the CTC node view window, the standby cross-connect ACT/STBY LED is amber and the active card ACT/STBY LED is green.

b. In the node view, select the **Maintenance > Cross-Connect > Card** tabs.

c. In the Cross-Connect Cards area, click **Switch**.

d. Click **Yes** in the Confirm Switch dialog box.

Note After the active cross-connect goes into standby mode, the original standby card becomes active and its ACT/STBY LED turns green. The former active card becomes standby and its ACT/STBY LED turns amber.

Step 3 Resend test traffic on the loopback circuit.

The test traffic now travels through the alternate cross-connect card.

Step 4 If the test set indicates a faulty circuit, assume the cross-connect card is not causing the problem. Clear the XC loopback circuit:

a. Click the **Circuits** tab.

b. Choose the XC loopback circuit being tested.

c. Click **Delete**.

d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

e. Confirm that the XC loopback circuit is deleted form the Circuits tab list. If the test set indicates a good circuit, the problem might be a defective cross-connect card.

Step 5 To confirm a defective original cross-connect card, complete the "Retest the Original XC-VXL Cross-Connect Card" procedure on page 1-34.

Retest the Original XC-VXL Cross-Connect Card

Note This procedure is performed only on STM-N and XC-VXL cards.

Step 1 Initiate an external switching command (side switch) on the cross-connect cards:

a. Determine the standby cross-connect card. On both the physical node and the CTC node view window, the standby cross-connect ACT/STBY LED is amber and the active card ACT/STBY LED is green.

b. In node view, select the **Maintenance > Cross-Connect > Card** tabs.

c. In the Cross-Connect Cards area, click **Switch**.

d. Click **Yes** in the Confirm Switch dialog box.

Note After the active cross-connect goes into standby mode, the original standby card becomes active and its ACT/STBY LED turns green. The former active card becomes standby and its ACT/STBY LED turns amber.

Step 2 Resend test traffic on the loopback circuit.

Step 3 If the test set indicates a faulty circuit, the problem is probably the defective card. Return the defective card to Cisco through the RMA process. Log into the Cisco 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 Cisco TAC numbers for your country.

Step 4 If the circuit is not shown to be faulty and the card is not shown to be defective, you are finished with testing.

Step 5 Complete the "Physically Replace an In-Service Cross-Connect Card" procedure on page 2-242 for the defective cross-connect card and perform Step 6.

Step 6 If the test set indicates a good circuit, the cross-connect card might have had a temporary problem that was cleared by the side switch. Clear the XC loopback circuit:

a. Click the **Circuits** tab.

b. Choose the XC loopback circuit being tested.

c. Click **Delete**.

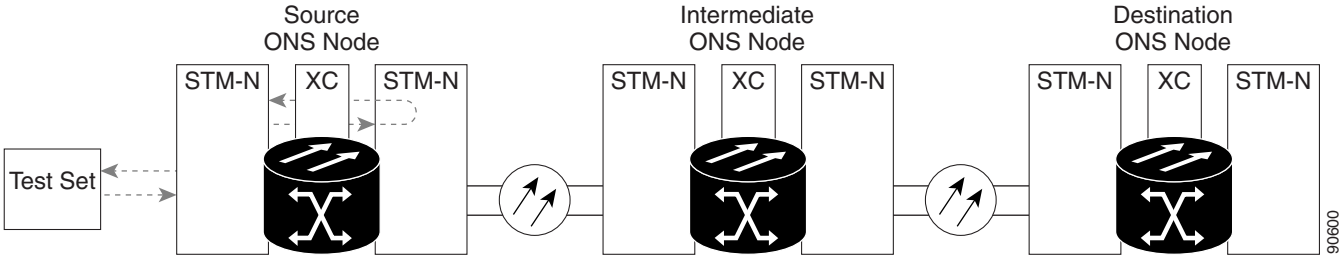
d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

Step 7 If the problem is not resolved, go to the "Perform a Terminal (Inward) Loopback on a Source-Node Electrical Port (East to West)" procedure on page 1-35.

1.2.8 Perform a Terminal (Inward) Loopback on a Source-Node Electrical Port (East to West)

The terminal (inward) loopback test is performed on the node source port in the circuit, such as a source-node electrical port. You first create a bidirectional circuit that starts on the destination-node electrical port and loops back on the source-node electrical port. Then you proceed with the terminal loopback test. Completing a successful terminal loopback to a source-node port verifies that the circuit is good to the source electrical port. Figure 1-14 shows an example of a terminal loopback on a source electrical port.

Figure 1-18 Terminal (Inward) Loopback on a Source Electrical Port



Caution Performing a loopback on an Unlocked circuit is service-affecting. To protect traffic, apply a lockout or Force switch to the target loopback port. See the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-230 for basic instructions. For detailed information, refer to the "Maintain the Node" chapter in the *Cisco ONS 15454 SDH Procedure Guide*.

Note Electrical circuit terminal loopbacks do not transmit an AIS condition in the direction away from the loopback. Instead of an AIS, a continuance of the signal transmitted to the loopback is provided.

Complete the "Create the Terminal (Inward) Loopback on a Source-Node Electrical Port" procedure on page 1-36.

Create the Terminal (Inward) Loopback on a Source-Node Electrical Port

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

a. If you just completed the "Perform an XC Loopback on a Source-Node STM-N VC (East to West) Carrying an Electrical Circuit" procedure on page 1-31, leave the electrical test set hooked up to the electrical port in the source node.

b. If you are starting the current procedure without the electrical test set hooked up to the electrical port, use appropriate cabling to attach the transmit and receive terminals of the electrical test set to the electrical panel or the FMEC connectors for the port you are testing. Both transmit and receive connect to the same port.

Step 2 Adjust the test set accordingly.

Step 3 In CTC node view, click the **Circuits** tab and click **Create**.

Step 4 In the Circuit Creation dialog box, choose the type and size, such as VC HO Path Circuit, and the number, such as 1.

Step 5 Click **Next**.

Step 6 In the next Circuit Creation dialog box, give the circuit an easily identifiable name such as ENtoEN.

Step 7 Leave the **Bidirectional** check box checked.

Step 8 Click **Next**.

Step 9 In the Circuit Creation source dialog box, select the **Node**, **Slot**, **Port**, and **VC4** where the test set is connected.

Step 10 Click **Next**.

Step 11 In the Circuit Creation destination dialog box, use the same **Node**, **Slot**, **Port**, **VC**, and **Tug** used for the source dialog box.

Step 12 Click **Next** and complete the following substeps:

a. In the Circuit Creation circuit routing preferences dialog box, leave all defaults.

b. In the VC Optimization dialog box, leave all defaults.

c. Click **Finish**.

Step 13 Confirm that the newly created circuit appears in the Dir column as a two-way circuit.

Note It is normal for a "LPBKTERMINAL (DS1, DS3)" condition on page 2-156 to appear during a loopback setup. The condition clears when you remove the loopback.

Note Electrical circuit terminal loopbacks do not transmit an AIS (see the "AIS" condition on page 2-31) in the direction away from the loopback. Instead of a, electrical line AIS, a continuance of the signal transmitted to the loopback is provided.

Step 14 Create the terminal (inward) loopback on the destination port being tested:

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

b. In node view, double-click the card that requires the loopback, such as the electrical card in the destination node.

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

d. Select **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 15 Complete the "Test and Clear the Electrical Port Terminal (Inward) Loopback Circuit" procedure on page 1-37.

Test and Clear the Electrical Port Terminal (Inward) Loopback Circuit

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

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

Step 3 If the test set indicates a good circuit, no further testing is necessary on the loopback circuit. Double-click the electrical card in the destination node with the terminal loopback.

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

Step 5 Select **None** from the Loopback Type column for the port being tested.

Step 6 Select the appropriate state (Unlocked; Locked,disabled; Unlocked,automaticInService) in the Admin State column for the port being tested.

Step 7 Click **Apply**.

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

Step 9 Clear the terminal loopback:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

Step 10 Complete the "Test the Source Electrical Card" procedure on page 1-38.

Test the Source Electrical Card

Step 1 Complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the suspected bad card and replace it with a known-good one.

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

Step 3 If the test set indicates a good circuit, the problem was probably the defective card. Return the defective card to Cisco through the RMA process. Log into the Cisco 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 Cisco TAC numbers for your country.

Step 4 Complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the defective electrical card.

Step 5 Clear the terminal (inward) loopback state on the port:

a. Double-click the electrical card in the destination 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. Select the appropriate state (Unlocked; Locked,disabled; Unlocked,automaticInService) in the Admin State column for the port being tested.

e. Click **Apply**.

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

Step 6 Delete the terminal (inward) loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete.**

d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

The circuit qualifies to carry traffic.

1.3 Troubleshooting Optical Circuit Paths With Loopbacks

Facility (line) loopbacks, terminal (inward) loopbacks, and cross-connect loopback circuits 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.

The procedures in this section apply to optical cards. (For instructions on G-Series Ethernet cards, go to the "1.4 Troubleshooting Ethernet Circuit Paths With Loopbacks" section on page 1-61. For information about troubleshooting MXP and TXP cards, go to the "1.5 Troubleshooting MXP, TXP, or FC_MR-4 Circuit Paths With Loopbacks" section on page 1-79.) The example in this section tests an

optical circuit on a three-node MS-SPRing. Using a series of facility, cross-connect, and terminal (inward) loopbacks, the example scenario traces the circuit path, tests the possible failure points, and eliminates them. The logical progression contains seven network test procedures:

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

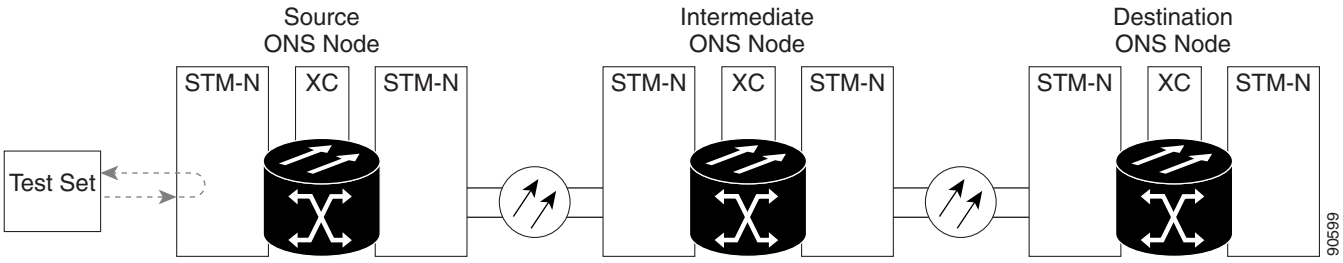
1. A facility (line) loopback on the source-node STM-N port
2. A terminal (inward) loopback on the source-node STM-N port
3. A cross-connect loopback on the source STM-N port
4. A facility (line) loopback on the intermediate-node STM-N port
5. A terminal (inward) loopback on the intermediate-node STM-N port
6. A facility (line) loopback on the destination-node STM-N port
7. A terminal (inward) loopback on the destination-node STM-N port

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

1.3.1 Perform a Facility (Line) Loopback on a Source-Node Optical Port

The facility (line) loopback test is performed on the node source port in the network circuit. In the testing situation used in this example, the source STM-N port in the source node. Completing a successful facility (line) loopback on this port isolates the optical port as a possible failure point. Figure 1-19 shows an example of a facility loopback on a circuit source STM-N port.

Figure 1-19 Facility Loopback on a Circuit Source STM-N Port



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

Complete the "Create the Facility (Line) Loopback on the Source Optical Port" procedure on page 1-39.

Create the Facility (Line) Loopback on the Source Optical Port

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

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

Use appropriate cabling to attach the transmit and receive terminals of the optical test set to the port you are testing. The transmit and receive terminals connect to the same port. Adjust the test set accordingly.

Step 2 In CTC node view, double-click the card to display the card view.

Step 3 Click the **Maintenance > Loopback > Port** tabs.

Step 4 Choose **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 5 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 6 Click **Apply**.

Step 7 Click **Yes** in the confirmation dialog box.

Note It is normal for a "LPBKFACILITY (STM1E, STMN)" condition, page 2-155 to appear during loopback setup. The condition clears when you remove the loopback.

Step 8 Complete the "Test and Clear the Facility (Line) Loopback Circuit" procedure on page 1-40.

Test and Clear the Facility (Line) Loopback Circuit

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

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

Step 3 If the test set indicates a good circuit, no further testing is necessary with the facility loopback. Clear the facility loopback:

- **a.** Click the **Maintenance > Loopback > Port** tabs.
- **b.** Choose **None** from the Loopback Type column for the port being tested.
- **c.** Choose the appropriate state (Unlocked; Locked,disabled; Unlocked,automaticInService) from the Admin State column for the port being tested.
- **d.** Click **Apply**.
- **e.** Click **Yes** in the confirmation dialog box.

Step 4 Complete the "Test the Optical Card" procedure on page 1-40.

Test the Optical Card

Step 1 Complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the suspected bad card and replace it with a known-good one.

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

Step 3 If the test set indicates a good circuit, the problem is probably the defective card. Return the defective card to Cisco through the RMA process. Log into the Cisco 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 Cisco TAC numbers for your country.

Step 4 Complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the faulty card.

Step 5 Clear the facility (line) loopback:

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

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

c. Choose the appropriate state (Unlocked; Locked,disabled; Unlocked,automaticInService) from the Admin State column for the port being tested.

d. Click **Apply**.

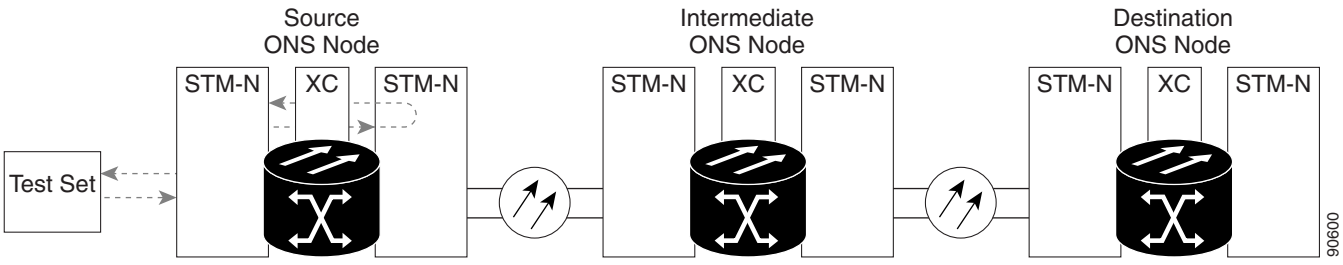
e. Click **Yes** in the confirmation dialog box.

Step 6 Complete the "Perform a Terminal (Inward) Loopback on a Source-Node Optical Port" procedure on page 1-41.

1.3.2 Perform a Terminal (Inward) Loopback on a Source-Node Optical Port

The terminal (inward) loopback test is performed on the source-node optical port. For the circuit in this example, the destination STM-N port in the source node. You first create a bidirectional circuit that starts on the node source optical port and loops back on the node destination optical port. You then proceed with the terminal loopback test. Completing a successful terminal loopback to a node destination port verifies that the circuit is good up to the destination port. Figure 1-20 shows an example of a terminal loopback on a source-node STM-N port.

Figure 1-20 Terminal Loopback on a Source-Node STM-N Port



STM-N cards placed in terminal loopback state display an icon in the CTC graphical user interface (GUI), shown in Figure 1-21.

Figure 1-21 Terminal Loopback Indicator

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

Complete the "Create the Terminal (Inward) Loopback on a Source-Node Optical Port" procedure on page 1-42.

Create the Terminal (Inward) Loopback on a Source-Node Optical Port

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

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

a. If you just completed the "Perform a Facility (Line) Loopback on a Source-Node Optical Port" procedure on page 1-39, 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-node port, use appropriate cabling to attach the transmit and receive terminals of the optical test set to the port you are testing. Both transmit and receive connect to the same port.

Step 2 Adjust the test set accordingly.

Step 3 Use CTC to set up the terminal (inward) loopback circuit on the port being tested:

a. In node view, click the **Circuits** tab and click **Create**.

b. In the Circuit Creation dialog box, choose the type and size, such as VC HO.

c. Click **Next**.

d. In the next Circuit Creation dialog box, give the circuit an easily identifiable name such as STMN1toSTMN2.

e. Leave the **Bidirectional** check box checked. Leave the default value for State.

f. Click **Next**.

g. In the Circuit Creation source dialog box, select the same **Node**, **Slot**, **Port**, **VC**, and **Tug** where the test set is connected.

h. Click **Next**.

i. In the Circuit Creation destination dialog box, use the same **Node**, **Slot**, **Port**, **VC**, and **Tug** used for the source dialog box.

j. In the Circuit Creation circuit routing preferences dialog box, leave all defaults.

k. In the VC Optimization dialog box, leave all defaults.

l. Click **Finish**.

Step 4 Confirm that the newly created circuit appears on the Circuits tab list and is described in the Dir column as a two-way circuit.

Note It is normal for the "LPBKTERMINAL (STM1E, STMN)" condition, page 2-159 to appear during a loopback setup. The condition clears when you remove the loopback.

Step 5 Create the terminal (inward) loopback on the destination port being tested:

a. In node view, double-click the card that requires the loopback, such as the destination optical card in the source node.

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

c. Select **Locked,maintenance** from the Admin State column. If this is a multiport card, select the row appropriate for the desired port.

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

e. Click **Apply**.

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

Step 6 Complete the "Test and Clear the Terminal Loopback Circuit" procedure on page 1-43.

Test and Clear the Terminal Loopback Circuit

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

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

Step 3 If the test set indicates a good circuit, 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 > Port** tabs.

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

d. Select the appropriate state (Unlocked; Locked,disabled; Unlocked,automaticInService) in the Admin State column for the port being tested.

e. Click **Apply**.

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

Step 4 Clear the terminal loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

Step 5 Complete the "Test the Optical Card" procedure on page 1-43.

Test the Optical Card

Step 1 Complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the suspected bad card and replace it with a known-good one.

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

Step 3 If the test set indicates a good circuit, the problem is probably the defective card. Return the defective card to Cisco through the RMA process. Log into the Cisco 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 Cisco TAC numbers for your country.

Step 4 Complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the faulty card.

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

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

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

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

d. Select the appropriate state (Unlocked; Locked,disabled; Unlocked,automaticInService) in the Admin State column for the port being tested.

e. Click **Apply**.

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

Step 6 Clear the terminal loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

Step 7 Complete the "Perform an XC Loopback on the Source Optical Port" procedure on page 1-44.

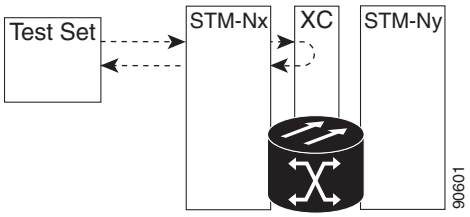
1.3.3 Perform an XC Loopback on the Source Optical Port

Note This procedure is only performed on STM-N cards and cross-connect cards.

Note You can perform an XC loopback on either the circuit source working or the protect port of a 1+1 protection group.

The cross-connect (XC) loopback test occurs on the XC-VXL cross-connect card in a network circuit. Completing a successful XC loopback from an optical card through the cross-connect card eliminates the cross-connect card as the source of trouble for a faulty circuit. Figure 1-22 shows an example of an XC loopback path on a source STM-N port.

Figure 1-22 XC Loopback on a Source STM-N Port



Complete the "Create the XC Loopback on the Source STM-N Port" procedure on page 1-45.

Create the XC Loopback on the Source STM-N Port

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

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

a. If you just completed the "Perform a Terminal (Inward) Loopback on a Source-Node Optical Port" procedure on page 1-41, 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 transmit and receive terminals of the optical test set to the port you are testing. The transmit and receive terminals connect to the same port.

Step 2 Adjust the test set accordingly.

Step 3 Use CTC to put the circuit being tested out of service:

a. In node view, click the **Circuits** tab.

b. Click the circuit and then click **Edit**.

c. In the Edit Circuit dialog box, click the **State** tab.

d. Choose **Locked,maintenance** from the Target Circuit State drop-down list.

e. Click **Apply**.

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

Step 4 Use CTC to set up the XC loopback on the circuit being tested:

a. In node view, double-click the optical card to display the card view.

b. Click the **Maintenance > Loopback > VC4** tabs.

c. Click the check box in the XC Loopback column for the port being tested.

d. Click **Apply**.

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

Step 5 Complete the "Test and Clear the XC Loopback Circuit" procedure on page 1-46.

Test and Clear the XC Loopback Circuit

Note This procedure is performed only on optical cards.

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

Step 2 Examine the test 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 a good circuit, no further testing is necessary with the cross-connect. Clear the XC loopback:

a. In card view, click the **Maintenance > Loopback > VC4** tabs.

b. Uncheck the check box in the XC Loopback column for the circuit being tested.

c. Click **Apply**.

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

Step 4 Complete the "Test the Standby XC-VXL Cross-Connect Card" procedure on page 1-46.

Test the Standby XC-VXL Cross-Connect Card

Note This procedure is performed only on XC cards.

Step 1 Perform a reset on the standby cross-connect card:

a. Determine the standby cross-connect card. On both the physical node and the CTC node view window, the standby cross-connect ACT/STBY LED is amber and the active card ACT/STBY LED is green.

b. Position the cursor over the standby cross-connect card.

c. Right-click and choose **RESET CARD**.

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

Step 2 Initiate an external switching command (side switch) on the cross-connect cards before you retest the loopback circuit:

Caution Cross-connect side switches are service-affecting. Any live traffic on any card in the node endures a hit of up to 50 ms.

a. Determine the standby cross-connect card. On both the physical node and the CTC node view window, the standby cross-connect ACT/STBY LED is amber and the active card ACT/STBY LED is green.

b. In the node view, select the **Maintenance > Cross-Connect > Card** tabs.

c. In the Cross-Connect Cards area, click **Switch**.

d. Click **Yes** in the Confirm Switch dialog box.

Note After the active cross-connect goes into standby mode, the original standby card becomes active and its ACT/STBY LED turns green. The former active card becomes standby and its ACT/STBY LED turns amber.

Step 3 Resend test traffic on the loopback circuit.

The test traffic now travels through the alternate cross-connect card.

Step 4 If the test set indicates a faulty circuit, assume the cross-connect card is not causing the problem. Clear the XC loopback circuit:

a. Click the **Circuits** tab.

b. Choose the XC loopback circuit being tested.

c. Click **Delete**.

d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

e. Confirm that the XC loopback circuit is deleted form the Circuits tab list. If the test set indicates a good circuit, the problem might be a defective cross-connect card.

Step 5 To confirm a defective original cross-connect card, complete the "Retest the Original XC-VXL Cross-Connect Card" procedure on page 1-47.

Retest the Original XC-VXL Cross-Connect Card

Note This procedure is performed only on STM-N and XC cards.

Step 1 Initiate an external switching command (side switch) on the cross-connect cards:

a. Determine the standby cross-connect card. On both the physical node and the CTC node view window, the standby cross-connect ACT/STBY LED is amber and the active card ACT/STBY LED is green.

b. In node view, select the **Maintenance > Cross-Connect > Card** tabs.

c. In the Cross-Connect Cards area, click **Switch**.

d. Click **Yes** in the Confirm Switch dialog box.

Note After the active cross-connect goes into standby mode, the original standby card becomes active and its ACT/STBY LED turns green. The former active card becomes standby and its ACT/STBY LED turns amber.

Step 2 Resend test traffic on the loopback circuit.

Step 3 If the test set indicates a faulty circuit, the problem is probably the defective card. Return the defective card to Cisco through the RMA process. Log into the Cisco 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 Cisco TAC numbers for your country.

Step 4 Proceed to Step 5. If the circuit is not shown to be faulty and the card is not shown to be defective, you are finished with testing.

Step 5 Complete the "Physically Replace an In-Service Cross-Connect Card" procedure on page 2-242 for the defective cross-connect card and perform Step 6.

Step 6 If the test set indicates a good circuit, the cross-connect card might have had a temporary problem that was cleared by the side switch. Clear the XC loopback circuit:

a. Click the **Circuits** tab.

b. Choose the XC loopback circuit being tested.

c. Click **Delete**.

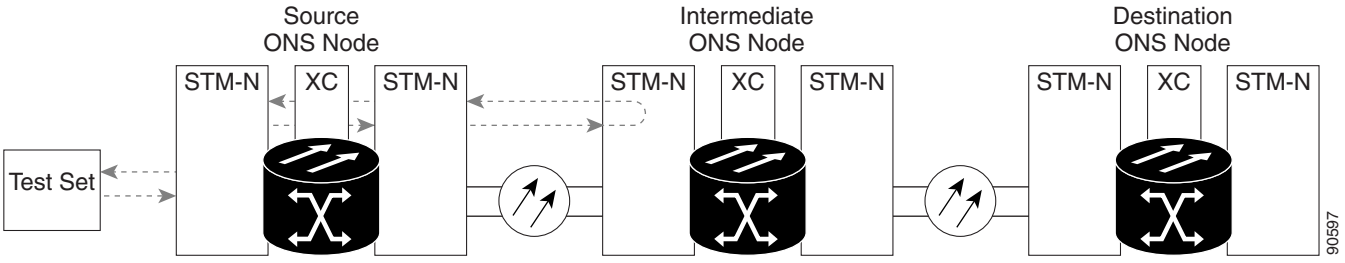
d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

Step 7 Complete the "Perform a Facility (Line) Loopback on an Intermediate-Node Optical Port" procedure on page 1-48.

1.3.4 Perform a Facility (Line) Loopback on an Intermediate-Node Optical Port

Performing the facility (line) loopback test on an intermediate port isolates whether this node is causing circuit failure. In the situation shown in Figure 1-23, the test is being performed on an intermediate STM-N port.

Figure 1-23 Facility Loopback Path to an Intermediate-Node STM-N Port



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

Complete the "Create the Facility (Line) Loopback on an Intermediate-Node Optical Port" procedure on page 1-48.

Create the Facility (Line) Loopback on an Intermediate-Node Optical Port

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

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

a. If you just completed the "Perform an XC Loopback on the Source Optical Port" procedure on page 1-44, 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-node port, use appropriate cabling to attach the transmit and receive terminals of the optical test set to the port you are testing. Both transmit and receive connect to the same port.

Step 2 Adjust the test set accordingly.

Step 3 Use CTC to set up the facility (line) loopback on the test port:

a. In node view, click the **Circuits** tab and click **Create**.

b. In the Circuit Creation dialog box, choose the type and size, such as a VC HO.

c. Click **Next**.

d. In the next Circuit Creation dialog box, give the circuit an easily identifiable name such as STMN1toSTMN3.

e. Leave the **Bidirectional** check box checked. Leave the default value for State.

f. Click **Next**.

g. In the Circuit Creation source dialog box, select the same **Node**, **Slot**, **Port**, **VC**, and **Tug** where the test set is connected.

h. Click **Next**.

i. In the Circuit Creation destination dialog box, use the same **Node**, **Slot**, **Port**, **VC**, and **Tug** used for the source dialog box.

j. Click **Next**.

k. In the Circuit Creation circuit routing preferences dialog box, leave all defaults.

l. If the VC Optimization dialog box appears, leave all defaults.

m. Click **Finish**.

Step 4 Confirm that the newly created circuit appears on the Circuits tab list and that it is described in the Dir column as a two-way circuit.

Note It is normal for a "LPBKFACILITY (STM1E, STMN)" condition, page 2-155. The condition clears when you remove the loopback.

Step 5 Create the facility (line) loopback on the destination port being tested:

a. Go to the node view of the intermediate node:

- From the **View** menu choose **Go To Other Node**.
- Choose the node from the drop-down list in the Select Node dialog box and click **OK**.

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

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

d. Select **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 6 Complete the "Test and Clear the Facility (Line) Loopback Circuit" procedure on page 1-50.

Test and Clear the Facility (Line) Loopback Circuit

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

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

Step 3 If the test set indicates a good circuit, no further testing is necessary with the facility loopback. Clear the facility loopback state on the port:

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

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

c. Choose the appropriate state (Unlocked; Locked,disabled; Unlocked,automaticInService) from the Admin State column for the port being tested.

d. Click **Apply**.

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

Step 4 Clear the facility (line) loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

Step 5 Complete the "Test the Optical Card" procedure on page 1-50.

Test the Optical Card

Step 1 Complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the suspected bad card and replace it with a known-good one.

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

Step 3 If the test set indicates a good circuit, the problem is probably the defective card. Return the defective card to Cisco through the RMA process. Log into the Cisco 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 Cisco TAC numbers for your country.

Step 4 Complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the faulty card.

Step 5 Clear the facility (line) loopback on the port:

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

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

c. Choose the appropriate state (Unlocked; Locked,disabled; Unlocked,automaticInService) from the Admin State column for the port being tested.

d. Click **Apply**.

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

Step 6 Clear the facility loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

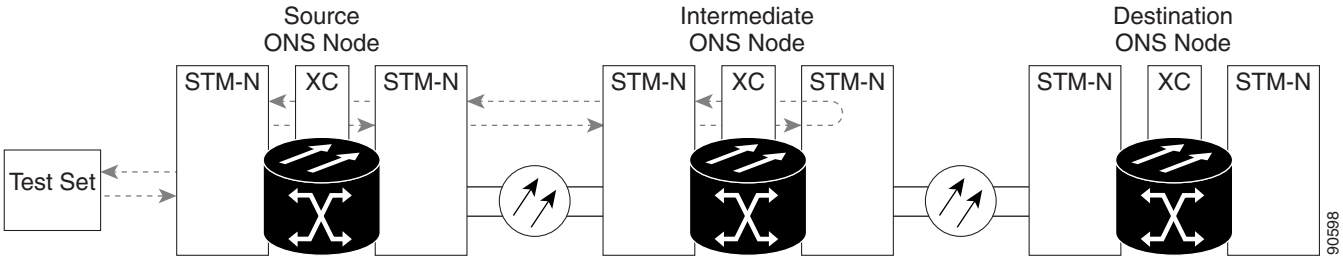
d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

Step 7 Complete the "Perform a Terminal (Inward) Loopback on an Intermediate-Node Optical Ports" procedure on page 1-51.

1.3.5 Perform a Terminal (Inward) Loopback on an Intermediate-Node Optical Ports

In the next trouble-shooting test, you perform a terminal loopback on the intermediate-node port to isolate whether the destination port is causing circuit trouble. In the example situation in Figure 1-24, the terminal loopback is performed on the intermediate optical port in the circuit. You first create a bidirectional circuit that originates on the source-node optical port and loops back on the node destination port. You then proceed with the terminal loopback test. If you successfully complete a terminal loopback on the node, this node is excluded from possible sources of circuit trouble.

Figure 1-24 Terminal Loopback Path to an Intermediate-Node STM-N Port



STM-N cards placed in facility loopback state display an icon, shown in Figure 1-25.

Figure 1-25 Facility Loopback Indicator

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

Complete the "Create the Terminal Loopback on Intermediate-Node Optical Ports" procedure on page 1-52.

Create the Terminal Loopback on Intermediate-Node Optical Ports

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

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

a. If you just completed the "Perform a Facility (Line) Loopback on an Intermediate-Node Optical Port" procedure on page 1-48, 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 transmit and receive terminals of the optical test set to the port you are testing. Both transmit and receive connect to the same port.

Step 2 Adjust the test set accordingly.

Step 3 Use CTC to set up the terminal (inward) loopback on the test port:

a. In node view, click the **Circuits** tab and click **Create**.

b. In the Circuit Creation dialog box, choose the type and size, such as a VC HO.

c. Click **Next**.

d. In the next Circuit Creation dialog box, give the circuit an easily identifiable name such as STM1toSTM4.

e. Leave the **Bidirectional** check box checked. Leave the default value for State.

f. Click **Next**.

g. In the Circuit Creation source dialog box, select the same **Node**, **Slot**, **Port**, **VC**, and **Tug** where the test set is connected.

h. Click **Next**.

i. In the Circuit Creation destination dialog box, use the same **Node**, **Slot**, **Port**, **VC**, and **Tug** used for the source dialog box.

j. Click **Next**.

k. In the Circuit Creation circuit routing preferences dialog box, leave all defaults.

l. If the VC Optimization dialog box appears, leave all defaults.

m. Click **Finish**.

Step 4 Confirm that the newly created circuit appears on the Circuits tab list and that it is described as a two-way circuit in the Dir column.

Note It is normal for the "LPBKTERMINAL (STM1E, STMN)" condition, page 2-159 to appear during a loopback setup. The condition clears when you remove the loopback.

Step 5 Create the terminal loopback on the destination port being tested:

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

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

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

d. Select **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 6 Complete the "Test and Clear the Optical Terminal Loopback Circuit" procedure on page 1-53.

Test and Clear the Optical Terminal Loopback Circuit

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

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

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

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

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

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

d. Select the appropriate state (Unlocked; Locked,disabled; Unlocked,automaticInService) in the Admin State column for the port being tested.

e. Click **Apply**.

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

Step 4 Clear the terminal loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

Step 5 Complete the "Test the Optical Card" procedure on page 1-54.

Test the Optical Card

Step 1 Complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the suspected bad card and replace it with a known-good one.

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

Step 3 If the test set indicates a good circuit, the problem is probably the defective card. Return the defective card to Cisco through the RMA process. Log into the Cisco 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 Cisco TAC numbers for your country.

Step 4 Complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the defective card.

Step 5 Clear the terminal loopback on the port:

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

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

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

d. Select the appropriate state (Unlocked; Locked,disabled; Unlocked,automaticInService) in the Admin State column for the port being tested.

e. Click **Apply**.

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

Step 6 Clear the terminal loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

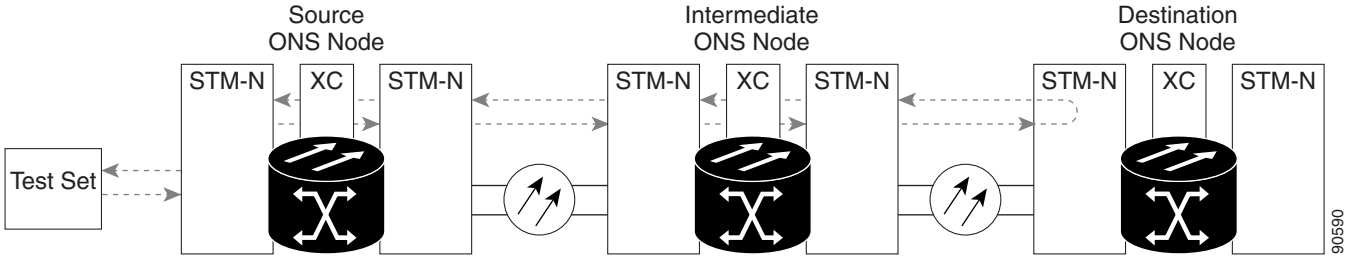
d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

Step 7 Complete the "Perform a Facility (Line) Loopback on a Destination-Node Optical Port" procedure on page 1-54.

1.3.6 Perform a Facility (Line) Loopback on a Destination-Node Optical Port

You perform a facility (line) loopback test at the destination port to determine whether this local port is the source of circuit trouble. The example in Figure 1-26 shows a facility loopback being performed on an STM-N port.

Figure 1-26 Facility Loopback Path to a Destination-Node STM-N Port



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

Complete the "Create the Facility (Line) Loopback on a Destination-Node Optical Port" procedure on page 1-55.

Create the Facility (Line) Loopback on a Destination-Node Optical Port

Step 1 Connect an optical test set to the port you are testing. For specific procedures to use the test set equipment, consult the manufacturer.

a. If you just completed the "Perform a Terminal (Inward) Loopback on an Intermediate-Node Optical Ports" procedure on page 1-51, 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 transmit and receive terminals of the optical test set to the port you are testing. Both transmit and receive connect to the same port.

Step 2 Adjust the test set accordingly.

Step 3 Use CTC to set up the hairpin circuit on the test port:

a. In node view, click the **Circuits** tab and click **Create**.

b. In the Circuit Creation dialog box, choose the type and size, such as VC HO.

c. Click **Next**.

d. In the next Circuit Creation dialog box, give the circuit an easily identifiable name such as STMN1toSTMN5.

e. Leave the **Bidirectional** check box checked. Leave the default value for State.

f. Click **Next**.

g. In the Circuit Creation source dialog box, select the same **Node**, **Slot**, **Port**, **VC,** and **Tug** where the test set is connected.

h. Click **Next**.

i. In the Circuit Creation destination dialog box, use the same **Node**, **Slot**, **Port**, **VC**, and **Tug** used for the source dialog box.

j. Click **Next**.

k. In the Circuit Creation circuit routing preferences dialog box, leave all defaults.

l. If the VC Optimization dialog box appears, leave all defaults.

m. Click **Finish**.

Step 4 Confirm that the newly created circuit appears on the Circuits tab list and that it is described in the Dir column as a two-way circuit.

Note It is normal for the "LPBKFACILITY (STM1E, STMN)" condition, page 2-155 to appear during a loopback setup. The condition clears when you remove the loopback.

Step 5 Create the facility (line) loopback on the destination port being tested:

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

b. In node view, double-click the card that requires the loopback, such as the destination-node optical, G-Series, MXP, or TXP card.

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

d. Select **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.

Note It is normal for the "LPBKFACILITY (STM1E, STMN)" condition, page 2-155 to appear during a loopback setup. The condition clears when you remove the loopback.

Step 6 Complete the "Test and Clear the Facility (Line) Loopback Circuit" procedure on page 1-50.

Test the Optical Facility (Line) Loopback Circuit

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

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

Step 3 If the test set indicates a good circuit, no further testing is necessary with the facility loopback. Clear the facility loopback on the port:

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

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

c. Choose the appropriate state (Unlocked; Locked,disabled; Unlocked,automaticInService) from the Admin State column for the port being tested.

d. Click **Apply**.

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

Step 4 Clear the facility loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

Step 5 Complete the "Test the Optical Card" procedure on page 1-57.

Test the Optical Card

Step 1 Complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the suspected bad card and replace it with a known-good one.

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

Step 3 If the test set indicates a good circuit, the problem is probably the defective card. Return the defective card to Cisco through the RMA process. Log into the Cisco 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 Cisco TAC numbers for your country.

Step 4 Complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the faulty card.

Step 5 Clear the facility (line) loopback on the port:

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

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

c. Choose the appropriate state (Unlocked; Locked,disabled; Unlocked,automaticInService) from the Admin State column for the port being tested.

d. Click **Apply**.

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

Step 6 Clear the facility loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

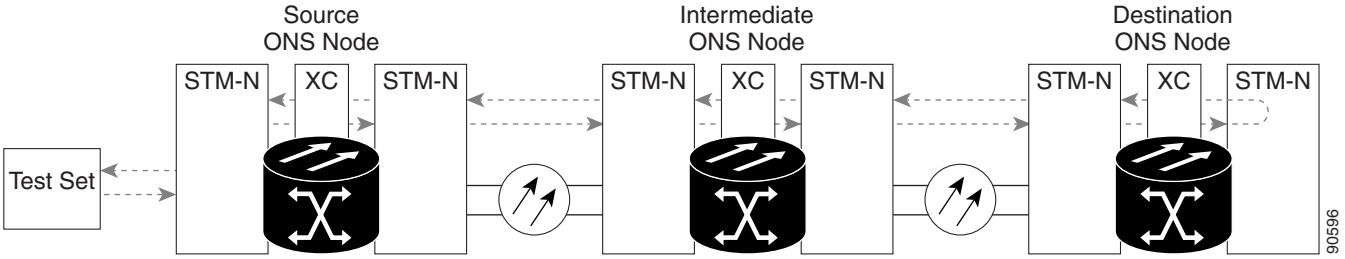
d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

Step 7 Complete the "Perform a Terminal Loopback on a Destination-Node Optical Port" procedure on page 1-57.

1.3.7 Perform a Terminal Loopback on a Destination-Node Optical Port

The terminal loopback at the destination-node port is the final local hardware error elimination in the circuit troubleshooting process. If this test is completed successfully, you have verified that the circuit is good up to the destination port. The example in Figure 1-27 shows a terminal loopback on an intermediate-node destination STM-N port.

Figure 1-27 Terminal Loopback Path to a Destination-Node STM-N Port



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

Complete the "Create the Terminal Loopback on a Destination-Node Optical Port" procedure on page 1-58.

Create the Terminal Loopback on a Destination-Node Optical Port

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

Note For instructions to use the test-set equipment, consult the manufacturer.

a. If you just completed the "Perform a Facility (Line) Loopback on a Destination-Node Optical Port" procedure on page 1-54, 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 transmit and receive terminals of the optical test set to the port you are testing. Both transmit and receive connect to the same port.

Step 2 Adjust the test set accordingly.

Step 3 Use CTC to set up the terminal loopback on the test port:

a. In node view, click the **Circuits** tab and click **Create**.

b. In the Circuit Creation dialog box, choose the type and size, such as a VC HO.

c. Click **Next**.

d. In the next Circuit Creation dialog box, give the circuit an easily identifiable name such as STMN1toSTMN6.

e. Leave the **Bidirectional** check box checked. Do not change the State default value.

f. Click **Next**.

g. In the Circuit Creation source dialog box, select the same **Node**, **Slot**, **Port**, **VC**, and **Tug** where the test set is connected.

h. Click **Next**.

i. In the Circuit Creation destination dialog box, use the same **Node**, **Slot**, **Port**, **VC**, and **Tug** used for the source dialog box.

j. Click **Next**.

k. In the Circuit Creation circuit routing preferences dialog box, leave all defaults.

l. If the VC Optimization dialog box appears, leave all defaults.

m. Click **Finish**.

Step 4 Confirm that the newly created circuit appears on the Circuits tab list and that it is described in the Dir column as a two-way circuit.

Note It is normal for the "LPBKTERMINAL (STM1E, STMN)" condition, page 2-159 to appear during a loopback setup. The condition clears when you remove the loopback.

Step 5 Create the terminal loopback on the destination port being tested:

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

- From the **View** menu choose **Go To Other Node**.
- Choose the node from the drop-down list in the Select Node dialog box and click **OK**.

b. In node view, double-click the card that requires the loopback, such as the destination-node optical, G-Series, MXP, or TXP card.

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

d. Select **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 6 Complete the "Test and Clear the Optical Terminal Loopback Circuit" procedure on page 1-59.

Test and Clear the Optical Terminal Loopback Circuit

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

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

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

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

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

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

d. Select the appropriate state (Unlocked; Locked,disabled; Unlocked,automaticInService) in the Admin State column for the port being tested.

e. Click **Apply**.

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

Step 4 Clear the terminal loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

Step 5 The entire circuit path has now passed its comprehensive series of loopback tests. This circuit qualifies to carry live traffic. If the test set indicates a faulty circuit, the problem might be a faulty card.

Step 6 Complete the "Test the Optical Card" procedure on page 1-60.

Test the Optical Card

Step 1 Complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the suspected bad card and replace it with a known-good one.

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

Step 3 If the test set indicates a good circuit, the problem is probably the defective card. Return the defective card to Cisco through the RMA process. Log into the Cisco 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 Cisco TAC numbers for your country.

Step 4 Complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the defective card.

Step 5 Clear the terminal loopback on the port:

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

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

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

d. Select the appropriate state (Unlocked; Locked,disabled; Unlocked,automaticInService) in the Admin State column for the port being tested.

e. Click **Apply**.

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

Step 6 Clear the terminal loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

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

1.4 Troubleshooting Ethernet Circuit Paths With Loopbacks

Terminal loopbacks, hairpin circuits, and terminal loopbacks can be used in the order shown in this section to troubleshoot an Ethernet circuit path for the G-Series card. E-Series and ML-Series do not have this capability in Software Release 6.0. The example in this section tests a G1000 circuit on a three-node MS-SPRing. Using a series of facility (line) loopbacks and terminal (inward) 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 The test sequence for your circuits will differ according to the type of circuit and network topology.

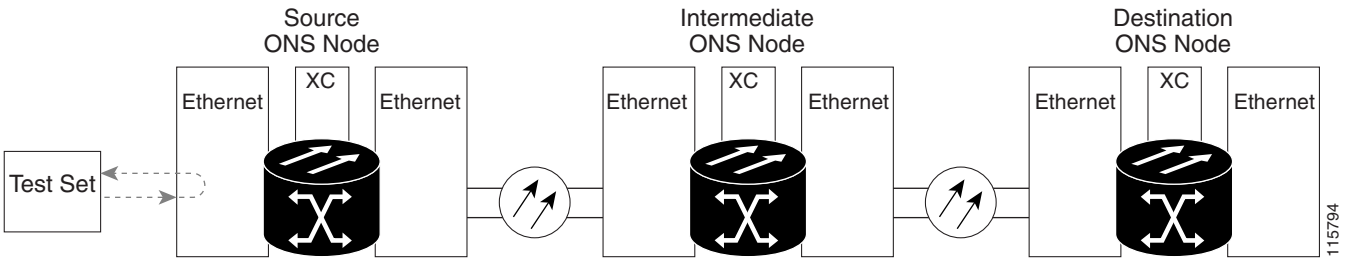
1. A facility (line) loopback on the source-node Ethernet port
2. A terminal (inward) loopback on the source-node Ethernet port
3. A facility (line) loopback on the intermediate-node Ethernet port
4. A terminal (inward) loopback on the intermediate-node Ethernet port
5. A facility (line) loopback on the destination-node Ethernet port
6. A terminal (inward) loopback on the destination-node Ethernet port

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

1.4.1 Perform a Facility (Line) Loopback on a Source-Node Ethernet Port

The facility (line) loopback test is performed on the node source port in the network circuit. In the testing situation used in this example, the source G1000 port in the source node. Completing a successful facility (line) loopback on this port isolates the G1000 port as a possible failure point. Figure 1-28 shows an example of a facility loopback on a circuit source Ethernet port.

Figure 1-28 Facility (Line) Loopback on a Circuit Source Ethernet Port



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

Complete the "Create the Facility (Line) Loopback on the Source-Node Ethernet Port" procedure on page 1-62.

Create the Facility (Line) Loopback on the Source-Node Ethernet Port

Step 1 Connect an optical test set to the port you are testing. For instructions to use the test-set equipment, consult the manufacturer.

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

Step 2 Adjust the test set accordingly.

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

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

Step 5 Choose **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 a "LPBKFACILITY (G1000)" condition on page 2-154 to appear during loopback setup. The condition clears when you remove the loopback.

Step 9 Complete the "Test and Clear the Facility (Line) Loopback Circuit" procedure on page 1-62.

Test and Clear the Facility (Line) Loopback Circuit

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

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

Step 3 If the test set indicates a good circuit, no further testing is necessary with the facility loopback. Clear the facility (line) loopback:

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

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

c. Choose the appropriate state (Unlocked; Locked,disabled; Unlocked,automaticInService) from the Admin State column for the port being tested.

d. Click **Apply**.

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

Step 4 Complete the "Test the Ethernet Card" procedure on page 1-63.

Test the Ethernet Card

Step 1 Complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the suspected bad card and replace it with a known-good one.

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

Step 3 If the test set indicates a good circuit, the problem was probably the defective card. Return the defective card to Cisco through the RMA process. Log into the Cisco 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 Cisco TAC numbers for your country.

Step 4 Complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the faulty card.

Step 5 Clear the facility (line) loopback:

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

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

c. Choose the appropriate state (Unlocked; Locked,disabled; Unlocked,automaticInService) from the Admin State column for the port being tested.

d. Click **Apply**.

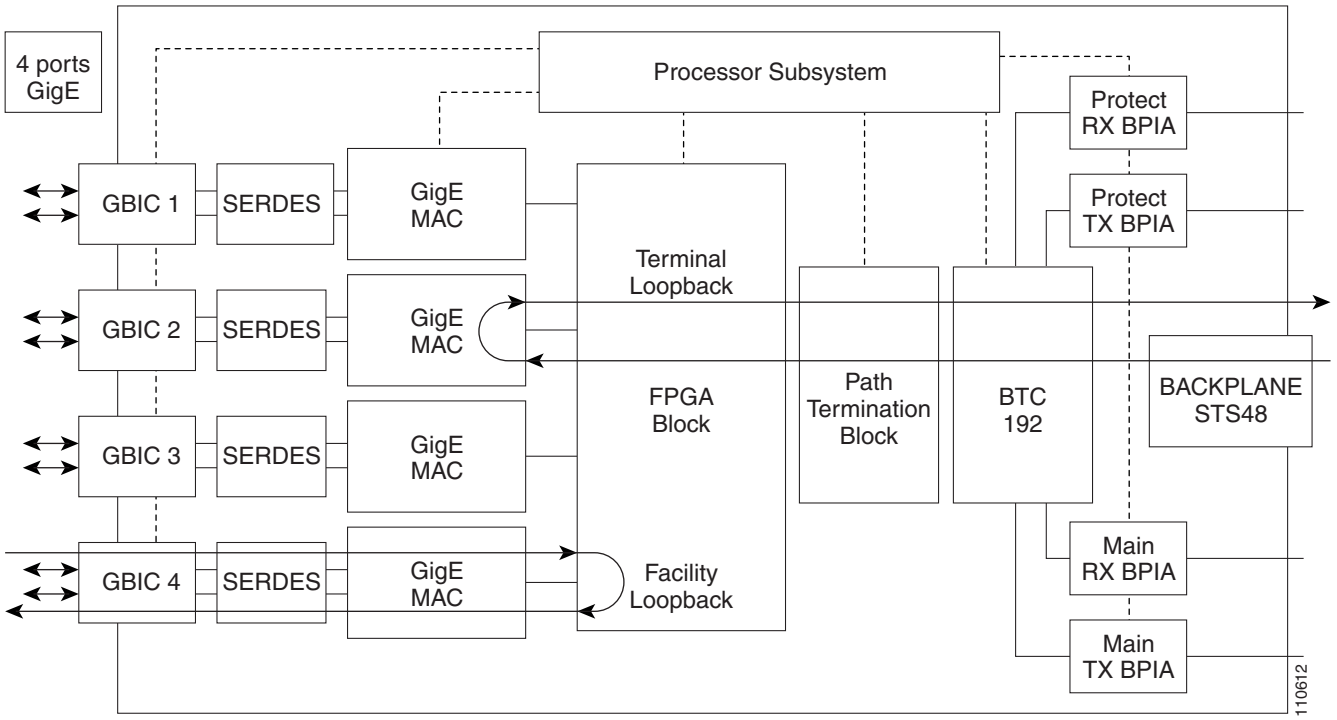
e. Click **Yes** in the confirmation dialog box.

Step 6 Complete the "Perform a Terminal (Inward) Loopback on a Source-Node Ethernet Port" procedure on page 1-63.

1.4.2 Perform a Terminal (Inward) Loopback on a Source-Node Ethernet Port

The terminal (inward) loopback test is performed on the node source Ethernet port. For the circuit in this example, it is the source G1000 port in the source node. You first create a bidirectional circuit that starts on the node destination G1000 port and loops back on the node source G1000 port.You then proceed with the terminal loopback test. Completing a successful terminal loopback to a node source port verifies that the circuit is good to the source port. Figure 1-29 shows terminal loopback on a G-Series port.

Figure 1-29 Terminal (Inward) Loopback on a G-Series Port



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

Complete the "Create the Terminal (Inward) Loopback on a Source-Node Ethernet Port" procedure on page 1-64.

Create the Terminal (Inward) Loopback on a Source-Node Ethernet Port

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

Note For instructions to use the test-set equipment, consult the manufacturer.

a. If you just completed the "Perform a Facility (Line) Loopback on a Source-Node Ethernet Port" procedure on page 1-61, leave the optical test set hooked up to the Ethernet 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 transmit and receive terminals of the optical test set to the port you are testing. Both transmit and receive connect to the same port.

Step 2 Adjust the test set accordingly.

Step 3 Use CTC to set up the terminal (inward) loopback on the test port:

a. In node view, click the **Circuits** tab and click **Create**.

b. In the Circuit Creation dialog box, choose the type, such as VC_HO, and number, such as 1.

c. Click **Next**.

d. In the next Circuit Creation dialog box, give the circuit an easily identifiable name such as G1K1toG1K2.

e. Leave the **Bidirectional** check box checked.

f. Click **Next**.

g. In the Circuit Creation source dialog box, select the same **Node**, **Slot**, **Port**, **VC, and Tug** where the test set is connected.

h. Click **Next**.

i. In the Circuit Creation destination dialog box, use the same **Node**, **Slot**, **Port**, **VC, and Tug** used for the source dialog box.

j. Click **Next**.

k. In the Circuit Creation circuit routing preferences dialog box, leave all defaults. Click **Finish**.

Step 4 Confirm that the newly created circuit appears on the Circuits tab list as a two-way circuit.

Note It is normal for the "LPBKTERMINAL (G1000)" condition on page 2-158 to appear during a loopback setup. The condition clears when you remove the loopback.

Step 5 Create the terminal (inward) loopback on the destination port being tested:

a. In node view, double-click the card that requires the loopback, such as the destination G1000 card in the source node.

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

c. Select **Locked,maintenance** from the Admin State column. If this is a multiport card, select the row appropriate for the desired port.

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

e. Click **Apply**.

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

Step 6 Complete the "Test and Clear the Ethernet Terminal Loopback Circuit" procedure on page 1-65.

Test and Clear the Ethernet Terminal Loopback Circuit

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

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

Step 3 If the test set indicates a good circuit, 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** tab.

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

d. Select the appropriate state (Unlocked; Locked,disabled; Unlocked,automaticInService) in the Admin State column for the port being tested.

e. Click **Apply**.

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

Step 4 Clear the terminal loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

Step 5 Complete the "Test the Ethernet Card" procedure on page 1-66.

Test the Ethernet Card

Step 1 Complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the suspected bad card and replace it with a known-good one.

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

Step 3 If the test set indicates a good circuit, the problem was probably the defective card. Return the defective card to Cisco through the RMA process. Log into the Cisco 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 Cisco TAC numbers for your country.

Step 4 Complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the defective card.

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

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

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

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

d. Select the appropriate state (Unlocked; Locked,disabled; Unlocked,automaticInService) in the Admin State column for the port being tested.

e. Click **Apply**.

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

Step 6 Clear the terminal loopback circuit before testing the next segment of the network circuit path:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

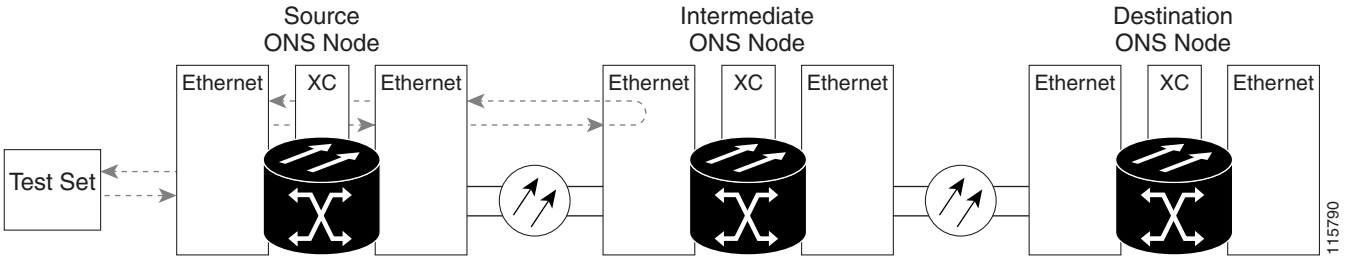
d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

Step 7 Complete the "Perform a Facility (Line) Loopback on an Intermediate-Node Ethernet Port" procedure on page 1-67.

1.4.3 Perform a Facility (Line) Loopback on an Intermediate-Node Ethernet Port

Performing the facility (line) loopback test on an intermediate port isolates whether this node is causing circuit failure. It is shown in Figure 1-30.

Figure 1-30 Facility (Line) Loopback on an Intermediate-Node Ethernet Port



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

Complete the "Create a Facility (Line) Loopback on an Intermediate-Node Ethernet Port" procedure on page 1-67.

Create a Facility (Line) Loopback on an Intermediate-Node Ethernet Port

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

Note For instructions to use the test-set equipment, consult the manufacturer.

a. If you just completed the "Perform a Terminal (Inward) Loopback on a Source-Node Ethernet Port" procedure on page 1-63, 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 transmit and receive terminals of the optical test set to the port you are testing. Both transmit and receive connect to the same port.

Step 2 Adjust the test set accordingly.

Step 3 Use CTC to set up the facility (line) loopback on the test port:

a. In node view, click the **Circuits** tab and click **Create**.

b. In the Circuit Creation dialog box, choose the type, such as VC_HO, and number, such as 1.

c. Click **Next**.

d. In the next Circuit Creation dialog box, give the circuit an easily identifiable name such as G1KtoG1K3.

e. Leave the **Bidirectional** check box checked.

f. Click **Next**.

g. In the Circuit Creation source dialog box, select the same **Node**, **Slot**, **Port**, **VC,** and **Tug** where the test set is connected.

h. Click **Next**.

i. In the Circuit Creation destination dialog box, use the same **Node**, **Slot**, **Port**, **VC**, and **Tug** used for the source dialog box.

j. Click **Next**.

k. In the Circuit Creation circuit routing preferences dialog box, leave all defaults. Click **Finish**.

Step 4 Confirm that the newly created circuit appears on the Circuits tab list as a two-way circuit.

Note It is normal for the "LPBKFACILITY (G1000)" condition on page 2-154 to appear during a loopback setup. The condition clears when you remove the loopback.

Step 5 Create the facility (line) loopback on the destination port being tested:

a. Go to the node view of the intermediate node:

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

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

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

d. Select **OOS,MT** 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 6 Complete the "Test and Clear the Ethernet Facility (Line) Loopback Circuit" procedure on page 1-68.

Test and Clear the Ethernet Facility (Line) Loopback Circuit

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

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

Step 3 If the test set indicates a good circuit, no further testing is necessary with the facility (line) loopback. Clear the facility loopback from the port:

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

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

c. Choose the appropriate state (Unlocked; Locked,disabled; Unlocked,automaticInService) from the Admin State column for the port being tested.

d. Click **Apply**.

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

Step 4 Clear the facility (line) loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

Step 5 Complete the "Test the Ethernet Card" procedure on page 1-69.

Test the Ethernet Card

Step 1 Complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the suspected bad card and replace it with a known-good one.

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

Step 3 If the test set indicates a good circuit, the problem was probably the defective card. Return the defective card to Cisco through the RMA process. Log into the Cisco 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 Cisco TAC numbers for your country.

Step 4 Complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the faulty card.

Step 5 Clear the facility (line) loopback from the port:

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

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

c. Choose the appropriate state (Unlocked; Locked,disabled; Unlocked,automaticInService) from the Admin State column for the port being tested.

d. Click **Apply**.

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

Step 6 Clear the facility loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

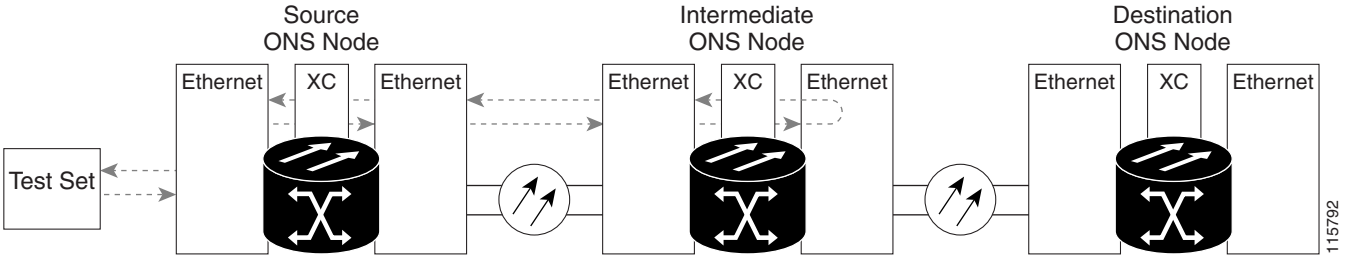
d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

Step 7 Complete the "Perform a Terminal (Inward) Loopback on an Intermediate-Node Ethernet Port" procedure on page 1-69.

1.4.4 Perform a Terminal (Inward) Loopback on an Intermediate-Node Ethernet Port

In the next troubleshooting test, you perform a terminal loopback on the intermediate-node port to isolate whether the destination port is causing circuit trouble. In the example situation in Figure 1-31, the terminal loopback is performed on an intermediate Ethernet port in the circuit. You first create a bidirectional circuit that originates on the source-node Ethernet port and loops back on the intermediate-node port. You then proceed with the terminal loopback test. If you successfully complete a terminal loopback on the node, this node is excluded from possible sources of circuit trouble.

Figure 1-31 Terminal Loopback on an Intermediate-Node Ethernet Port



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

Complete the "Create a Terminal Loopback on an Intermediate-Node Ethernet Port" procedure on page 1-70.

Create a Terminal Loopback on an Intermediate-Node Ethernet Port

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

Note For instructions to use the test-set equipment, consult the manufacturer.

a. If you just completed the "Perform a Facility (Line) Loopback on an Intermediate-Node Ethernet Port" procedure on page 1-67, 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 transmit and receive terminals of the optical test set to the port you are testing. Both transmit and receive connect to the same port.

Step 2 Adjust the test set accordingly.

Step 3 Use CTC to set up the terminal (inward) loopback on the test port:

a. In node view, click the **Circuits** tab and click **Create**.

b. In the Circuit Creation dialog box, choose the type, such as VC_HO, and number, such as 1.

c. Click **Next**.

d. In the next Circuit Creation dialog box, give the circuit an easily identifiable name such as G1K1toG1K4.

e. Leave the **Bidirectional** check box checked.

f. Click **Next**.

g. In the Circuit Creation source dialog box, select the same **Node**, **Slot**, **Port**, **VC**, and **Tug** where the test set is connected.

h. Click **Next**.

i. In the Circuit Creation destination dialog box, use the same **Node**, **Slot**, **Port**, **VC**, and **Tug** used for the source dialog box.

j. Click **Next**.

k. In the Circuit Creation circuit routing preferences dialog box, leave all defaults. Click **Finish**.

Step 4 Confirm that the newly created circuit appears on the Circuits tab list and that it is described in the Dir column as a two-way circuit.

Note It is normal for the "LPBKTERMINAL (G1000)" condition on page 2-158 to appear during a loopback setup. The condition clears when you remove the loopback.

Step 5 Create the terminal loopback on the destination port being tested:

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

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

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

d. Select **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 6 Complete the "Test and Clear the Ethernet Terminal Loopback Circuit" procedure on page 1-71.

Test and Clear the Ethernet Terminal Loopback Circuit

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

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

Step 3 If the test set indicates a good circuit, 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** tab.

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

d. Select the appropriate state (Unlocked; Locked,disabled; Unlocked,automaticInService) in the Admin State column for the port being tested.

e. Click **Apply**.

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

Step 4 Clear the terminal loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

Step 5 Complete the "Test the Ethernet Card" procedure on page 1-72.

Test the Ethernet Card

Step 1 Complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the suspected bad card and replace it with a known-good one.

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

Step 3 If the test set indicates a good circuit, the problem was probably the defective card. Return the defective card to Cisco through the RMA process. Log into the Cisco 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 Cisco TAC numbers for your country.

Step 4 Complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the defective card.

Step 5 Clear the terminal loopback on the port:

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

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

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

d. Select the appropriate state (Unlocked; Locked,disabled; Unlocked,automaticInService) in the Admin State column for the port being tested.

e. Click **Apply**.

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

Step 6 Clear the terminal loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

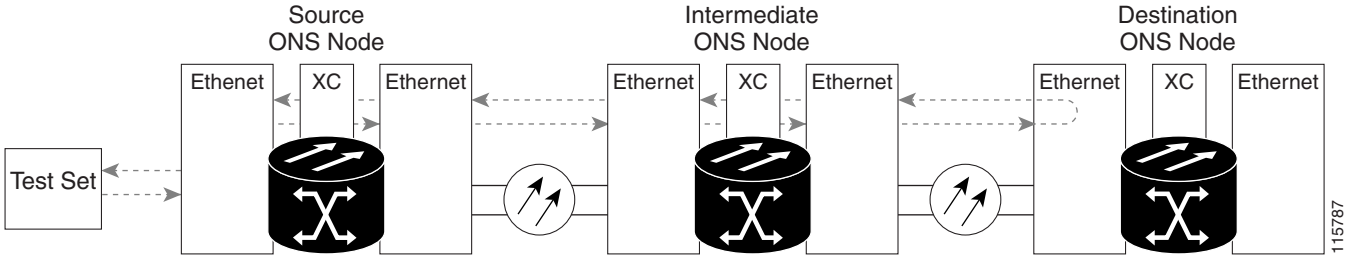
d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

Step 7 Complete the "Perform a Facility (Line) Loopback on a Destination-Node Ethernet Port" procedure on page 1-72.

1.4.5 Perform a Facility (Line) Loopback on a Destination-Node Ethernet Port

You perform a facility (line) loopback test at the destination port to determine whether this local port is the source of circuit trouble. The example in Figure 1-32 shows a facility loopback being performed on an Ethernet port.

Figure 1-32 Facility (Line) Loopback on a Destination-Node Ethernet Port



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

Complete the "Create the Facility (Line) Loopback on a Destination-Node Ethernet Port" procedure on page 1-73.

Create the Facility (Line) Loopback on a Destination-Node Ethernet Port

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

Note For instructions to use the test-set equipment, consult the manufacturer.

a. If you just completed the "Perform a Terminal (Inward) Loopback on an Intermediate-Node Ethernet Port" procedure on page 1-69, 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 transmit and receive terminals of the optical test set to the port you are testing. Both transmit and receive connect to the same port.

Step 2 Adjust the test set accordingly.

Step 3 Use CTC to set up the hairpin circuit on the test port:

a. In node view, click the **Circuits** tab and click **Create**.

b. In the Circuit Creation dialog box, choose the type, such as VC_HO, and number, such as 1.

c. Click **Next**.

d. In the next Circuit Creation dialog box, give the circuit an easily identifiable name such as G1K1toG1K5.

e. Leave the **Bidirectional** check box checked.

f. Click **Next**.

g. In the Circuit Creation source dialog box, select the same **Node**, **Slot**, **Port**, **VC**, and **Tug** where the test set is connected.

h. Click **Next**.

i. In the Circuit Creation destination dialog box, use the same **Node**, **Slot**, **Port**, **VC**, and **Tug** used for the source dialog box.

j. Click **Next**.

k. In the Circuit Creation circuit routing preferences dialog box, leave all defaults. Click **Finish**.

Step 4 Confirm that the newly created circuit appears on the Circuits tab list as a two-way circuit.

Note It is normal for a "LPBKFACILITY (G1000)" condition on page 2-154 to appear during a loopback setup. The condition clears when you remove the loopback.

Step 5 Create the facility (line) loopback on the destination port being tested:

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

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

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

d. Select **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 6 Complete the "Test and Clear the Ethernet Facility (Line) Loopback Circuit" procedure on page 1-74.

Test and Clear the Ethernet Facility (Line) Loopback Circuit

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

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

Step 3 If the test set indicates a good circuit, no further testing is necessary with the facility loopback. Clear the facility (line) loopback from the port:

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

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

c. Choose the appropriate state (Unlocked; Locked,disabled; Unlocked,automaticInService) from the Admin State column for the port being tested.

d. Click **Apply**.

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

Step 4 Clear the facility (line) loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

Step 5 Complete the "Test the Ethernet Card" procedure on page 1-75.

Test the Ethernet Card

Step 1 Complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the suspected bad card and replace it with a known-good one.

Step 2 If the test set indicates a good circuit, the problem was probably the defective card. Return the defective card to Cisco through the RMA process. Log into the Cisco 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 Cisco TAC numbers for your country.

Step 3 Complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the faulty card.

Step 4 Clear the facility (line) loopback on the port:

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

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

c. Choose the appropriate state (Unlocked; Locked,disabled; Unlocked,automaticInService) from the Admin State column for the port being tested.

d. Click **Apply**.

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

Step 5 Clear the facility loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

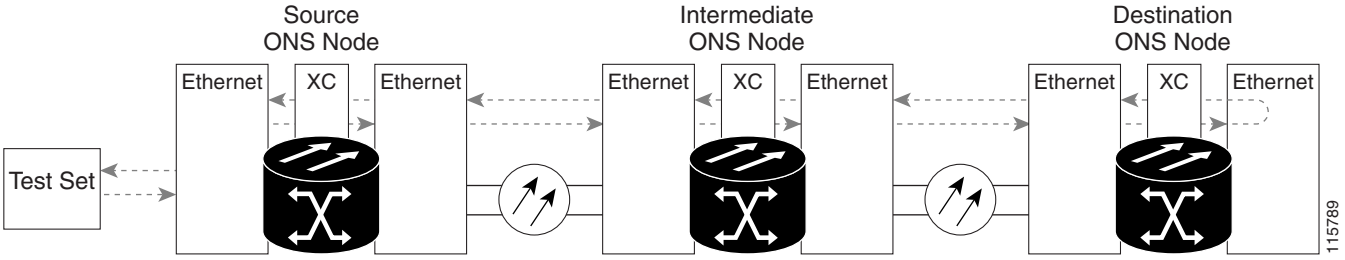
d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

Step 6 Complete the "Perform a Terminal Loopback on a Destination-Node Ethernet Port" procedure on page 1-75.

1.4.6 Perform a Terminal Loopback on a Destination-Node Ethernet Port

The terminal loopback at the destination-node port is the final local hardware error elimination in the circuit troubleshooting process. If this test is completed successfully, you have verified that the circuit is good up to the destination port. The example in Figure 1-33 shows a terminal loopback on an intermediate-node destination Ethernet port.

Figure 1-33 Terminal Loopback on a Destination-Node Ethernet Port



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

Complete the "Create the Terminal Loopback on a Destination-Node Ethernet Port" procedure on page 1-76.

Create the Terminal Loopback on a Destination-Node Ethernet Port

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

Note For instructions to use the test-set equipment, consult the manufacturer.

a. If you just completed the "Perform a Facility (Line) Loopback on a Destination-Node Ethernet Port" procedure on page 1-72, 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 transmit and receive terminals of the optical test set to the port you are testing. Both transmit and receive connect to the same port.

Step 2 Adjust the test set accordingly.

Step 3 Use CTC to set up the terminal loopback on the test port:

a. In node view, click the **Circuits** tab and click **Create**.

b. In the Circuit Creation dialog box, choose the type, such as VC_HO, and number, such as 1.

c. Click **Next**.

d. In the next Circuit Creation dialog box, give the circuit an easily identifiable name such as G1K1toG1K6.

e. Leave the **Bidirectional** check box checked.

f. Click **Next**.

g. In the Circuit Creation source dialog box, select the same **Node**, **Slot**, **Port**, **VC**, and **Tug** where the test set is connected.

h. Click **Next**.

i. In the Circuit Creation destination dialog box, use the same **Node**, **Slot**, **Port**, **VC**, and **Tug** used for the source dialog box.

j. Click **Next**.

k. In the Circuit Creation circuit routing preferences dialog box, leave all defaults. Click **Finish**.

Step 4 Confirm that the newly created circuit appears on the Circuits tab list as a two-way circuit.

Note It is normal for the "LPBKTERMINAL (G1000)" condition on page 2-158 to appear during a loopback setup. The condition clears when you remove the loopback.

Step 5 Create the terminal loopback on the destination port being tested:

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

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

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

d. Select **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 6 Complete the "Test and Clear the Ethernet Terminal Loopback Circuit" procedure on page 1-77.

Test and Clear the Ethernet Terminal Loopback Circuit

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

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

Step 3 If the test set indicates a good circuit, 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** tab.

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

d. Select the appropriate state (Unlocked; Locked,disabled; Unlocked,automaticInService) in the Admin State column for the port being tested.

e. Click **Apply**.

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

Step 4 Clear the terminal loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

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

Step 5 If the test set indicates a faulty circuit, the problem might be a faulty card.

Step 6 Complete the "Test the Ethernet Card" procedure on page 1-78.

Test the Ethernet Card

Step 1 Complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the suspected bad card and replace it with a known-good card.

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

Step 3 If the test set indicates a good circuit, the problem was probably the defective card. Return the defective card to Cisco through the RMA process. Log into the Cisco 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 Cisco TAC numbers for your country.

Step 4 Complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the defective card.

Step 5 Clear the terminal loopback on the port:

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

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

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

d. Select the appropriate state (Unlocked; Locked,disabled; Unlocked,automaticInService) in the Admin State column for the port being tested.

e. Click **Apply**.

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

Step 6 Clear the terminal loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

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

1.5 Troubleshooting MXP, TXP, or FC_MR-4 Circuit Paths With Loopbacks

The MXP, TXP, and FC_MR-4 loopback test for circuit path failure differs from electrical, optical, and Ethernet testing in that loopback testing does not require circuit creation. MXP, TXP, and FC_MR-4 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), muxponder cards (MXP, MXPP), and FC_MR-4 cards. The example in this section tests a circuit on a three-node MS-SPRing. Using a series of facility (line) loopbacks, hairpin circuits, and terminal (inward) loopbacks, the example scenario traces the circuit path, tests the possible failure points, and eliminates them. The logical progression contains six network test procedures:

1. A facility (line) loopback on the source-node MXP/TXP/FC_MR-4 port
2. A terminal (inward) loopback on the source-node MXP/TXP/FC_MR-4 port
3. A facility (line) loopback on the intermediate-node MXP/TXP/FC_MR-4 port
4. A terminal (inward) loopback on the intermediate-node MXP/TXP/FC_MR-4 port
5. A facility (line) loopback on the destination-node MXP/TXP/FC_MR-4 port
6. A terminal (inward) loopback on the destination-node MXP/TXP/FC_MR-4 port

Note Loopbacks are not available for DWDM cards in this release.

Note MXP and TXP card client ports do not appear in the Maintenance > Loopback tab unless they have been provisioned. To provision TXP and MXP pluggable port modules (PPMs), refer to the "Provision Transponder and Muxponder Cards" chapter in the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

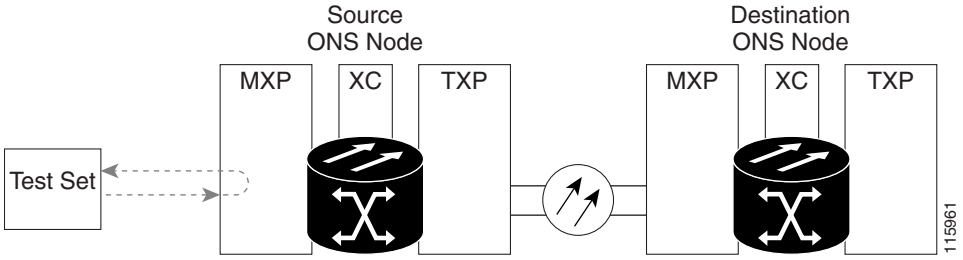
Note The test sequence for your circuits will differ according to the type of circuit and network topology.

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

1.5.1 Perform a Facility (Line) Loopback on a Source-Node MXP/TXP/FC_MR-4 Port

The facility (line) loopback test is performed on the node source port in the network circuit. In the testing situation used in this example, the source muxponder or transponder MXP/TXP/FC_MR-4 port in the source node. Completing a successful facility (line) loopback on this port isolates the MXP/TXP/FC_MR-4 port as a possible failure point. Figure 1-34 shows an example of a facility loopback on a circuit source MXP/TXP/FC_MR-4 port.

Figure 1-34 Facility (Line) Loopback on a Circuit Source MXP/TXP/FC_MR-4 Port



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

Complete the "Create the Facility (Line) Loopback on the Source-Node MXP/TXP/FC_MR-4 Port" procedure on page 1-80.

Create the Facility (Line) Loopback on the Source-Node MXP/TXP/FC_MR-4 Port

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

Note For instructions to use the test-set equipment, consult the manufacturer.

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

Step 2 Adjust the test set accordingly.

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

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

Step 5 Choose **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 a "LPBKFACILITY (FCMR)" condition on page 2-154 to appear during loopback setup. The condition clears when you remove the loopback.

Step 9 Complete the "Test and Clear the MXP/TXP/FC_MR-4 Facility (Line) Loopback Circuit" procedure on page 1-81.

Test and Clear the MXP/TXP/FC_MR-4 Facility (Line) Loopback Circuit

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

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

Step 3 If the test set indicates a good circuit, no further testing is necessary with the facility loopback. Clear the facility (line) loopback:

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

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

c. Choose the appropriate state (Unlocked; Locked,disabled; Unlocked,automaticInService) from the Admin State column for the port being tested.

d. Click **Apply**.

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

Step 4 Complete the "Test the MXP/TXP/FC_MR-4 Card" procedure on page 1-81.

Test the MXP/TXP/FC_MR-4 Card

Step 1 Complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the suspected bad card and replace it with a known-good one.

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

Step 3 If the test set indicates a good circuit, the problem was probably the defective card. Return the defective card to Cisco through the RMA process. Log into the Cisco 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 Cisco TAC numbers for your country.

Step 4 Complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the faulty card.

Step 5 Clear the facility (line) loopback:

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

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

c. Choose the appropriate state (Unlocked; Locked,disabled; Unlocked,automaticInService) from the Admin State column for the port being tested.

d. Click **Apply**.

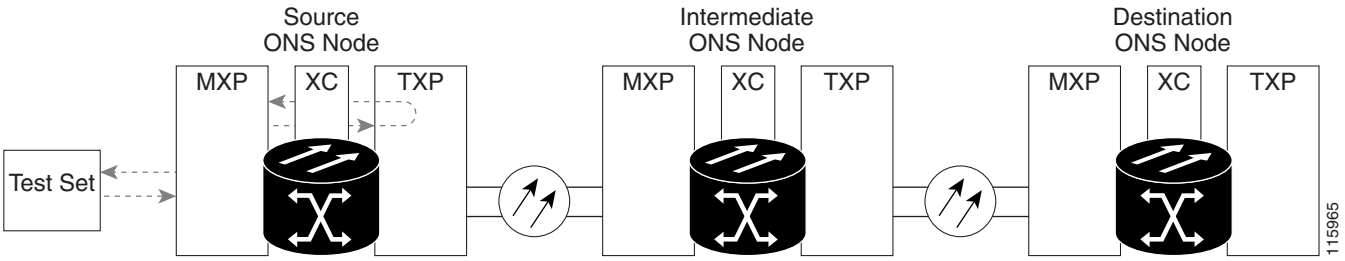
e. Click **Yes** in the confirmation dialog box.

Step 6 Complete the "Perform a Terminal (Inward) Loopback on a Source-Node MXP/TXP/FC_MR-4 Port" procedure on page 1-82.

1.5.2 Perform a Terminal (Inward) Loopback on a Source-Node MXP/TXP/FC_MR-4 Port

The terminal (inward) loopback test is performed on the source-node MXP/TXP/FC_MR-4 port. For the circuit in this example, it is the source MXP/TXP/FC_MR-4 port in the source node. Completing a successful terminal loopback to a node source port verifies that the circuit is good to the source port. Figure 1-35 shows an example of a terminal loopback on a source MXP/TXP/FC_MR-4 port.

Figure 1-35 Terminal (Inward) Loopback on a Source-Node MXP/TXP/FC_MR-4 Port



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

Complete the "Create the Terminal (Inward) Loopback on a Source-Node MXP/TXP/FC_MR-4 Port" procedure on page 1-82.

Create the Terminal (Inward) Loopback on a Source-Node MXP/TXP/FC_MR-4 Port

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

Note For instructions to use the test-set equipment, consult the manufacturer.

a. If you just completed the "Perform a Facility (Line) Loopback on a Source-Node MXP/TXP/FC_MR-4 Port" procedure on page 1-79, leave the optical test set hooked up to the MXP/TXP/FC_MR-4 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 transmit and receive terminals of the optical test set to the port you are testing. Both transmit and receive connect to the same port.

Step 2 Adjust the test set accordingly.

Step 3 In node view, double-click the card that requires the loopback, such as the destination STM-N card in the source node.

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

Step 5 Select **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/FC_MR-4 Port Terminal Loopback Circuit" procedure on page 1-83.

Test and Clear the MXP/TXP/FC_MR-4 Port Terminal Loopback Circuit

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

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

Step 3 If the test set indicates a good circuit, 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** tab.
- **c.** Select **None** from the Loopback Type column for the port being tested.
- **d.** Select the appropriate state (Unlocked; Locked,disabled; Unlocked,automaticInService) in the Admin State column for the port being tested.
- **e.** Click **Apply**.
- **f.** Click **Yes** in the confirmation dialog box.

Step 4 Complete the "Test the MXP/TXP/FC_MR-4 Card" procedure on page 1-83.

Test the MXP/TXP/FC_MR-4 Card

Step 1 Complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the suspected bad card and replace it with a known-good one.

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

Step 3 If the test set indicates a good circuit, the problem was probably the defective card. Return the defective card to Cisco through the RMA process. Log into the Cisco 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 Cisco TAC numbers for your country.

Step 4 Complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the defective card.

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

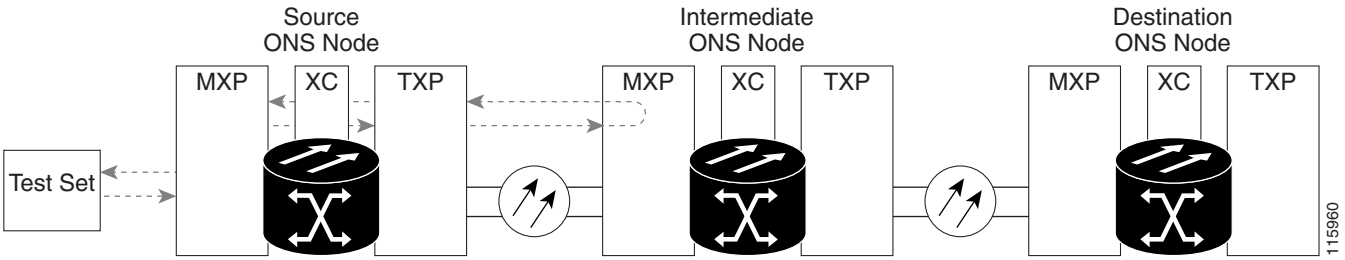
- **a.** Double-click the card in the source node with the terminal loopback.
- **b.** Click the **Maintenance > Loopback** tab.
- **c.** Select **None** from the Loopback Type column for the port being tested.
- **d.** Select the appropriate state (Unlocked; Locked,disabled; Unlocked,automaticInService) in the Admin State column for the port being tested.
- **e.** Click **Apply**.
- **f.** Click **Yes** in the confirmation dialog box.

Step 6 Complete the "Perform a Facility (Line) Loopback on an Intermediate-Node MXP/TXP/FC_MR-4 Port" procedure on page 1-84.

1.5.3 Perform a Facility (Line) Loopback on an Intermediate-Node MXP/TXP/FC_MR-4 Port

Performing the facility (line) loopback test on an intermediate port isolates whether this node is causing circuit failure. In the situation shown in Figure 1-36, the test is being performed on an intermediate MXP/TXP/FC_MR-4 port.

Figure 1-36 Facility (Line) Loopback on an Intermediate-Node MXP/TXP/FC_MR-4 Port



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

Complete the "Create a Facility (Line) Loopback on an Intermediate-Node MXP/TXP/FC_MR-4 Port" procedure on page 1-84.

Create a Facility (Line) Loopback on an Intermediate-Node MXP/TXP/FC_MR-4 Port

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

Note For instructions to use the test-set equipment, consult the manufacturer.

a. If you just completed the "Perform a Terminal (Inward) Loopback on a Source-Node MXP/TXP/FC_MR-4 Port" procedure on page 1-82, 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 transmit and receive terminals of the optical test set to the port you are testing. Both transmit and receive connect to the same port.

Step 2 Adjust the test set accordingly.

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

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

Step 5 Select **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/TXP/FC_MR-4 Port Facility (Line) Loopback Circuit" procedure on page 1-85.

Test and Clear the MXP/TXP/FC_MR-4 Port Facility (Line) Loopback Circuit

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

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

Step 3 If the test set indicates a good circuit, no further testing is necessary with the facility (line) loopback. Clear the facility loopback from the port:

- **a.** Click the **Maintenance > Loopback** tab.
- **b.** Choose **None** from the Loopback Type column for the port being tested.
- **c.** Choose the appropriate state (Unlocked; Locked,disabled; Unlocked,automaticInService) from the Admin State column for the port being tested.
- **d.** Click **Apply**.
- **e.** Click **Yes** in the confirmation dialog box.

Step 4 Complete the "Test the MXP/TXP/FC_MR-4 Card" procedure on page 1-85.

Test the MXP/TXP/FC_MR-4 Card

Step 1 Complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the suspected bad card and replace it with a known-good one.

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

Step 3 If the test set indicates a good circuit, the problem was probably the defective card. Return the defective card to Cisco through the RMA process. Log into the Cisco 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 Cisco TAC numbers for your country.

Step 4 Complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the faulty card.

Step 5 Clear the facility (line) loopback from the port:

- **a.** Click the **Maintenance > Loopback** tab.
- **b.** Choose **None** from the Loopback Type column for the port being tested.
- **c.** Choose the appropriate state (Unlocked; Locked,disabled; Unlocked,automaticInService) from the Admin State column for the port being tested.
- **d.** Click **Apply**.

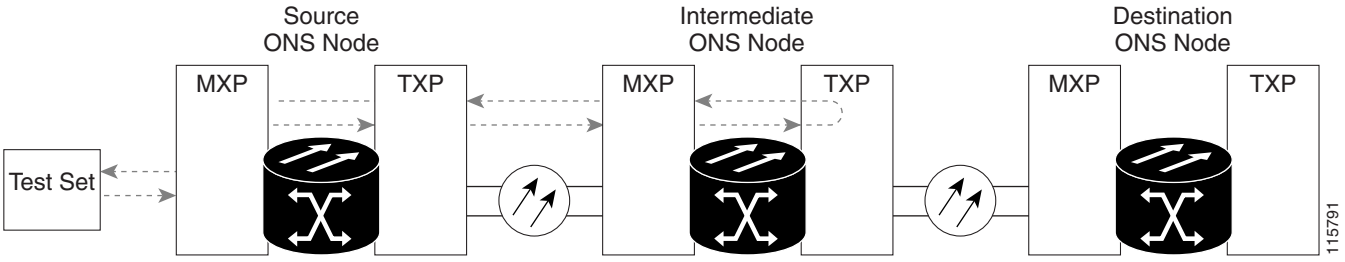
e. Click **Yes** in the confirmation dialog box.

Step 6 Complete the "Perform a Terminal (Inward) Loopback on Intermediate-Node MXP/TXP/FC_MR-4 Ports" procedure on page 1-86.

1.5.4 Perform a Terminal (Inward) Loopback on Intermediate-Node MXP/TXP/FC_MR-4 Ports

In the next troubleshooting test, you perform a terminal loopback on the intermediate-node port to isolate whether the destination port is causing circuit trouble. In the example situation in Figure 1-37, the terminal loopback is performed on an intermediate MXP/TXP/FC_MR-4 port in the circuit. If you successfully complete a terminal loopback on the node, this node is excluded from possible sources of circuit trouble.

Figure 1-37 Terminal Loopback on an Intermediate-Node MXP/TXP/FC_MR-4 Port



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

Complete the "Create a Terminal Loopback on Intermediate-Node MXP/TXP/FC_MR-4 Ports" procedure on page 1-86.

Create a Terminal Loopback on Intermediate-Node MXP/TXP/FC_MR-4 Ports

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

Note For instructions to use the test-set equipment, consult the manufacturer.

a. If you just completed the "Perform a Facility (Line) Loopback on an Intermediate-Node MXP/TXP/FC_MR-4 Port" procedure on page 1-84, 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 transmit and receive terminals of the optical test set to the port you are testing. Both transmit and receive connect to the same port.

Step 2 Adjust the test set accordingly.

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

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

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

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

d. Select **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/FC_MR-4 Terminal Loopback Circuit" procedure on page 1-87.

Test and Clear the MXP/TXP/FC_MR-4 Terminal Loopback Circuit

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

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

Step 3 If the test set indicates a good circuit, 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** tab.

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

d. Select the appropriate state (Unlocked; Locked,disabled; Unlocked,automaticInService) in the Admin State column for the port being tested.

e. Click **Apply**.

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

Step 4 Complete the "Test the MXP/TXP/FC_MR-4 Card" procedure on page 1-87.

Test the MXP/TXP/FC_MR-4 Card

Step 1 Complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the suspected bad card and replace it with a known-good one.

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

Step 3 If the test set indicates a good circuit, the problem was probably the defective card. Return the defective card to Cisco through the RMA process. Log into the Cisco 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 Cisco TAC numbers for your country.

Step 4 Complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the defective card.

Step 5 Clear the terminal loopback on the port:

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

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

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

d. Select the appropriate state (Unlocked; Locked,disabled; Unlocked,automaticInService) in the Admin State column for the port being tested.

e. Click **Apply**.

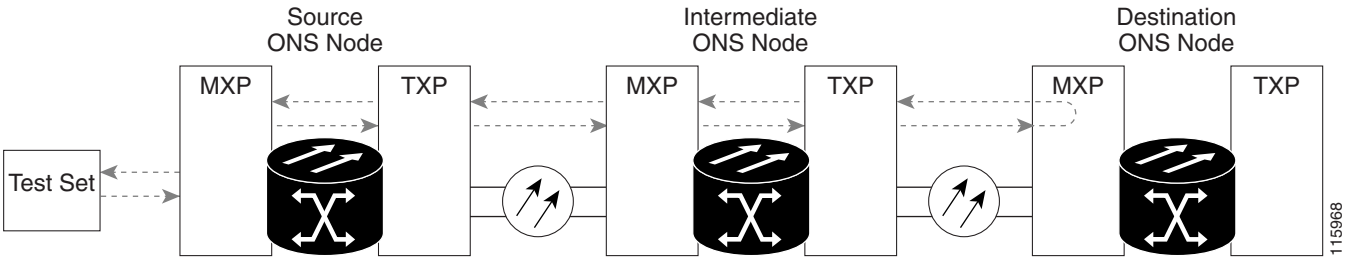
f. Click **Yes** in the confirmation dialog box.

Step 6 Complete the "Perform a Facility (Line) Loopback on a Destination-Node MXP/TXP/FC_MR-4 Port" procedure on page 1-88.

1.5.5 Perform a Facility (Line) Loopback on a Destination-Node MXP/TXP/FC_MR-4 Port

You perform a facility (line) loopback test at the destination port to determine whether this local port is the source of circuit trouble. The example in Figure 1-38 shows a facility loopback being performed on an MXP/TXP/FC_MR-4 port.

Figure 1-38 Facility (Line) Loopback on a Destination-Node MXP/TXP/FC_MR-4 Port



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

Complete the "Create the Facility (Line) Loopback on a Destination-Node MXP/TXP/FC_MR-4 Port" procedure on page 1-89.

Create the Facility (Line) Loopback on a Destination-Node MXP/TXP/FC_MR-4 Port

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

Note For instructions to use the test-set equipment, consult the manufacturer.

a. If you just completed the "Perform a Terminal (Inward) Loopback on Intermediate-Node MXP/TXP/FC_MR-4 Ports" procedure on page 1-86, 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 transmit and receive terminals of the optical test set to the port you are testing. Both transmit and receive connect to the same port.

Step 2 Adjust the test set accordingly.

Step 3 Create the facility (line) loopback on the destination port being tested:

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

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

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

d. Select **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/FC_MR-4 Facility (Line) Loopback Circuit" procedure on page 1-89.

Test and Clear the MXP/TXP/FC_MR-4 Facility (Line) Loopback Circuit

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

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

Step 3 If the test set indicates a good circuit, no further testing is necessary with the facility loopback. Clear the facility (line) loopback from the port:

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

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

c. Choose the appropriate state (Unlocked; Locked,disabled; Unlocked,automaticInService) from the Admin State column for the port being tested.

d. Click **Apply**.

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

Step 4 Complete the "Test the MXP/TXP/FC_MR-4 Card" procedure on page 1-90.

Test the MXP/TXP/FC_MR-4 Card

Step 1 Complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the suspected bad card and replace it with a known-good one.

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

Step 3 If the test set indicates a good circuit, the problem was probably the defective card. Return the defective card to Cisco through the RMA process. Log into the Cisco 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 Cisco TAC numbers for your country.

Step 4 Complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the faulty card.

Step 5 Clear the facility (line) loopback on the port:

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

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

c. Choose the appropriate state (Unlocked; Locked,disabled; Unlocked,automaticInService) from the Admin State column for the port being tested.

d. Click **Apply**.

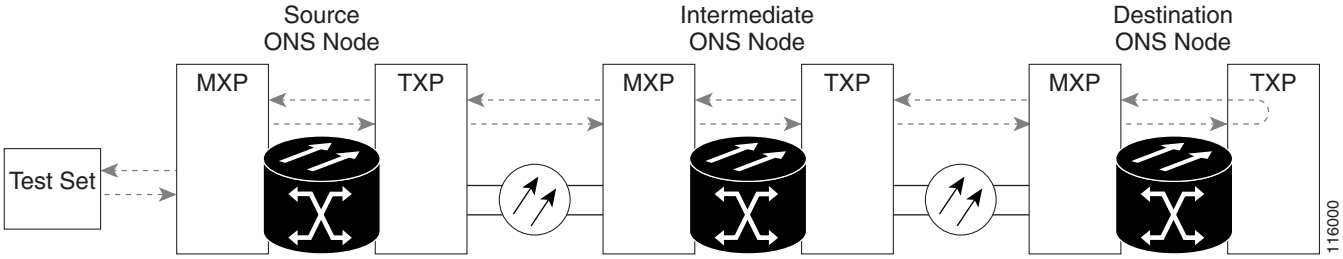
e. Click **Yes** in the confirmation dialog box.

Step 6 Complete the "Perform a Terminal Loopback on a Destination-Node MXP/TXP/FC_MR-4 Port" procedure on page 1-90.

1.5.6 Perform a Terminal Loopback on a Destination-Node MXP/TXP/FC_MR-4 Port

The terminal loopback at the destination-node port is the final local hardware error elimination in the circuit troubleshooting process. If this test is completed successfully, you have verified that the circuit is good up to the destination port. The example in Figure 1-39 shows a terminal loopback on an intermediate-node destination MXP/TXP/FC_MR-4 port.

Figure 1-39 Terminal Loopback on a Destination-Node MXP/TXP/FC_MR-4 port



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

Complete the "Create the Terminal Loopback on a Destination-Node MXP/TXP/FC_MR-4 Port" procedure on page 1-91.

Create the Terminal Loopback on a Destination-Node MXP/TXP/FC_MR-4 Port

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

Note For instructions to use the test-set equipment, consult the manufacturer.

a. If you just completed the "Perform a Facility (Line) Loopback on a Destination-Node MXP/TXP/FC_MR-4 Port" procedure on page 1-88, 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 transmit and receive terminals of the optical test set to the port you are testing. Both transmit and receive connect to the same port.

Step 2 Adjust the test set accordingly.

Step 3 Confirm that the newly created circuit appears on the Circuits tab list as a two-way circuit.

Note It is normal for the "LP-ENCAP-MISMATCH" condition on page 2-160 or the "LPBKFACILITY (FCMR)" condition on page 2-154 to appear during a loopback setup. The condition clears when you remove the loopback.

Step 4 Create the terminal loopback on the destination port being tested:

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

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

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

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

d. Select **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 5 Complete the "Test and Clear the MXP/TXP/FC_MR-4 Terminal Loopback Circuit" procedure on page 1-92.

Test and Clear the MXP/TXP/FC_MR-4 Terminal Loopback Circuit

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

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

Step 3 If the test set indicates a good circuit, 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** tab.

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

d. Select the appropriate state (Unlocked; Locked,disabled; Unlocked,automaticInService) in 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 a faulty circuit, the problem might be a faulty card.

Step 5 Complete the "Test the MXP/TXP/FC_MR-4 Card" procedure on page 1-92.

Test the MXP/TXP/FC_MR-4 Card

Step 1 Complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the suspected bad card and replace it with a known-good card.

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

Step 3 If the test set indicates a good circuit, the problem was probably the defective card. Return the defective card to Cisco through the RMA process. Log into the Cisco 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 Cisco TAC numbers for your country.

Step 4 Complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the defective card.

Step 5 Clear the terminal loopback on the port:

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

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

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

d. Select the appropriate state (Unlocked; Locked,disabled; Unlocked,automaticInService) in the Admin State column for the port being tested.

e. Click **Apply**.

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

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

1.6 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 performance monitoring and threshold crossing alerts (TCAs).

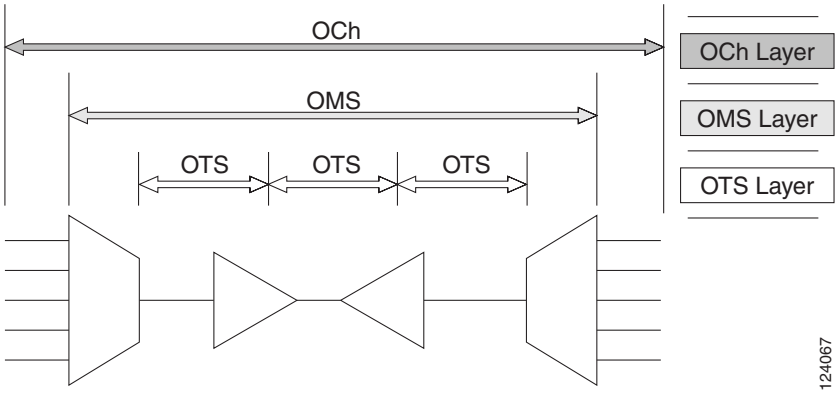
1.6.1 ITU-T G.709 Monitoring in Optical Transport Networks

ITU-T Recommendation G.709 is part of a suite of recommendations covering the full functionality of an OTN. ITU-T G.709 takes single-wavelength SDH technology a step further by enabling transparent optical wavelength-based networks. It adds extra overhead to existing SDH, Ethernet, or asynchronous transfer mode (ATM) bit streams for performance management and improvement.

ITU-T G.709 adds the operations, administration, maintenance, and provisioning (OAM&P) functionality of SONET/SDH to DWDM optical networks.

Like traditional SDH networks, ITU-T G.709 optical networks have a layered design (Figure 1-40). This structure enables localized monitoring that helps you isolate and troubleshoot network problems.

Figure 1-40 Optical Transport Network Layers



1.6.2 Optical Channel Layer

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

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

1.6.3 Optical Multiplex Section Layer

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

1.6.4 Optical Transmission Section Layer

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

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

1.6.5 Performance Monitoring Counters and Threshold Crossing Alerts

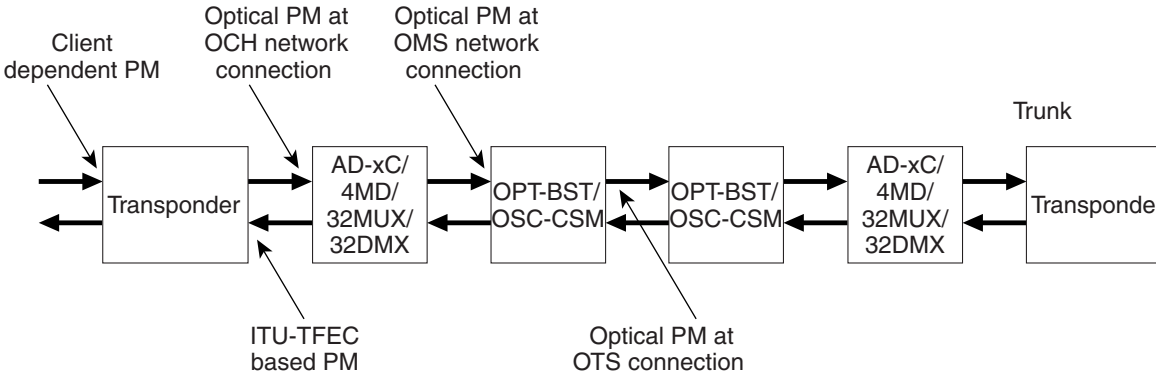
Performance monitoring (PM) counters and TCAs can be used for identifying trouble and troubleshooting problems in ITU-T G.709 optical transport networks. ITU-T Recommendation M.2401 recommends that the following PM parameters be monitored at the ODUk Layer:

- SES (severely errored seconds)—A one-second period which 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 performance monitoring count parameters are associated with different read points in a network. Figure 1-41 illustrates the performance monitoring read points that are useful in identifying DWDM circuit points of failure. Chapter 5, "Performance Monitoring," lists all PM parameters and provides block diagrams of signal entry points, exit points and interconnections between the individual

circuit cards. Consult these specifications to determine which performance monitoring parameters are associated with the system points you want to monitor or provision with CTC or TL1. The monitoring points can vary according to your configuration.

Figure 1-41 Performance Monitoring Points on ONS DWDM



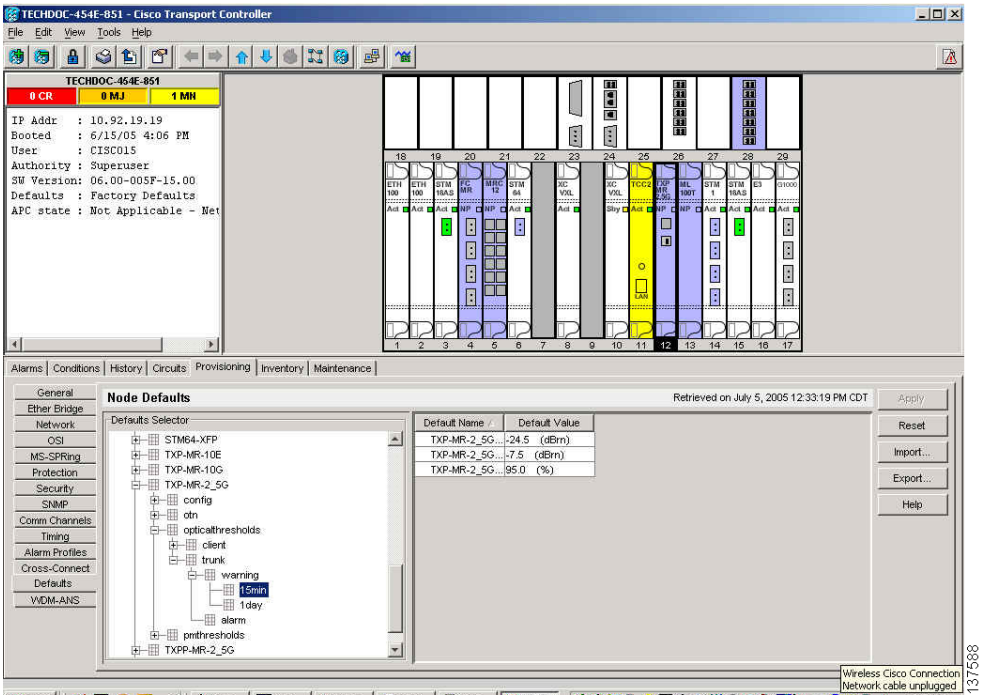
TCAs are used to monitor performance through the management interface by indicating whether preset thresholds have been crossed, or whether a transmission (such as a laser transmission) is degraded. TCAs are not associated with severity levels. They are usually associated with rate, counter, and percentage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

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

Set Node Default BBE or SES Card Thresholds

Step 1 In node view, click the **Provisioning > Defaults** tabs (Figure 1-42).

Figure 1-42 Set Default BBE/SES Card Thresholds



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

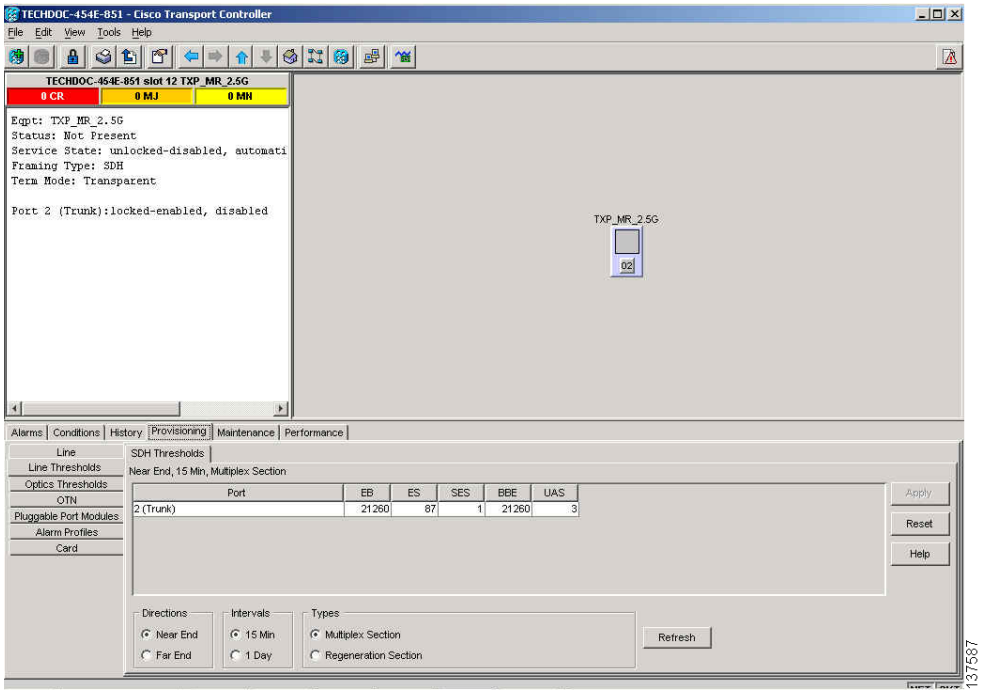
Complete the following procedure to provision BBE or SES PM thresholds in CTC for an individual TXP card.

Provision Individual Card BBE or SES Thresholds in CTC

Step 1 In node view, double-click the TXP_MR_2.5G card.
(In this example, other transponder and muxponder cards are also applicable, such as TXP_MR_10G, TXPP_MR_2.5G, and MXP_2.5G_10G.)

Step 2 Click the **Provisioning > OTN > G.709 Thresholds** tabs (Figure 1-43).

Figure 1-43 Provision Card BBE/SES Thresholds



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

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

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

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

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

Provision Card PM Thresholds Using TL1

Step 1 Open a TL1 command line.

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

`set-th-{och|clnt}::aid:ctag::montype,thlev,,,[tmper];`

Where:

- The modifier is och, as applicable to the trunk port.
- Montype can be one of the following items:
  - BBE-PM
  - SES-PM
  - LBCL-MAX
- The parameter thlev is optional and indicates a threshold count value, which is the number of errors that must be exceeded before the threshold is crossed.

- 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.

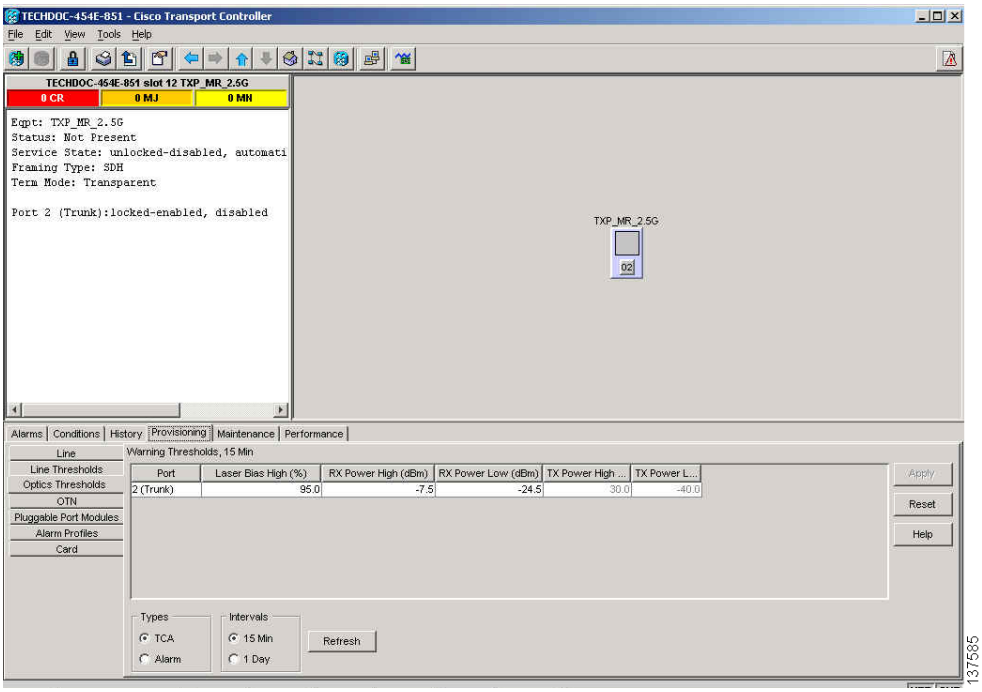
Note For a list of TL1 commands, refer to the *Cisco ONS 15454 TL1 Command Guide*.

Complete the following procedure to provision TCA thresholds in CTC.

Provision Optical TCA Thresholds

Step 1 In node view, click the **Provisioning > Optics Thresholds** tabs (Figure 1-44).

Figure 1-44 Provision Optical TCA Thresholds



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

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

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

1.6.6 Forward Error Correction

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

- BIT-EC—Bit errors corrected (BIT-EC) indicates the number of bit errors corrected in the DWDM trunk line during the PM time interval.
- UNC-WORDS—The number of uncorrectable words detected in the DWDM trunk line during the PM time interval.

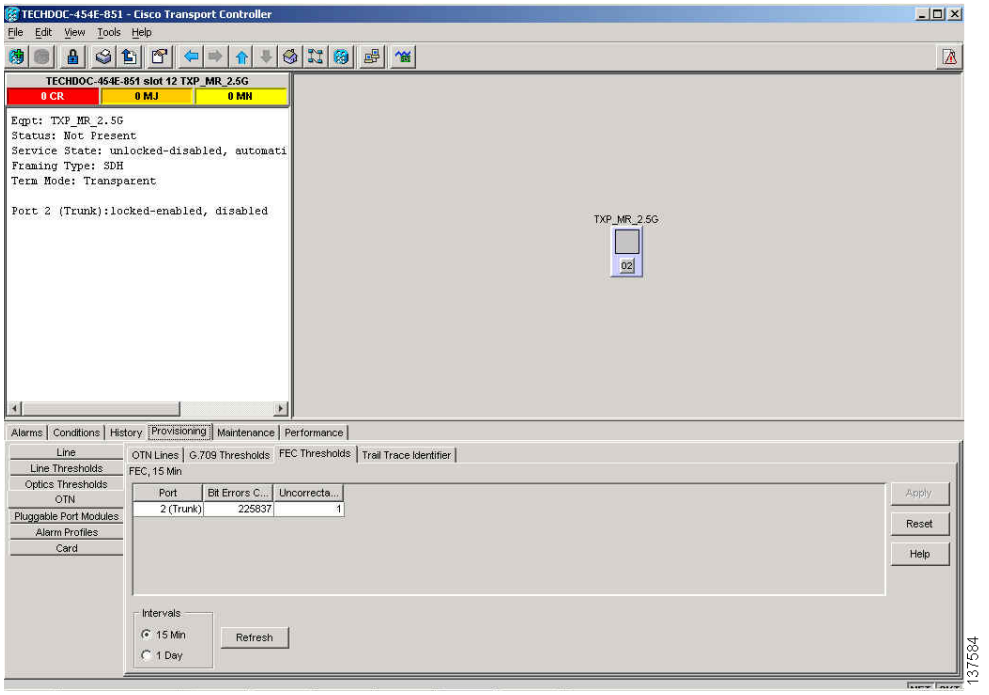
Complete the following procedure to provision BIT-EC and UNC-WORDS PM parameters for FEC.

Provision Card FEC Thresholds

Step 1 In node view, double-click the TXP_MR_2.5G card to open the card view.
(In this example, other transponder and muxponder cards are also applicable, such as TXP_MR_10G, TXPP_MR_2.5G, and MXP_2.5G_10G.)

Step 2 Click the **Provisioning > OTN > FEC Thresholds** tabs (Figure 1-45).

Figure 1-45 Provision Card FEC Thresholds



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

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

1.6.7 Sample Trouble Resolutions

Some sample trouble resolutions using performance monitoring and TCAs for isolating points of degrade are provided below.

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

Possible Cause The transponder input power is out of range.

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

Possible Cause There are dirty trunk connectors on the transponder.

Recommended Action Check the connector on the trunk port.

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

Recommended Action Check the patch cord on the transponder DWDM port.

Possible Cause There are dirty client connectors on the channel add-drop (ADxC) transmit port or the demultiplexer has crossed the near-end TCA.

Recommended Action Check the connector on the OCH port of the ADxC.

Possible Cause There are dirty client connectors on the ADxC receive port or the multiplexer has crossed the far-end TCA point.

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

Symptom There is a BBE TCA on all transponders connected to a band add-drop card (ADxB).

Possible Cause The transponder input power is out of range.

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

Possible Cause There is a dirty connector on the 4MD port.

Recommended Action Check the connector on the drop port of the ADxB.

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

Recommended Action Check the connector on the drop port of the 4MD.

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

Recommended Action Check the patch cord on the 4MD or AD1B.

Possible Cause There is a degraded patch cord between the ADxB and the 4MD.

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

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

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

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

Symptom You have an LBC TCA on a single transponder.

Possible Cause The laser of the transponder is degrading.

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

1.7 Using CTC Diagnostics

CTC provides diagnostics for the following functions:

- Verification of proper card ASICS function
- Verification of standby card operation
- Verification of proper card LED operation
- Notification of problems detected via alarms
- A downloaded, machine-readable diagnostic file to be used by Cisco TAC

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 window. Other diagnostic functions—verifying card LED function and downloading diagnostic files for technical support—are available in the node view Maintenance > Diagnostic tab. The user-accessible diagnostic features are described in the following paragraphs.

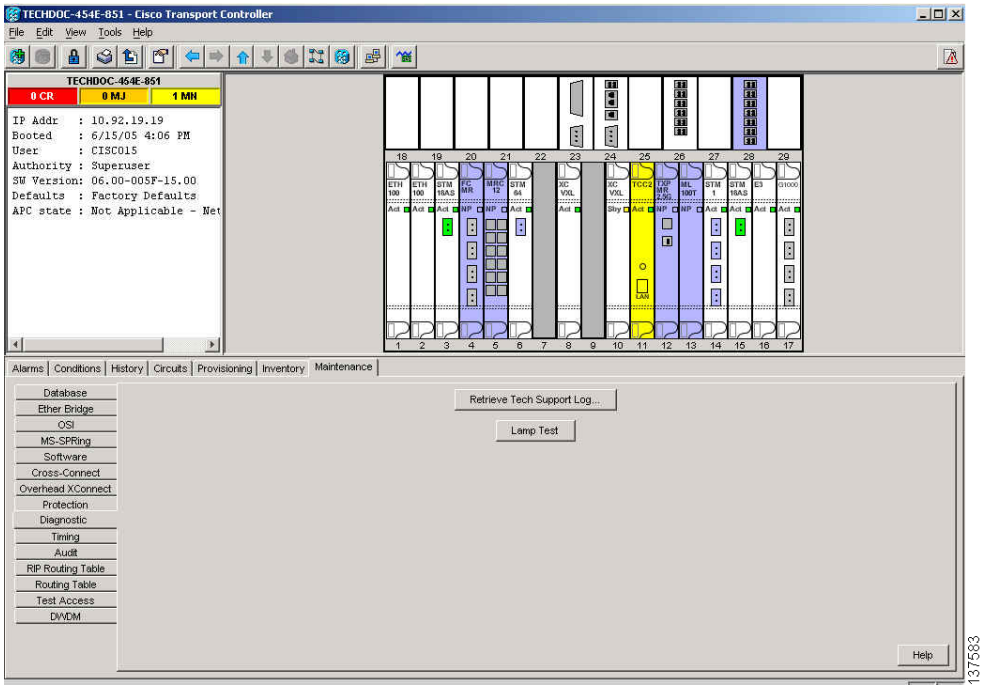
1.7.1 Card LED Lamp Tests

A card LED lamp test determines whether card-level indication LEDs are operational. This diagnostic test is run as part of the initial ONS 15454 SDH turnup, 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 General Card LED Operation

Step 1 In node view, click the **Maintenance > Diagnostic** tab (Figure 1-46).

Figure 1-46 CTC Node View Diagnostic Window



Step 2 Click **Lamp Test**.

Step 3 Watch to make sure all the port LEDs illuminate simultaneously for several seconds.

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

With the exceptions previously described, if an STM-N or electrical port LED does not light up, the LED is faulty. Return the defective card to Cisco through the RMA process. Log into the Cisco 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 Cisco TAC numbers for your country.

Verify G-Series Ethernet or FC_MR-4-4 Card LED Operation

Note G-Series and FC_MR-4 card-level LEDs illuminate during a lamp test, but the port-level LEDs do not.

Step 1 Complete the "Verify General Card LED Operation" procedure on page 1-101 to verify that card-level LEDs are operational.

Step 2 Use the following list of guidelines to physically test whether the G-Series Ethernet port LEDs are operating correctly. If the LED appears as described when the listed state is occurring for the port, the LED is considered to be functioning correctly. Consult the following guidelines:

- Clear port LED: Should only occur if there is a loss of receive link (such as a disconnected link or unplugged Ethernet Gigabit Interface Converters [GBICs]). An LOS alarm could be present on the port.

- Amber port LED: Should only occur if a port is disabled but the link is connected; or if the port is enabled and the link is connected, but a transport failure is present. A TPTFAIL alarm can be present on the port.
- Green port LED: Should occur if the port is enabled and has no errors against it or traffic in it; can also occur if the port is enabled, has no errors, and is running traffic proportionate to the blink rate. No traffic-affecting port alarms should be present.

Step 3 If you are unable to determine the port state, log into the Cisco 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 Cisco TAC numbers for your country.

Verify E-Series and ML-Series Ethernet Card LED Operation

Note E-Series and ML-Series card-level LEDs illuminate during a lamp test, but the port-level LEDs do not.

Note For information about the ML-Series card, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.*

Step 1 Complete the "Verify General Card LED Operation" procedure on page 1-101 to verify that card-level LEDs are operational.

Step 2 Use the following list of guidelines to physically test whether the single E-Series or ML-Series Ethernet port LED is operating correctly. If the LED appears as described when the listed state is occurring for the port, the LED is considered to be functioning correctly.

- Clear port LED: Should only occur is there is a loss of receive link (such as a disconnected link or unplugged GBIC), or if traffic is flowing in one direction (either transmit or receive). A CARLOSS alarm could be present on the port.
- Amber port LED: Should only occur if the link is connected and the physical port is transmitting and receiving traffic.
- Green port LED: Should occur if the link is up and no traffic is flowing on the port.

Step 3 If you are unable to determine the port state, log into the Cisco 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 Cisco TAC numbers for your country.

1.7.2 Retrieve Diagnostics File Button

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

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

Off-Load the Diagnostics File

Step 1 In the node view, click the **Maintenance > Diagnostic** tab (Figure 1-46).

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

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

Step 4 Enter a name in the File Name field.

You do not have to give the archive file a particular extension. It is readable in any application that supports text files, such as WordPad, Microsoft Word (imported), etc.

Step 5 Click **Save**.

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

Step 6 Click **OK**.

1.8 Restoring the Database and Default Settings

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

1.8.1 Restore the Node Database

Symptom One or more nodes does not function properly or has incorrect data.

Possible Cause Incorrect or corrupted node database.

Recommended Action Restore the database using the procedure in the "Maintain the Node" chapter of the *Cisco ONS 15454 SDH Procedure Guide*.

1.9 PC Connectivity Troubleshooting

This section contains information about system minimum requirements, supported platforms, browsers, and JREs for R6.0, and troubleshooting procedures for PC and network connectivity to the ONS 15454 SDH.

1.9.1 PC System Minimum Requirements

Workstations running CTC R6.0 for the ONS products on Windows platforms need to have the following minimum requirements:

- Pentium III or higher processor
- Processor speed of at least 700 MHz
- 256 MB or more of RAM
- 50 MB or more of available hard disk space
- 20 GB or larger hard drive

1.9.2 Sun System Minimum Requirements

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

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

1.9.3 Supported Platforms, Browsers, and JREs

Software R6.0 CTC supports the following platforms:

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

Software R6.0 CTC supports the following browsers and JREs:

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

Note You can obtain browsers at the following URLs:
Netscape: http://browser.netscape.com/
Internet Explorer: http://www.microsoft.com
Mozilla: http://www.mozilla.org/

Note The required JRE version is JRE 1.4.2.

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

1.9.4 Unsupported Platforms and Browsers

Software R6.0 does not support the following platforms:

- Windows 95
- Solaris 2.5
- Solaris 2.6

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

- Netscape 4.73 for Windows.
- Netscape 4.76 on Solaris is not supported.
- Netscape 7 on Solaris 8 or 9 is only supported with JRE 1.4.2

1.9.5 Unable to Verify the IP Configuration of Your PC

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

Possible Cause The IP address was typed incorrectly.

Recommended Action Verify that the IP address used to ping the PC matches the IP address shown in the Windows IP Configuration information retrieved from the system. See "Verify the IP Configuration of Your PC" procedure on page 1-106.

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

Recommended Action Verify the IP configuration of your PC. See the "Verify the IP Configuration of Your PC" procedure on page 1-106. If this procedure is unsuccessful, contact your Network Administrator for instructions to correct the IP configuration of your PC.

Verify the IP Configuration of Your PC

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

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

Step 3 At the prompt in the DOS window, type one of the following appropriate commands:

- For Windows 98, NT, 2000, and XP, type **ipconfig** and press the **Enter** key.

Note The **winipcfg** command only returns IP configuration information if you are on a network.

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

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

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

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

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

1.9.6 Browser Login Does Not Launch Java

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

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

Recommended Action Reconfigure the PC operating system java plug-in control panel and the browser settings. See the "Reconfigure the PC Operating System Java Plug-in Control Panel" procedure on page 1-107 and the "Reconfigure the Browser" procedure on page 1-107.

Reconfigure the PC Operating System Java Plug-in Control Panel

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

Step 2 If the **Java Plug-in Control Panel** does not appear, the JRE might not be installed on your PC. Complete the following steps:

a. Run the Cisco ONS 15454 SDH software CD.

b. Open the *CD drive*:**Windows\JRE** folder.

c. Double-click the **j2re-1_4_2-win** icon to run the JRE installation wizard.

d. Follow the JRE installation wizard steps.

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

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

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

Step 6 From the Java Run Time Environment menu, select **JRE 1.4 in C:\ProgramFiles\JavaSoft\JRE\1.4.2**.

Step 7 Click **Apply**.

Step 8 Close the Java Plug-in Control Panel window.

Reconfigure the Browser

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

Step 2 If you are using Netscape Navigator:

a. On the Netscape Navigator menu bar, click **Edit > Preferences**.

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. On the Netscape Navigator menu bar, click **Edit > Preferences**.

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

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

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

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

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

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

Step 3 If you are using Internet Explorer:

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

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

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

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

Step 4 Temporarily disable any virus-scanning software on the computer. See the "1.10.3 Browser Stalls When Downloading CTC JAR Files From TCC2/TCC2P Card" section on page 1-112.

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 on to the ONS 15454 SDH.

1.9.7 Unable to Verify the NIC Connection on Your PC

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

Possible Cause The c cable is not plugged in properly.

Recommended Action Confirm 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 Category-5 cable is damaged.

Recommended Action Ensure that the cable is in good condition. If in doubt, use a known-good cable. Often, cabling is damaged due to pulling or bending.

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

Recommended Action If connecting an ONS 15454 SDH directly to your laptop/PC or a router, use a straight-through Category-5 cable. When connecting the ONS 15454 SDH to a hub or a LAN switch, use a crossover Category-5 cable. For details on the types of Category-5 cables, see the "Crimp Replacement LAN Cables" procedure on page 1-131.

Possible Cause The NIC is improperly inserted or installed.

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

Possible Cause The NIC is faulty.

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

1.9.8 Verify PC Connection to the ONS 15454 SDH (ping)

Symptom The TCP/IP connection was established and then lost, and a DISCONNECTED transient alarm appears on CTC.

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

Recommended Action Use a standard ping command to verify the TCP/IP connection between the PC and the ONS 15454 SDH TCC2/TCC2P card. A ping command will work if the PC connects directly to the TCC2/TCC2P card or uses a LAN to access the TCC2/TCC2P card. See the "Ping the ONS 15454 SDH" procedure on page 1-109.

Ping the ONS 15454 SDH

Step 1 Open the command prompt:

a. If you are using a Microsoft Windows operating system, from the Start Menu choose **Run**, type **command prompt** 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 type:

```
ping ONS-15454-SDH-IP-address
```

For example:

```
ping 192.1.0.2
```

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

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

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

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

1.9.9 The IP Address of the Node is Unknown

Symptom The IP address of the node is unknown and you are unable to log in.

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

Recommended Action Leave one TCC2/TCC2P card in the shelf. Connect a PC directly to the remaining TCC2/TCC2P card and perform a hardware reset of the card. The TCC2/TCC2P card will transmit the IP address after the reset to enable you to capture the IP address for login. See the "Retrieve Unknown Node IP Address" procedure on page 1-110.

Retrieve Unknown Node IP Address

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

Step 2 Start the Sniffer application on your PC.

Step 3 Perform a hardware reset by removing and reinserting (reseating) the active TCC2/TCC2P card.

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

1.10 CTC Operation Troubleshooting

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

1.10.1 Unable to Launch CTC Help After Removing Netscape

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

Possible Cause Loss of association between browser and Help files.

Recommended Action When the CTC software and Netscape are installed, the Help files are associated with Netscape by default. When you remove Netscape, the Help files are not automatically associated with Internet Explorer as the default browser. Reset Internet Explorer as

the default browser so that CTC will associate the Help files to the correct browser. See the "Reset Internet Explorer as the Default Browser for CTC" procedure on page 1-111 to associate the CTC Help files to the correct browser.

Reset Internet Explorer as the Default Browser for CTC

Step 1 Open the Internet Explorer browser.

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

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

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

Step 5 Click **OK**.

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

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

1.10.2 Unable to Change Node View to Network View

Symptom When activating a large, multinode MS-SPRing, some of the nodes appear grayed out. Logging into the new CTC, you are unable to change node view to network view on any and all 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 MS-SPRing requires more memory for the GUI environment variables.

Recommended Action Set the system or user CTC_HEAP environment variable to increase the memory limits. See the "Set the CTC_HEAP and CTC_MAX_PERM_SIZE_HEAP Environment Variables for Windows" procedure on page 1-111 or the "Set the CTC_HEAP and CTC_MAX_PERM_SIZE_HEAP Environment Variables for Solaris" procedure on page 1-112 to enable the CTC_HEAP variable change.

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

Set the CTC_HEAP and CTC_MAX_PERM_SIZE_HEAP Environment Variables for Windows

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

Step 1 Close all open CTC sessions and browser windows.

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

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

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

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

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

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

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

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

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

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

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

Set the CTC_HEAP and CTC_MAX_PERM_SIZE_HEAP Environment Variables for Solaris

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

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

Example

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

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

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

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

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

Recommended Action Disable the VirusScan Download Scan feature. See the "Disable the VirusScan Download Scan" procedure on page 1-112.

Disable the VirusScan Download Scan

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

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

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

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

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

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

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

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

Step 9 Close the McAfee VirusScan window.

1.10.4 CTC Does Not Launch

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

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

Recommended Action Redirect the Netscape cache to a valid directory. See the "Redirect the Netscape Cache to a Valid Directory" procedure on page 1-113.

Redirect the Netscape Cache to a Valid Directory

Step 1 Launch Netscape.

Step 2 From the **Edit** menu, choose **Preferences**.

Step 3 In the Category column on the left side, expand the **Advanced** category and choose the **Cache** tab.

Step 4 Change your disk cache folder to point to the cache file location.

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

1.10.5 Slow CTC Operation or Login Problems

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

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

Table 1-3 Slow CTC Operation or Login Problems

Possible Problem	Solution
The CTC cache file might be corrupted or might need to be replaced.	Delete the CTC cache file. This operation forces the ONS 15454 SDH to download a new set of JAR files to your computer hard drive. See the "Delete the CTC Cache File Automatically" procedure on page 1-114 or the "Delete the CTC Cache File Manually" procedure on page 1-115.
Insufficient heap memory allocation.	Increase the heap size if you are using CTC to manage more than 50 nodes concurrently. See the "Set the CTC_HEAP and CTC_MAX_PERM_SIZE_HEAP Environment Variables for Windows" procedure on page 1-111 or the "Set the CTC_HEAP and CTC_MAX_PERM_SIZE_HEAP Environment Variables for Solaris" procedure on page 1-112. **Note** To avoid network performance issues, Cisco recommends managing a maximum of 50 nodes concurrently with CTC. To manage more than 50 nodes, Cisco recommends using Cisco Transport Manager (CTM). Cisco does not recommend running multiple CTC sessions when managing two or more large networks.

Delete the CTC Cache File Automatically

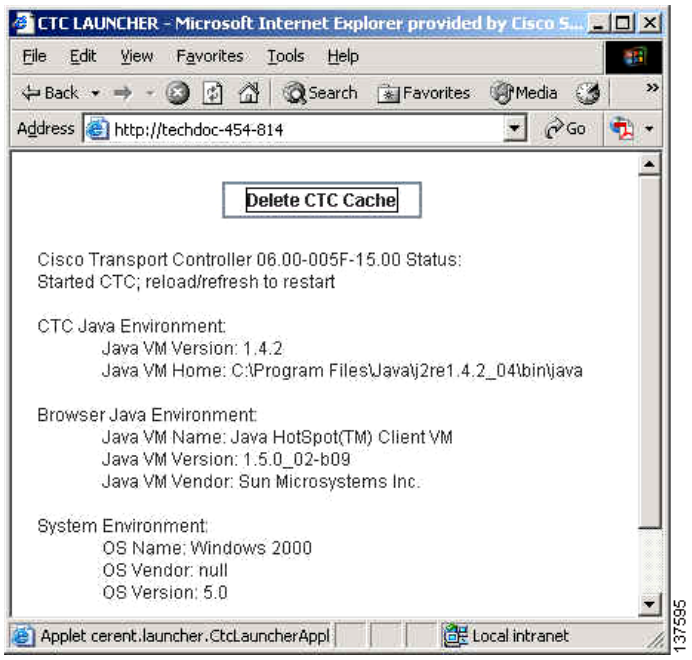
Caution All running sessions of CTC must be closed before deleting the CTC cache. Deleting CTC cache can cause any CTC session running on this node to behave in an unexpected manner.

Step 1 Enter an ONS 15454 SDH 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** on the initial browser window to clear the CTC cache. Figure 1-47 shows the Delete CTC Cache window.

Figure 1-47 Deleting the CTC Cache



Delete the CTC Cache File Manually

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

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

Step 2 Enter **ctc*.jar** or **cms*.jar** in the Search for files or folders named field on the Search Results dialog box and click **Search Now**.

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

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

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

1.10.6 Node Icon is Gray on CTC Network View

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

Possible Cause Different CTC releases not recognizing each other.

Recommended Action Correct the core version build as described in the "1.10.9 Different CTC Releases Do Not Recognize Each Other" section on page 1-118.

Possible Cause A username/password mismatch.

Recommended Action Correct the username and password as described in the "1.10.10 Username or Password Do Not Match" section on page 1-119.

Possible Cause No IP connectivity between nodes.

Recommended Action Usually accompanied by Ethernet-specific alarms. Verify the Ethernet connections as described in the "1.10.15 Ethernet Connections" section on page 1-121.

Possible Cause A lost DCC connection.

Recommended Action Usually accompanied by an "EOC" alarm on page 2-76. Clear the EOC alarm and verify the DCC connection as described in the "Clear the EOC Alarm" procedure on page 2-77.

1.10.7 CTC Cannot Launch Due to Applet Security Restrictions

Symptom The error message "Unable to launch CTC due to applet security restrictions" appears after you enter the IP address in the browser window.

Possible Cause You are logging into a node running CTC Software R4.0 or earlier. Releases before R4.1 require a modification to the java.policy file so that CTC JAR files can be downloaded to the computer. The modified java.policy file might not exist on the computer.

Recommended Action Install the software CD for the release of the node you are logging into. Run the CTC Setup Wizard (double-click Setup.exe). Choose Custom installation, then choose the Java Policy option. For additional information, refer to the CTC installation information in the "Connect to the PC and Log Into the GUI" chapter in the *Cisco ONS 15454 SDH Procedure Guide*. If the software CD is not available, you must manually edit the java.policy file on your computer. See the "Manually Edit the java.policy File" procedure on page 1-116.

Manually Edit the java.policy File

Step 1 Search your computer for this file and open it with a text editor (Notepad or Wordpad).

Step 2 Verify that the end of this file has the following lines:

```
    // Insert this into the system-wide or a per-user java.policy file.
// DO NOT OVERWRITE THE SYSTEM-WIDE POLICY FILE--ADD THESE LINES!

grant codeBase "http://*/fs/LAUNCHER.jar" {
```

```
permission java.security.AllPermission;
    };
```

Step 3 If these five lines are not in the file, enter them manually.

Step 4 Save the file and restart Netscape.

CTC should now start correctly.

Step 5 If the error message is still reported, save the java.policy file as (**.java.policy**). On Win98/2000/XP PCs, save the file to the C:\Windows folder. On WinNT4.0 PCs, save the file to all of the user folders on that PC, for example, C:\Winnt\profiles\joeuser.

1.10.8 Java Runtime Environment Incompatible

Symptom The CTC application does not run properly.

Possible Cause The compatible Java 2 JRE is not installed.

Recommended Action The JRE contains the Java virtual machine, runtime class libraries, and Java application launcher that are necessary to run programs written in the Java programming language. The ONS 15454 SDH CTC is a Java application. A Java application, unlike an applet, cannot rely completely on a web browser for installation and runtime services. When you run an application written in the Java programming language, you need the correct JRE installed. The correct JRE for each CTC software release is included on the Cisco ONS 15454 SDH software CD and on the Cisco ONS 15454 SDH documentation CD. See the "Launch CTC to Correct the Core Version Build" procedure on page 1-118. If you are running multiple CTC software releases on a network, the JRE installed on the computer must be compatible with the different software releases. Table 1-4 shows JRE compatibility with ONS 15454 SDH software releases.

Table 1-4 JRE Compatibility

ONS Software Release	JRE 1.2.2 Compatible	JRE 1.3 Compatible	JRE 1.4 Compatible
ONS 15454 SDH Release 3.3	Yes	Yes	No
ONS 15454 SDH Release 3.4	No	Yes	No
ONS 15454 SDH Release 4.0[1]	No	Yes	No
ONS 15454 SDH Release 4.1	No	Yes	No
ONS 15454 SDH Release 4.5	No	Yes	No
ONS 15454 SDH Release 4.6	No	Yes	Yes
ONS 15454 SDH Release 4.7	No	Yes	Yes
ONS 15454 SDH Release 5.0	No	Yes	Yes
ONS 15454 SDH Release 6.0	No	No	Yes

1. Software R4.0 will notify you if an older version JRE is running on your PC or UNIX workstation.

Launch CTC to Correct the Core Version Build

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

Step 2 Start the browser.

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

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

1.10.9 Different CTC Releases Do Not Recognize Each Other

Symptom This situation is often accompanied by the INCOMPATIBLE-SW transient alarm.

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

Recommended Action This occurs when the TCC2/TCC2P 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. See the "Launch CTC to Correct the Core Version Build" procedure on page 1-118.

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

Launch CTC to Correct the Core Version Build

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

Step 2 Start the browser.

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

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

1.10.10 Username or Password Do Not Match

Symptom A mismatch often occurs concurrently with a NOT-AUTHENTICATED transient alarm.

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

Recommended Action All ONS nodes must have the same username and password created to display every ONS node in the network. You can also be locked out of certain ONS nodes on a network if your username and password were not created on those specific ONS nodes. For initial login to the ONS 15454 SDH, enter the CISCO15 user name in capital letters and click **Login** and use the password "otbu+1," which is case-sensitive. See the "Verify Correct Username and Password" procedure on page 1-119. If the node has been configured for Radius authentication (new in R6.0), 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" chapter in the *Cisco ONS 15454 SDH Reference Manual*.

Verify Correct Username and Password

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

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

Step 3 Contact Cisco Technical Support to have them enter your system and create a new user name and password. Log into the Cisco 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 Cisco TAC numbers for your country.

1.10.11 No IP Connectivity Exists Between Nodes

Symptom The nodes have a gray icon and is usually accompanied by alarms.

Possible Cause A lost Ethernet connection.

Recommended Action Usually accompanied by Ethernet-specific alarms. Verify the Ethernet connections as described in the "1.10.15 Ethernet Connections" section on page 1-121.

1.10.12 DCC Connection Lost

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

Possible Cause A lost DCC connection.

Recommended Action Usually accompanied by an EOC alarm. Clear the EOC alarm and verify the DCC connection as described in the "2.7.73 EOC" section on page 2-76.

1.10.13 "Path in Use Error" When Creating a Circuit

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

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

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

1.10.14 Calculate and Design IP Subnets

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

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

Recommended Action Cisco provides a free online tool to calculate and design IP subnets. Go to http://www.cisco.com/pcgi-bin/Support/IpSubnet/home.pl.
For information about ONS 15454 SDH IP capability, refer to the "Management Network Connectivity" chapter in the *Cisco ONS 15454 SDH Reference Manual*.

1.10.15 Ethernet Connections

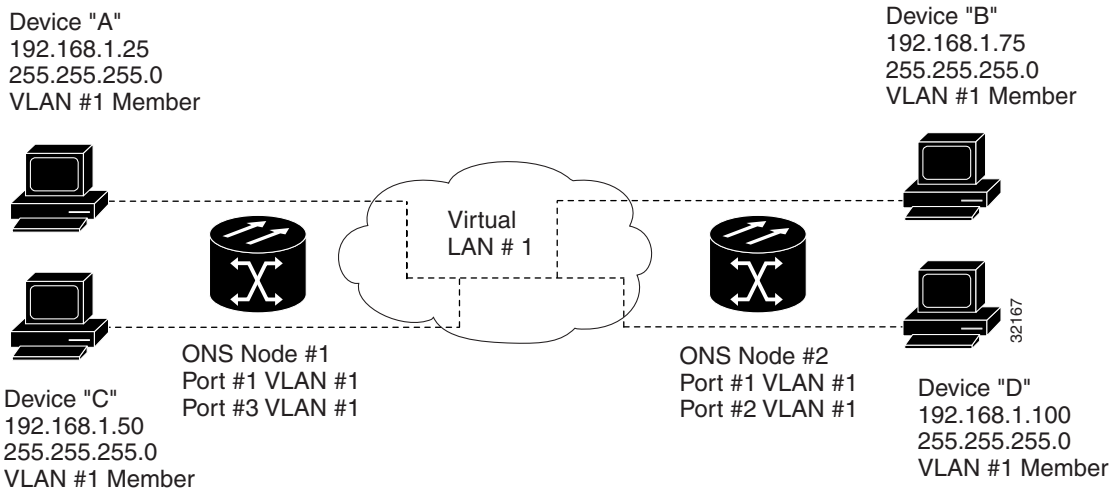
Symptom Ethernet connections appear to be broken or are not working properly.

Possible Cause Improperly seated connections.

Possible Cause Incorrect connections.

Recommended Action You can fix most connectivity problems in an Ethernet network by following a few guidelines. Refer to Figure 1-48 to complete the "Verify Ethernet Connections" procedure on page 1-121.

Figure 1-48 Ethernet Connectivity Reference



Verify Ethernet Connections

Step 1 Verify that the alarm filter is turned OFF.

Step 2 Check for SDH/MXP/TXP/FC_MR-4 alarms on the VC that carries VLAN 1. Clear any alarms by looking them up in Chapter 2, "Alarm Troubleshooting."

Step 3 Check for Ethernet-specific alarms. Clear any raised alarms by looking up that alarm in Chapter 2, "Alarm Troubleshooting."

Step 4 Verify that the ACT LED on the Ethernet card is green.

Step 5 Verify that Ports 1 and 3 on Node 1 and Ports 1 and 2 on Node 2 have green link-integrity LEDs illuminated.

Step 6 If no green link-integrity LED is illuminated for any of these ports, complete the following substeps:

- **a.** Verify physical connectivity between the node and the attached device.
- **b.** Verify that the ports are enabled on the Ethernet cards.
- **c.** Verify that you are using the proper Ethernet cable and that it is wired correctly, or replace the cable with a known-good Ethernet cable.

d. Check the status LED on the Ethernet card faceplate to ensure that the card booted up properly. This LED should be solid green. If necessary, remove and reinsert the card and allow it to reboot.

e. It is possible that the Ethernet port is functioning properly but the link LED itself is broken. Complete the procedures in the "Verify G-Series Ethernet or FC_MR-4-4 Card LED Operation" section on page 1-102 or the "Verify E-Series and ML-Series Ethernet Card LED Operation" section on page 1-103 as appropriate.

Step 7 Verify connectivity between Device A and Device C by pinging between these locally attached devices (see the "Verify PC Connection to the ONS 15454 SDH (ping)" procedure on page 1-109). If the ping is unsuccessful:

a. Verify that Device A and Device C are on the same IP subnet.

b. Open the Ethernet card in CTC card view and click the **Provisioning > VLAN** tabs to verify that both Port 1 and Port 3 on the card are assigned to the same VLAN.

c. If a port is not assigned to the correct VLAN, click that port column in the VLAN row and set the port to Tagged or Untag.

d. Click **Apply**.

Step 8 Repeat Step 7 for Devices B and D.

Step 9 Verify that the Ethernet circuit that carries VLAN No. 1 is provisioned and that Node 1 and Node 2 ports also use VLAN 1.

1.10.16 VLAN Cannot Connect to Network Device from Untag Port

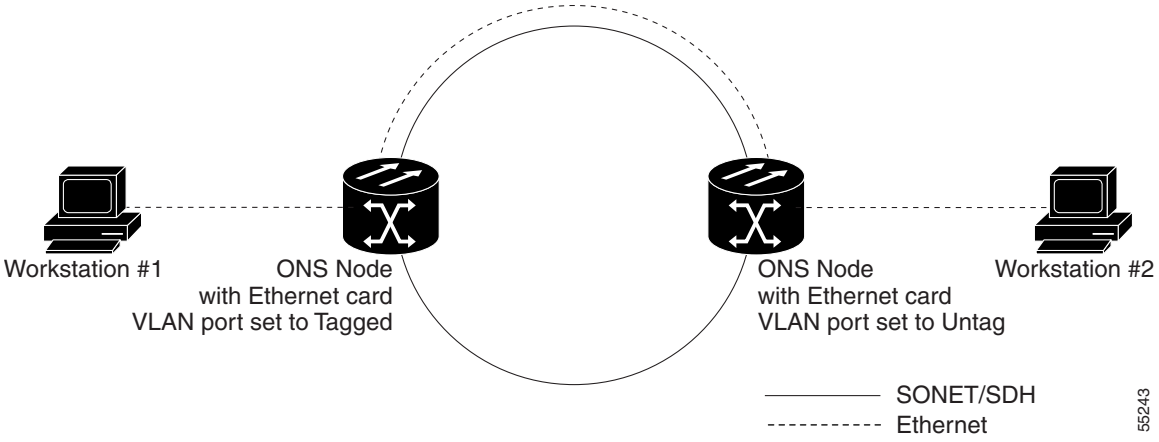
Symptom Networks that have a VLAN with one ONS 15454 SDH Ethernet card port set to Tagged and one ONS 15454 SDH Ethernet card set to Untag might have difficulty implementing Address Resolution Protocol (ARP) for a network device attached to the Untag port (Figure 1-49). There might also be a higher than normal runt packets count at the network device attached to the Untag port. This symptom/limitation also exists when ports within the same card or ports within the same chassis are put on the same VLAN, with a mix of tagged and untagged.

Possible Cause The Tagged ONS 15454 SDH adds the IEEE 802.1Q tag and the Untag ONS 15454 SDH removes the Q-tag without replacing the bytes. The NIC of the network device categorizes the packet as a runt and drops the packet.

Possible Cause Dropped packets can also occur when ARP attempts to match the IP address of the network device attached to the Untag port with the physical MAC address required by the network access layer.

Recommended Action Set both ports in the VLAN to Tagged to stop the stripping of the 4 bytes from the data packet and prevent the NIC card in the network access device from recognizing the packet as a runt and dropping it. Network devices with NIC cards that are not IEEE 802.1Q-compliant accept the tagged packets. Network devices with NIC cards that are not IEEE 802.1Q compliant still drop these tagged packets. You might need to upgrade network devices with NIC cards that are not IEEE 802.1Q compliant to IEEE 802.1Q-compliant NIC cards. You can also set both ports in the VLAN to Untag, but you lose IEEE 802.1Q compliance.

Figure 1-49 VLAN With Ethernet Ports at Tagged and Untag

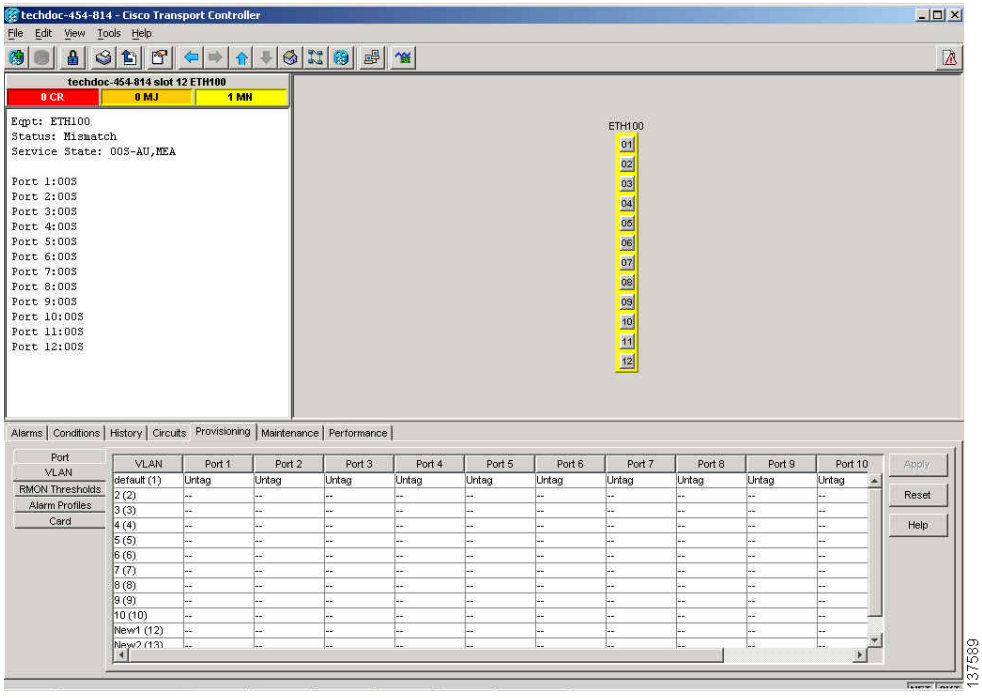


Change VLAN Port Tagged and Untag Settings

Step 1 In node view, double-click the Ethernet card involved in the problem VLAN. The card view appears.

Step 2 Click the **Provisioning > VLAN** tabs (Figure 1-50).

Figure 1-50 Configuring VLAN Membership for Individual Ethernet Ports



Step 3 If the port is set to **Tagged**, continue to look at other cards and their ports in the VLAN until you find the port that is set to **Untag**.

Step 4 At the VLAN port set to **Untag**, click the port and choose **Tagged**.

Note The attached external devices must recognize IEEE 802.1Q VLANs.

Step 5 After each port is in the appropriate VLAN, click **Apply**.

1.11 Circuits and Timing

This section provides solutions to circuit creation and reporting errors, as well as to common timing reference errors and alarms.

1.11.1 STM-N Circuit Transitions to Partial State

Symptom An automatic or manual transition of a circuit from one state to another results in the OOS-PARTIAL status. At least one of the connections in the circuit is in the Unlocked-enabled service state, and at least one other connection in the circuit is in the Locked-enabled,maintenance; Locked-enabled,disabled; or Unlocked-disabled,automaticInService service state.

Possible Cause During a Manual transition, CTC cannot communicate with one of the nodes, or one of the nodes is on a version of software that does not support the new state model.

Recommended Action Repeat the Manual transition operation. If the PARTIAL status persists, determine which node in the circuit is not changing to the desired state. Refer to the "View the State of Circuit Nodes" procedure on page 1-124. Log onto the circuit node that did not change to the desired state and determine the software version.

Note If the node software cannot be upgraded to R6.0, the PARTIAL status condition can be avoided by only using the circuit state(s) supported in the earlier software version.

Possible Cause During an automatic transition, some path-level defects and/or alarms were detected on the circuit.

Possible Cause One end of the circuit is not properly terminated.

Recommended Action Determine which node in the circuit is not changing to the desired state. Refer to the "View the State of Circuit Nodes" procedure on page 1-124. Log onto the circuit node that did not change to the desired state and examine the circuit for path-level defects, improper circuit termination, or alarms. Refer to the "Manage Alarms" chapter in the *Cisco ONS 15454 SDH Procedure Guide* for procedures to clear alarms and change circuit configuration settings. Resolve and clear the defects and/or alarms on the circuit node and verify that the circuit transitions to the desired state.

View the State of Circuit Nodes

Step 1 Click the **Circuits** tab.

Step 2 From the Circuits tab list, select the circuit with the OOS-PARTIAL status condition.

Step 3 Click **Edit**. The Edit Circuit window appears.

Step 4 In the Edit Circuit window, click the **State** tab.

The State tab window lists the Node, CRS End A, CRS End B, and CRS State for each of the nodes in the circuit.

1.11.2 DS3i-N-12 Card Does Not Report MS-AIS From External Equipment

Symptom A DS3i-N-12 card does not report MS-AIS from the external equipment/line side.

Possible Cause The card is functioning as designed.

Recommended Action This card terminates the port signal at the backplane, so VC MS-AIS is not reported from the external equipment/line side. DS3i-N-12 cards have DS3 header monitoring functionality, which allows you to view PMs on the DS3 path. Nevertheless, you cannot view MS-AIS on the VC path. For more information on the PM capabilities of the DS3i-N-12 cards, refer to the "Electrical Cards" chapter in the *Cisco ONS 15454 SDH Reference Manual*.

1.11.3 STM-1 and DCC Limitations

Symptom Limitations to STM-1 and DCC usage.

Possible Cause STM-1 and DCC have limitations for the ONS 15454 SDH.

Recommended Action For an explanation of STM-1 and DCC limitations, refer to the "Turn Up Network" chapter in the *Cisco ONS 15454 SDH Procedure Guide.*

1.11.4 ONS 15454 SDH Switches Timing Reference

Symptom Timing references switch when one or more problems occur.

Possible Cause The optical or 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 Sync Status Messaging (SSM) message is set to Do Not Use for Synchronization (DUS).

Possible Cause The synchronous status messaging (SSM) indicates a Stratum 3 or lower clock quality.

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

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

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

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

1.11.5 Holdover Synchronization Alarm

Symptom The clock is running at a different frequency than normal and the holdover synchronization (HLDOVRSYNC) condition appears.

Possible Cause The last reference input has failed.

Recommended Action The clock is running at the frequency of the last known-good reference input. This alarm is raised when the last reference input fails. See the "HLDOVRSYNC" alarm on page 2-119 for a detailed description of this alarm.

Note The ONS 15454 SDH supports holdover timing per the ITU when provisioned for external (BITS) timing.

1.11.6 Free-Running Synchronization Mode

Symptom The clock is running at a different frequency than normal and the free-running synchronization (FRNGSYNC) condition appears.

Possible Cause No reliable reference input is available.

Recommended Action The clock is using the internal oscillator as its only frequency reference. This occurs when no reliable, prior timing reference is available. See the "FRNGSYNC" condition, page 2-107 for a detailed description of this condition.

1.11.7 Daisy-Chained BITS Not Functioning

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

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

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

1.11.8 Blinking STAT LED after Installing a Card

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

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

Recommended Action The blinking STAT LED indicates that POST diagnostics are being performed. If the LED continues to blink more than 60 seconds, the card has failed the POST diagnostics test and has failed to boot. If the card has truly failed, an EQPT alarm is raised against the slot number with an "Equipment Failure" description. Check the alarm tab for this alarm to appear for the slot where the card was installed. To attempt recovery, remove and reinstall the card and observe the card boot process. If the card fails to boot, replace the card. Complete the "Physically Replace a Traffic Card" procedure on page 2-242.

Caution Removing an active card can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-230 for basic instructions. For detailed information, refer to the "Maintain the Node" chapter in the *Cisco ONS 15454 SDH Procedure Guide*.

1.11.9 Circuits Remain in PARTIAL Status

Symptom Circuits remain in the PARTIAL status.

Possible Cause The MAC address changed.

Recommended Action Repair the circuits. See the "Repair Circuits" procedure on page 1-128.

1.11.9.1 Repair Circuits

Step 1 In node view, click the **Circuits** tab. Note that all circuits listed are PARTIAL.

Step 2 In node view, choose **Repair Circuits** from the **Tools** drop-down list. The Circuit Repair dialog box appears.

Step 3 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 4 The Node MAC Addresses dialog box appears:

a. From the Node drop-down list, choose the name of the node where you replaced the AIE.

b. In the Old MAC Address field, enter the old MAC address.

c. Click **Next**.

Step 5 The Repair Circuits dialog box appears. Read the information in the dialog box and click **Finish**.

Note 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.

When the circuit repair is complete, the Circuits Repaired dialog box appears.

Step 6 Click **OK**.

Step 7 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).

1.12 Fiber and Cabling

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

1.12.1 Bit Errors Appear for a Traffic Card

Symptom A traffic card has multiple bit errors.

Possible Cause Faulty cabling or low optical-line levels.

Recommended Action Bit errors on line (traffic) cards usually originate from cabling problems or low optical-line levels. The errors can be caused by synchronization problems, especially if (pointer justification (PJ) errors are reported. Moving cards into different error-free slots will isolate the cause. Use a test set whenever possible because the cause of the errors could be external cabling, fiber, or external equipment connecting to the ONS 15454 SDH. Troubleshoot cabling problems using the "1.1 Troubleshooting Non-DWDM Circuit Paths with Loopbacks" section on page 1-2. Troubleshoot low optical levels using the "1.12.2 Faulty Fiber-Optic Connections" section on page 1-129.

1.12.2 Faulty Fiber-Optic Connections

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

Possible Cause Faulty fiber-optic connections.

Recommended Action Faulty fiber-optic connections can be the source of SDH alarms and signal errors. See the "Verify Fiber-Optic Connections" procedure on page 1-129.

Possible Cause Faulty Category-5 cables.

Recommended Action Faulty Category-5 cables can be the source of SDH alarms and signal errors. See the "Crimp Replacement LAN Cables" procedure on page 1-131.

Possible Cause Faulty GBICs.

Recommended Action Faulty GBICs can be the source of SDH alarms and signal errors. See the "Replace Faulty GBIC or SFP Connectors" procedure on page 1-133.

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

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

Verify Fiber-Optic Connections

Step 1 Ensure that a single-mode fiber connects to the ONS 15454 ONS 15454 SDH optical card.

SM or SM Fiber should be printed on the fiber span cable. ONS 15454 SDH optical cards do not use multimode fiber.

Step 2 Ensure that the connector keys on the SC fiber connector are properly aligned and locked.

Step 3 Check that the single-mode fiber power level is within the specified range:

a. Remove the receive end of the suspect fiber.

b. Connect the receive end of the suspect fiber to a fiber-optic power meter, such as a GN Nettest LP-5000.

c. Determine the power level of fiber with the fiber-optic power meter.

d. Verify the power meter is set to the appropriate wavelength for the optical card being tested (either 1310 nm or 1550 nm depending on the specific card).

e. Verify that the power level falls within the range specified for the card; see the "1.12.3 Optical Card Transmit and Receive Levels" section on page 1-135.

Step 4 If the power level falls below the specified range:

a. Clean or replace the fiber patchcords. Clean the fiber according to site practice or, if none exists, follow the procedure in the "Maintain the Node" chapter in the *Cisco ONS 15454 SDH Procedure Guide*. If possible, do this for the optical card you are working on and the far-end card.

b. Clean the optical connectors on the card. Clean the connectors according to site practice or, if none exists, follow the procedure in the "Maintain the Node" chapter in the *Cisco ONS 15454 Procedure Guide*. If possible, do this for the optical card you are working on and the far-end card.

c. Ensure that the far-end transmitting card is not an ONS 15454 SDH IR card when an ONS 15454 SDH LR card is appropriate.IR cards transmit a lower output power than LR cards.

d. Replace the far-end transmitting optical card to eliminate the possibility of a degrading transmitter on this optical card.

Caution Removing an active card can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-230 for basic instructions. For detailed information, refer to the "Maintain the Node" chapter in the *Cisco ONS 15454 SDH Procedure Guide*.

e. If the power level still falls below the specified range with the replacement fibers and replacement card, check for one of these three factors that attenuate the power level and affect link loss (LL):

- Excessive fiber distance; single-mode fiber attenuates at approximately 0.5 dB/km.
- Excessive number or fiber connectors; connectors take approximately 0.5 dB each.
- Excessive number of fiber splices; splices take approximately 0.5 dB each.

Note These are typical attenuation values. Refer to the specific product documentation for the actual values or use an optical time domain reflectometer (OTDR) to establish precise link loss and budget requirements.

Step 5 If no power level shows on the fiber, the fiber is bad or the transmitter on the optical card failed.

a. Check that the transmit and receive fibers are not reversed. LOS and EOC alarms normally accompany reversed transmit and receive fibers. Switching reversed transmit and receive fibers clears the alarms and restores the signal.

b. Clean or replace the fiber patchcords. Clean the fiber according to site practice or, if none exists, follow the procedure in the "Maintain the Node" chapter of the *Cisco ONS 15454 SDH Procedure Guide*. If possible, do this for the optical card you are working on and the far-end card.

c. Retest the fiber power level.

d. If the replacement fiber still shows no power, replace the optical card.

Step 6 If the power level on the fiber is above the range specified for the card, ensure that an ONS 15454 SDH LR card is not being used when an ONS 15454 SDH IR card is appropriate.

LR cards transmit a higher output power than IR cards. When used with short runs of fiber, an LR transmitter is be too powerful for the receiver on the receiving optical card.

Receiver overloads occur when maximum receiver power is exceeded.

Tip To prevent overloading the receiver, use an attenuator on the fiber between the ONS 15454 SDH optical card transmitter and the receiver. Place the attenuator on the receive transmitter of the ONS 15454 SDH optical cards. Refer to the attenuator documentation for specific instructions.

Tip Most fiber has text printed on only one of the two fiber strands. Use this to identify which fiber is connected to transmit and which fiber is connected to receive.

Crimp Replacement LAN Cables

You can crimp your own LAN cables for use with the ONS 15454 SDH.

Use Category-5 cable RJ-45 T-568B, Color Code (100 Mbps) and a crimping tool. Use a cross-over cable when connecting an ONS 15454 SDH to a hub, LAN modem, or switch, and use a LAN cable when connecting an ONS 15454 SDH to a router or workstation.

Figure 1-51 shows the layout of an RJ-45 connector.

Figure 1-51 RJ-45 Pin Numbers

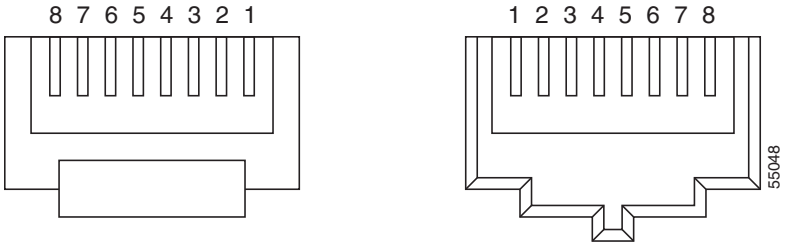


Figure 1-52 shows a LAN cable layout.

Figure 1-52 LAN Cable Layout

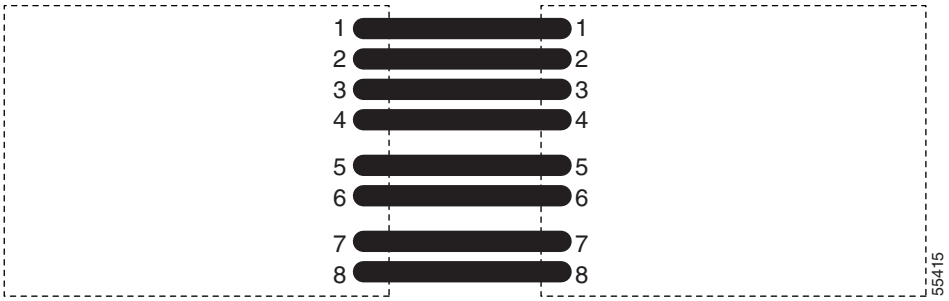


Table 1-5 provides the LAN cable pinouts.

Table 1-5 LAN Cable Pinout

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

Figure 1-53 shows a cross-over cable layout.

Figure 1-53 Cross-Over Cable Layout

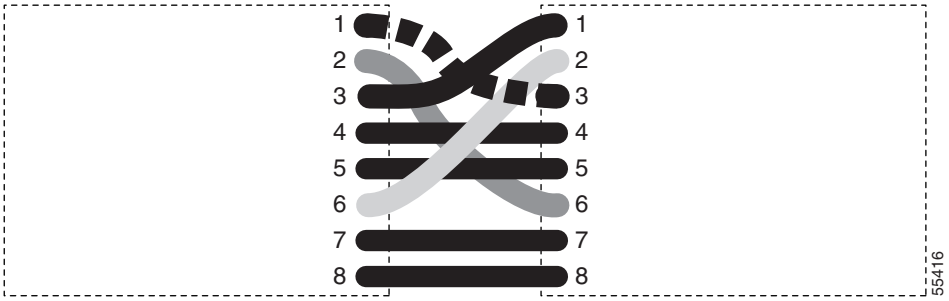


Table 1-6 provides cross-over cable pinouts.

Table 1-6 Cross-Over Cable Pinout

Pin	Color	Pair	Name	Pin
1	white/orange	2	Transmit Data +	3
2	orange	2	Transmit Data –	6

Table 1-6 Cross-Over Cable Pinout (continued)

Pin	Color	Pair	Name	Pin
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 GBIC or SFP Connectors

GBICs and SFPs are hot-swappable and can be installed or removed while the card or shelf assembly is powered and running.

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

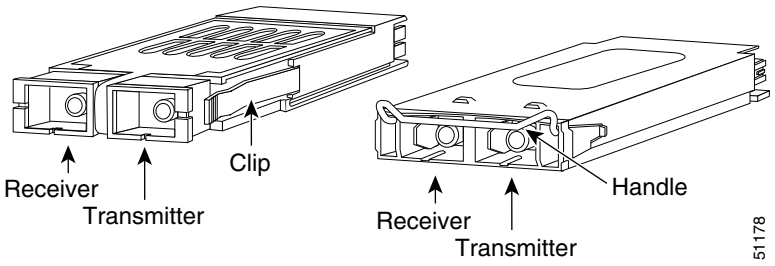
Warning **Invisible laser radiation may be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments.** Statement 1051

GBICs and SFPs are input/output devices that plug into a Gigabit Ethernet card or MXP card to link the port with the fiber-optic network. The type of GBIC or SFP determines the maximum distance that the Ethernet traffic can travel from the card to the next network device.

Note GBICs and SFPs must be matched on either end by type: SX to SX, LX to LX, or ZX to ZX.

GBICs are available in two different models. One GBIC model has two clips (one on each side of the GBIC) that secure the GBIC in the slot on the E1000-2-G or G-Series card. The other model has a locking handle. Both models are shown in Figure 1-54.

Figure 1-54 Gigabit Interface Converters



For a list of available GBICs and SFPs for Ethernet cards and FC_MR-4 cards, refer to the "Ethernet Cards" chapter in the *Cisco ONS 15454 SDH Reference Manual*. For a list of available SFPs for TXP and MXP cards, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Note The GBICs are very similar in appearance. Check the GBIC label carefully before installing it.

Remove GBIC or SFP Connectors

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

Step 1 Disconnect the network fiber cable from the GBIC SC connector or SFP LC duplex connector.

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

Step 3 Slide the GBIC or SFP out of the Gigabit Ethernet module slot. A flap closes over the GBIC or SFP slot to protect the connector on the Gigabit Ethernet card.

Step 4 To replace a GBIC, see the "Install a GBIC with Clips" procedure on page 1-134 or the "Install a GBIC with a Handle" procedure on page 1-135. To replace an SFP, see the "Replace Faulty GBIC or SFP Connectors" procedure on page 1-133.

Install a GBIC with Clips

Step 1 Remove the GBIC from its protective packaging.

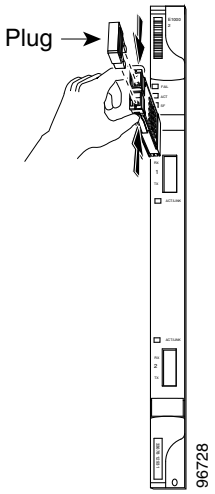
Step 2 Check the label to verify that the GBIC is the correct type (SX, LX, or ZX) for your network.

Step 3 Verify that you are installing compatible GBICs; for example, SX to SX, LX to LX, or ZX to ZX.

Step 4 Grip the sides of the GBIC with your thumb and forefinger and insert the GBIC into the slot on the E1000-2, E1000-2-G, or G-Series card (Figure 1-55).

Note GBICs are keyed to prevent incorrect installation.

Figure 1-55 GBIC Installation With Clips



Step 5 Slide the GBIC through the flap that covers the opening until you hear a click. The click indicates the GBIC is locked into the slot.

Step 6 When you are ready to attach the network fiber-optic cable, remove the protective plug from the GBIC and save the plug for future use.

Install a GBIC with a Handle

Step 1 Remove the GBIC from its protective packaging.

Step 2 Check the label to verify that the GBIC is the correct type (SX, LX, or ZX) for your network.

Step 3 Verify that you are installing compatible GBICs; for example, SX to SX, LX to LX, or ZX to ZX.

Step 4 Remove the protective plug from the SC-type connector.

Step 5 Grip the sides of the GBIC with your thumb and forefinger and insert the GBIC into the slot on the E1000-2-G or G-Series card.

Note GBICs are keyed to prevent incorrect installation.

Step 6 Lock the GBIC into place by closing the handle down. The handle is in the correct closed position when it does not obstruct access to SC-type connector.

1.12.3 Optical Card Transmit and Receive Levels

Each STM-N card has a transmit and receive connector on its faceplate. The transmit and receive levels for each card are listed in Table 1-7.

Table 1-7 Optical Card Transmit and Receive Levels

Optical Card	Receive	Transmit
OC3 IR 4/STM1 SH 1310	–28 to –8 dBm	–15 to –8 dBm
OC3 IR/STM1SH 1310-8	–30 to –8 dBm	–15 to –8 dBm
OC12 IR/STM4 SH 1310	–28 to –8 dBm	–15 to –8 dBm
OC12 LR/STM4 LH 1310	–28 to –8 dBm	–3 to +2 dBm
OC12 LR/STM4 LH 1550	–28 to –8 dBm	–3 to +2 dBm
OC12 IR/STM4 SH 1310-4	–28 to –8 dBm	–3 to +2 dBm
OC48 IR/STM16 SH AS 1310	–18 to 0 dBm	–5 to 0 dBm
OC48 LR/STM16 LH AS 1550	–28 to –8 dBm	–2 to +3 dBm
OC48 ELR/STM16 EH 100 GHz	–28 to –8 dBm	–2 to 0 dBm
OC192 SR/STM64 IO 1310	–11 to –1 dBm	–6 to –1 dBm
OC192 IR STM64 SH 1550	–14 to –1 dBm	–1 to +2 dBm
OC192 LR/STM64 LH 1550	–21 to –9 dBm	+7 to +10 dBm
OC192 LR/STM64 LH ITU 15xx.xx	–22 to –9 dBm	+3 to +6 dBm
TXP-MR-10G Trunk side: Client side:	 –26 to –8 dBm –14 to –1 dBm	 –16 to +3 dBm –6 to –1 dBm
MXP-2.5G-10G Trunk side: Client side:	 –26 to –8 dBm depends on SFP	 –16 to +3 dBm depends on SFP

1.13 Power Supply Problems

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

Possible Cause Loss of power or low voltage.

Possible Cause Improperly connected power supply.

Recommended Action The ONS 15454 SDH requires a constant source of DC power to properly function. Input power is –48 VDC. Power requirements range from –42 VDC to –57 VDC. A newly installed ONS 15454 SDH that is not properly connected to its power supply does not operate. Power problems can be confined to a specific ONS 15454 SDH or affect several pieces of equipment on the site. A loss of power or low voltage can result in a loss of traffic and causes the LCD clock on the ONS 15454 SDH to default to January 1, 1970, 00:04:15. To reset the clock, in node view click the **Provisioning > General > General** tabs and change the Date and Time fields. See the "Isolate the Cause of Power Supply Problems" procedure on page 1-137.

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

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

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

Isolate the Cause of Power Supply Problems

Step 1 If a single ONS 15454 SDH 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 FMEC card under the clear plastic cover.
- **b.** Verify that the power cable is #12 or #14 AWG and in good condition.
- **c.** Verify that the power cable connections are properly crimped. Stranded #12 or #14 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 ONS 15454 SDH FMEC. 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 –42 VDC to –57 VDC.
  - Check the age of the batteries. Battery performance decreases with age.
  - Check for opens and shorts in batteries, which might affect power output.
  - If brownouts occur, the power load and fuses might be too high for the battery plant.

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

- **a.** Check the uninterruptible power supply (UPS) or rectifiers that supply the equipment. Refer to the UPS manufacturer's documentation for specific instructions.
- **b.** Check for excessive power drains caused by other equipment, such as generators.
- **c.** Check for excessive power demand on backup power systems or batteries, when alternate power sources are used.

1.13.1 Power Consumption for Node and Cards

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

Possible Cause Improper power supply.

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

CHAPTER 2

Alarm Troubleshooting

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

This chapter gives a description, severity, and troubleshooting procedure for each commonly encountered Cisco ONS 15454 SDH alarm and condition. Tables 2-1 through 2-5 provide lists of ONS 15454 SDH alarms organized by severity. Table 2-6 on page 2-9 provides a list of alarms organized alphabetically. Table 2-7 gives definitions of all ONS 15454 SDH alarm logical objects, which are the basis of the alarm profile list in Table 2-8 on page 2-19. For a comprehensive list of all conditions, refer to the *Cisco ONS 15454 SDH TL1 Reference Guide*. For instructions on using Transaction Language One (TL1) commands, refer to the *Cisco ONS 15454 SDH TL1 Command Guide*.

An alarm's troubleshooting procedure applies to both the Cisco Transport Controller (CTC) and TL1 version of that alarm. If the troubleshooting procedure does not clear the alarm log into the Technical Support Website at http://www.cisco.com/techsupport for more information or 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.

More information about alarm profile information modification and downloads is located in the "Manage Alarms" chapter of the *Cisco ONS 15454 SDH Procedure Guide*.

2.1 Alarm Index by Default Severity

The following tables group alarms and conditions by their default severities in the ONS 15454 SDH system. These severities are reported in the CTC Alarms window severity (SEV) column.

Note The CTC default alarm profile contains some alarms or conditions that are not currently implemented but are reserved for future use.

The following tables group alarms and conditions by the severity displayed in the CTC Alarms window in the severity (SEV) column. All severities listed in this manual are the default profile settings. Alarm severities can be altered from default settings for individual alarms or groups of alarms by creating a

nondefault alarm profile and applying it on a port, card, or shelf basis. All settings (default or user-defined) that are Critical (CR) or Major (MJ) are demoted to Minor (MN) in situations that do not affect service.

Note The CTC default alarm profile in some cases contains two severities for one alarm (for example, MJ/MN). The ONS 15454 SDH 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.

2.1.1 Critical Alarms (CR)

Table 2-1 alphabetically lists ONS 15454 SDH Critical (CR) alarms.

Table 2-1 ONS 15454 SDH Critical Alarm List

AU-LOF (VCTRM-HP)	IMPROPRMVL (EQPT)	MFGMEM (BPLANE)
AU-LOP (VCMON-HP)	IMPROPRMVL (PPM)	MFGMEM (FAN)
AU-LOP (VCTRM-HP)	LOA (VCG)	MFGMEM (PPM)
AUTOLSROFF (STMN)	LOF (DS3)	OPWR-HFAIL (AOTS)
AUTOLSROFF (TRUNK)	LOF (E4)	OPWR-HFAIL (OCH)
AWG-FAIL (OTS)	LOF (STM1E)	OPWR-HFAIL (OMS)
AWG-OVERTEMP (OTS)	LOF (STMN)	OPWR-HFAIL (OTS)
BKUPMEMP (EQPT)	LOF (TRUNK)	OPWR-LFAIL (AOTS)
COMIOXC (EQPT)	LOM (TRUNK)	OPWR-LFAIL (OCH)
CONTBUS-DISABLED (EQPT)	LOM (VCMON-HP)	OPWR-LFAIL (OMS)
CTNEQPT-PBPROT (EQPT)	LOS (DS3)	OPWR-LFAIL (OTS)
CTNEQPT-PBWORK (EQPT)	LOS (E3)	OTUK-LOF (TRUNK)
EQPT (AICI-AEP)	LOS (E4)	OTUK-TIM (TRUNK)
EQPT (AICI-AIE)	LOS (ESCON)	PORT-ADD-PWR-FAIL-HIGH (OCH)
EQPT (EQPT)	LOS (ISC)	PORT-ADD-PWR-FAIL-LOW (OCH)
EQPT (PPM)	LOS (OTS)	PORT-FAIL (OCH)
EQPT-MISS (FAN)	LOS (STM1E)	RS-TIM (STMN)
FAN (FAN)	LOS (STMN)	SQM (VCTRM-HP)
GAIN-HFAIL (AOTS)	LOS (TRUNK)	SWMTXMOD-PROT (EQPT)
GAIN-LFAIL (AOTS)	LOS-P (OCH)	SWMTXMOD-WORK (EQPT)
GE-OOSYNC (FC)	LOS-P (OMS)	TIM (STMN)
GE-OOSYNC (GE)	LOS-P (OTS)	TIM (TRUNK)
GE-OOSYNC (ISC)	LOS-P (TRUNK)	VOA-HFAIL (AOTS)
GE-OOSYNC (TRUNK)	LP-ENCAP-MISMATCH (VCTRM-LP)	VOA-HFAIL (OCH)
HITEMP (NE)	MEA (BIC)	VOA-HFAIL (OMS)
HP-ENCAP-MISMATCH (VCTRM-HP)	MEA (EQPT)	VOA-HFAIL (OTS)

Table 2-1 ONS 15454 SDH Critical Alarm List (continued)

HP-TIM (VCTRM-HP)	MEA (FAN)	VOA-LFAIL (AOTS)
HP-UNEQ (VCMON-HP)	MEA (PPM)	VOA-LFAIL (OCH)
HP-UNEQ (VCTRM-HP)	MFGMEM (AICI-AEP)	VOA-LFAIL (OMS)
I-HITEMP (NE)	MFGMEM (AICI-AIE)	VOA-LFAIL (OTS)

2.1.2 Major Alarms (MJ)

Table 2-2 alphabetically lists ONS 15454 SDH Major (MJ) alarms.

Table 2-2 ONS 15454 SDH Major Alarm List

APSCM (STMN)	GFP-LFD (CE100T)	PTIM (TRUNK)
APSCNMIS (STMN)	GFP-LFD (FCMR)	RCVR-MISS (DS1)
BAT-FAIL (PWR)	GFP-LFD (GFP-FAC)	RCVR-MISS (E1)
CARLOSS (CE100T)	GFP-LFD (ML1000)	RING-ID-MIS (OSC-RING)
CARLOSS (E1000F)	GFP-LFD (ML100T)	RING-ID-MIS (STMN)
CARLOSS (E100T)	GFP-LFD (MLFX)	RING-MISMATCH (STMN)
CARLOSS (EQPT)	GFP-NO-BUFFERS (FCMR)	SIGLOSS (FC)
CARLOSS (FC)	GFP-NO-BUFFERS (GFP-FAC)	SIGLOSS (FCMR)
CARLOSS (G1000)	GFP-UP-MISMATCH (CE100T)	SIGLOSS (GE)
CARLOSS (GE)	GFP-UP-MISMATCH (FCMR)	SIGLOSS (ISC)
CARLOSS (ISC)	GFP-UP-MISMATCH (GFP-FAC)	SIGLOSS (TRUNK)
CARLOSS (ML1000)	GFP-UP-MISMATCH (ML1000)	SQM (VCTRM-LP)
CARLOSS (ML100T)	GFP-UP-MISMATCH (ML100T)	SYNCLOSS (FC)
CARLOSS (MLFX)	GFP-UP-MISMATCH (MLFX)	SYNCLOSS (FCMR)
CARLOSS (TRUNK)	INVMACADR (BPLANE)	SYNCLOSS (GE)
DBOSYNC (NE)	LASERBIAS-FAIL (AOTS)	SYNCLOSS (ISC)
DSP-COMM-FAIL (TRUNK)	LOF (DS1)	SYNCLOSS (TRUNK)
DSP-FAIL (TRUNK)	LOF (E1)	SYNCPRI (NE-SREF)
EHIBATVG (PWR)	LOM (VCTRM-HP)	SYSBOOT (NE)
ELWBATVG (PWR)	LOS (DS1)	TIM (STM1E)
E-W-MISMATCH (STMN)	LOS (E1)	TPTFAIL (CE100T)
EXTRA-TRAF-PREEMPT (STMN)	LP-PLM (VCTRM-LP)	TPTFAIL (FCMR)
FC-NO-CREDITS (FC)	LP-TIM (VCTRM-LP)	TPTFAIL (G1000)
FC-NO-CREDITS (FCMR)	LP-UNEQ (VCMON-LP)	TPTFAIL (ML1000)
FC-NO-CREDITS (TRUNK)	LP-UNEQ (VCTRM-LP)	TPTFAIL (ML100T)
FEC-MISM (TRUNK)	MEM-GONE (EQPT)	TPTFAIL (MLFX)
GFP-CSF (CE100T)	MSSP-OOSYNC (STMN)	TRMT (DS1)

Table 2-2 ONS 15454 SDH Major Alarm List (continued)

GFP-CSF (FCMR)	MSSP-SW-VER-MISM (STMN)	TRMT (E1)
GFP-CSF (GFP-FAC)	ODUK-TIM-PM (TRUNK)	TRMT-MISS (DS1)
GFP-CSF (ML1000)	OPTNTWMIS (NE)	TRMT-MISS (E1)
GFP-CSF (ML100T)	OUT-OF-SYNC (FC)	TU-LOP (VCMON-LP)
GFP-CSF (MLFX)	OUT-OF-SYNC (GE)	TU-LOP (VCTRM-LP)
GFP-DE-MISMATCH (FCMR)	OUT-OF-SYNC (TRUNK)	UT-COMM-FAIL (TRUNK)
GFP-DE-MISMATCH (GFP-FAC)	PEER-NORESPONSE (EQPT)	UT-FAIL (TRUNK)
GFP-EX-MISMATCH (FCMR)	PRC-DUPID (STMN)	WVL-MISMATCH (TRUNK)
GFP-EX-MISMATCH (GFP-FAC)	—	—

2.1.3 Minor Alarms (MN)

Table 2-3 alphabetically lists ONS 15454 SDH Minor (MN) alarms.

Table 2-3 ONS 15454 SDH Minor Alarm List

APSB (STMN)	HI-RXPOWER (GE)	LO-TXPOWER (STMN)
APSCDFLTK (STMN)	HI-RXPOWER (ISC)	LO-TXPOWER (TRUNK)
APSC-IMP (STMN)	HI-RXPOWER (STMN)	MEM-LOW (EQPT)
APSCINCON (STMN)	HI-RXPOWER (TRUNK)	MS-EOC (STMN)
APSIMP (STMN)	HITEMP (EQPT)	OPWR-HDEG (OCH)
APS-INV-PRIM (STMN)	HI-TXPOWER (EQPT)	OPWR-HDEG (OMS)
APSMM (STMN)	HI-TXPOWER (ESCON)	OPWR-HDEG (OTS)
APS-PRIM-SEC-MISM (STMN)	HI-TXPOWER (FC)	OPWR-LDEG (AOTS)
AUTORESET (EQPT)	HI-TXPOWER (GE)	OPWR-LDEG (OCH)
AUTOSW-UNEQ-SNCP (VCMON-LP)	HI-TXPOWER (ISC)	OPWR-LDEG (OMS)
AWG-DEG (OTS)	HI-TXPOWER (PPM)	OPWR-LDEG (OTS)
CASETEMP-DEG (AOTS)	HI-TXPOWER (STMN)	OTUK-IAE (TRUNK)
COMM-FAIL (EQPT)	HI-TXPOWER (TRUNK)	PORT-ADD-PWR-DEG-HI (OCH)
CONTBUS-A-18 (EQPT)	HP-TIM (VCMON-HP)	PORT-ADD-PWR-DEG-LOW (OCH)
CONTBUS-B-18 (EQPT)	ISIS-ADJ-FAIL (STMN)	PROTNA (EQPT)
CONTBUS-IO-A (EQPT)	KBYTE-APS-CHANNEL-FAILURE (STMN)	PROV-MISMATCH (PPM)
CONTBUS-IO-B (EQPT)	LASERBIAS-DEG (AOTS)	PWR-FAIL-A (EQPT)
DATAFLT (NE)	LASERBIAS-DEG (OTS)	PWR-FAIL-B (EQPT)
DUP-IPADDR (NE)	LASERTEMP-DEG (AOTS)	PWR-FAIL-RET-A (EQPT)
DUP-NODENAME (NE)	LOF (BITS)	PWR-FAIL-RET-B (EQPT)
EOC (STMN)	LO-LASERBIAS (EQPT)	SFTWDOWN (EQPT)
EOC (TRUNK)	LO-LASERBIAS (PPM)	SH-INS-LOSS-VAR-DEG-HIGH (OTS)

Table 2-3 ONS 15454 SDH Minor Alarm List (continued)

EOC-L (TRUNK)	LO-LASERBIAS (STMN)	SH-INS-LOSS-VAR-DEG-LOW (OTS)
ERROR-CONFIG (EQPT)	LO-LASERTEMP (EQPT)	SNTP-HOST (NE)
EXCCOL (EQPT)	LO-LASERTEMP (PPM)	SSM-FAIL (BITS)
EXT (ENVALRM)	LO-LASERTEMP (STMN)	SSM-FAIL (E1)
FEPRLF (STMN)	LOM (VCTRM-LP)	SSM-FAIL (TRUNK)
FIBERTEMP-DEG (AOTS)	LO-RXPOWER (ESCON)	SYNCPRI (EXT-SREF)
GAIN-HDEG (AOTS)	LO-RXPOWER (FC)	SYNCSEC (EXT-SREF)
GAIN-LDEG (AOTS)	LO-RXPOWER (GE)	SYNCSEC (NE-SREF)
GCC-EOC (TRUNK)	LO-RXPOWER (ISC)	SYNCTHIRD (EXT-SREF)
HELLO (STMN)	LO-RXPOWER (STMN)	SYNCTHIRD (NE-SREF)
HI-LASERBIAS (EQPT)	LO-RXPOWER (TRUNK)	TIM-MON (STMN)
HI-LASERBIAS (ESCON)	LOS (BITS)	TIM-MON (TRUNK)
HI-LASERBIAS (FC)	LOS (FUDC)	UNREACHABLE-TARGET-POWER (OCH)
HI-LASERBIAS (GE)	LOS (MSUDC)	VOA-HDEG (AOTS)
HI-LASERBIAS (ISC)	LOS-O (OCH)	VOA-HDEG (OCH)
HI-LASERBIAS (PPM)	LOS-O (OMS)	VOA-HDEG (OMS)
HI-LASERBIAS (STMN)	LOS-O (OTS)	VOA-HDEG (OTS)
HI-LASERBIAS (TRUNK)	LO-TXPOWER (EQPT)	VOA-LDEG (AOTS)
HI-LASERTEMP (EQPT)	LO-TXPOWER (ESCON)	VOA-LDEG (OCH)
HI-LASERTEMP (PPM)	LO-TXPOWER (FC)	VOA-LDEG (OMS)
HI-LASERTEMP (STMN)	LO-TXPOWER (GE)	VOA-LDEG (OTS)
HI-RXPOWER (ESCON)	LO-TXPOWER (ISC)	OPWR-HDEG (AOTS)
HI-RXPOWER (FC)	LO-TXPOWER (PPM)	—

2.1.4 Not Alarmed Conditions (NA)

Table 2-4 alphabetically lists ONS 15454 SDH Not Alarmed (NA) conditions.

Table 2-4 ONS 15454 SDH Not Alarmed Conditions List

ALS (AOTS)	FORCED-REQ-SPAN (ESCON)	ROLL (VCMON-LP)
ALS (ESCON)	FORCED-REQ-SPAN (FC)	ROLL (VCTRM-HP)
ALS (FC)	FORCED-REQ-SPAN (GE)	ROLL-PEND (VCMON-HP)
ALS (GE)	FORCED-REQ-SPAN (ISC)	ROLL-PEND (VCMON-LP)
ALS (ISC)	FORCED-REQ-SPAN (STMN)	RPRW (ML1000)
ALS (TRUNK)	FORCED-REQ-SPAN (TRUNK)	RPRW (ML100T)
AMPLI-INIT (AOTS)	FRCDSWTOINT (NE-SREF)	RPRW (MLFX)
APC-CORRECTION-SKIPPED (AOTS)	FRCDSWTOPRI (EXT-SREF)	RUNCFG-SAVENEED (EQPT)

Table 2-4 ONS 15454 SDH Not Alarmed Conditions List (continued)

APC-CORRECTION-SKIPPED (OCH)	FRCDSWTOPRI (NE-SREF)	SD (DS1)
APC-CORRECTION-SKIPPED (OMS)	FRCDSWTOSEC (EXT-SREF)	SD (DS3)
APC-CORRECTION-SKIPPED (OTS)	FRCDSWTOSEC (NE-SREF)	SD (E1)
APC-DISABLED (NE)	FRCDSWTOTHIRD (EXT-SREF)	SD (E3)
APC-END (NE)	FRCDSWTOTHIRD (NE-SREF)	SD (E4)
APC-OUT-OF-RANGE (AOTS)	FRNGSYNC (NE-SREF)	SD (STM1E)
APC-OUT-OF-RANGE (OCH)	FSTSYNC (NE-SREF)	SD (STMN)
APC-OUT-OF-RANGE (OMS)	FULLPASSTHR-BI (STMN)	SD (TRUNK)
APC-OUT-OF-RANGE (OTS)	HLDOVRSYNC (NE-SREF)	SDBER-EXCEED-HO (VCMON-HP)
APS-PRIM-FAC (STMN)	INC-ISD (DS3)	SDBER-EXCEED-HO (VCTRM-HP)
AS-CMD (AOTS)	INC-ISD (E3)	SDBER-EXCEED-LO (VCMON-LP)
AS-CMD (BPLANE)	INHSWPR (EQPT)	SDBER-EXCEED-LO (VCTRM-LP)
AS-CMD (CE100T)	INHSWWKG (EQPT)	SD-L (STM1E)
AS-CMD (DS1)	INTRUSION-PSWD (NE)	SF (DS1)
AS-CMD (DS3)	IOSCFGCOPY (EQPT)	SF (DS3)
AS-CMD (E1)	KB-PASSTHR (STMN)	SF (E1)
AS-CMD (E1000F)	LAN-POL-REV (NE)	SF (E3)
AS-CMD (E100T)	LASER-APR (AOTS)	SF (E4)
AS-CMD (E3)	LCAS-CRC (VCTRM-HP)	SF (STMN)
AS-CMD (E4)	LCAS-CRC (VCTRM-LP)	SF (TRUNK)
AS-CMD (EQPT)	LCAS-RX-FAIL (VCTRM-HP)	SFBER-EXCEED-HO (VCMON-HP)
AS-CMD (ESCON)	LCAS-RX-FAIL (VCTRM-LP)	SFBER-EXCEED-HO (VCTRM-HP)
AS-CMD (FC)	LCAS-TX-ADD (VCTRM-HP)	SFBER-EXCEED-LO (VCMON-LP)
AS-CMD (FCMR)	LCAS-TX-ADD (VCTRM-LP)	SFBER-EXCEED-LO (VCTRM-LP)
AS-CMD (G1000)	LCAS-TX-DNU (VCTRM-HP)	SF-L (STM1E)
AS-CMD (GE)	LCAS-TX-DNU (VCTRM-LP)	SHUTTER-OPEN (OTS)
AS-CMD (GFP-FAC)	LKOUTPR-S (STMN)	SPAN-SW-EAST (STMN)
AS-CMD (ISC)	LOCKOUT-REQ (EQPT)	SPAN-SW-WEST (STMN)
AS-CMD (ML1000)	LOCKOUT-REQ (ESCON)	SQUELCH (STMN)
AS-CMD (ML100T)	LOCKOUT-REQ (FC)	SQUELCHED (ESCON)
AS-CMD (MLFX)	LOCKOUT-REQ (GE)	SQUELCHED (FC)

Table 2-4 ONS 15454 SDH Not Alarmed Conditions List (continued)

AS-CMD (NE)	LOCKOUT-REQ (ISC)	SQUELCHED (GE)
AS-CMD (OCH)	LOCKOUT-REQ (STMN)	SQUELCHED (ISC)
AS-CMD (OMS)	LOCKOUT-REQ (TRUNK)	SQUELCHED (STMN)
AS-CMD (OTS)	LOCKOUT-REQ (VCMON-HP)	SQUELCHED (TRUNK)
AS-CMD (PPM)	LOCKOUT-REQ (VCMON-LP)	SSM-DUS (BITS)
AS-CMD (PWR)	LPBKCRS (VCMON-HP)	SSM-DUS (E1)
AS-CMD (STM1E)	LPBKCRS (VCTRM-HP)	SSM-DUS (STMN)
AS-CMD (STMN)	LPBKDS1FEAC-CMD (DS1)	SSM-LNC (BITS)
AS-CMD (TRUNK)	LPBKDS3FEAC (DS3)	SSM-LNC (NE-SREF)
AS-MT (AOTS)	LPBKDS3FEAC-CMD (DS3)	SSM-LNC (STMN)
AS-MT (CE100T)	LPBKDS3FEAC-CMD (E3)	SSM-LNC (TRUNK)
AS-MT (DS1)	LPBKE1FEAC (E3)	SSM-OFF (BITS)
AS-MT (DS3)	LPBKE3FEAC (E3)	SSM-OFF (E1)
AS-MT (E1)	LPBKFACILITY (CE100T)	SSM-OFF (TRUNK)
AS-MT (E3)	LPBKFACILITY (DS1)	SSM-PRC (BITS)
AS-MT (E4)	LPBKFACILITY (DS3)	SSM-PRC (NE-SREF)
AS-MT (EQPT)	LPBKFACILITY (E1)	SSM-PRC (STMN)
AS-MT (ESCON)	LPBKFACILITY (E3)	SSM-PRC (TRUNK)
AS-MT (FC)	LPBKFACILITY (E4)	SSM-PRS (E1)
AS-MT (FCMR)	LPBKFACILITY (ESCON)	SSM-PRS (TRUNK)
AS-MT (G1000)	LPBKFACILITY (FC)	SSM-RES (E1)
AS-MT (GE)	LPBKFACILITY (FCMR)	SSM-RES (TRUNK)
AS-MT (GFP-FAC)	LPBKFACILITY (G1000)	SSM-SDH-TN (BITS)
AS-MT (ISC)	LPBKFACILITY (GE)	SSM-SDH-TN (NE-SREF)
AS-MT (ML1000)	LPBKFACILITY (ISC)	SSM-SDH-TN (TRUNK)
AS-MT (ML100T)	LPBKFACILITY (STM1E)	SSM-SETS (BITS)
AS-MT (MLFX)	LPBKFACILITY (STMN)	SSM-SETS (NE-SREF)
AS-MT (OCH)	LPBKFACILITY (TRUNK)	SSM-SETS (STMN)
AS-MT (OMS)	LPBKTERMINAL (CE100T)	SSM-SETS (TRUNK)
AS-MT (OTS)	LPBKTERMINAL (DS1)	SSM-SMC (E1)
AS-MT (PPM)	LPBKTERMINAL (DS3)	SSM-SMC (TRUNK)
AS-MT (STM1E)	LPBKTERMINAL (E1)	SSM-ST2 (E1)
AS-MT (STMN)	LPBKTERMINAL (E3)	SSM-ST2 (TRUNK)
AS-MT (TRUNK)	LPBKTERMINAL (E4)	SSM-ST3 (E1)
AS-MT-OOG (VCTRM-HP)	LPBKTERMINAL (ESCON)	SSM-ST3 (TRUNK)
AS-MT-OOG (VCTRM-LP)	LPBKTERMINAL (FC)	SSM-ST3E (E1)
AUD-LOG-LOSS (NE)	LPBKTERMINAL (FCMR)	SSM-ST3E (TRUNK)

Table 2-4 ONS 15454 SDH Not Alarmed Conditions List (continued)

AUD-LOG-LOW (NE)	LPBKTERMINAL (G1000)	SSM-ST4 (E1)
AUTOSW-LOP-SNCP (VCMON-HP)	LPBKTERMINAL (GE)	SSM-ST4 (STMN)
AUTOSW-LOP-SNCP (VCMON-LP)	LPBKTERMINAL (ISC)	SSM-ST4 (TRUNK)
—	LPBKTERMINAL (STM1E)	SSM-STU (BITS)
AUTOSW-SDBER-SNCP (VCMON-HP)	LPBKTERMINAL (STMN)	SSM-STU (E1)
AUTOSW-SFBER-SNCP (VCMON-HP)	LPBKTERMINAL (TRUNK)	SSM-STU (NE-SREF)
AUTOSW-UNEQ-SNCP (VCMON-HP)	MAN-REQ (EQPT)	SSM-STU (STMN)
AWG-WARM-UP (OTS)	MAN-REQ (VCMON-HP)	SSM-STU (TRUNK)
CLDRESTART (EQPT)	MAN-REQ (VCMON-LP)	SSM-TNC (STMN)
CTNEQPT-MISMATCH (EQPT)	MANRESET (EQPT)	SSM-TNC (TRUNK)
DS3-MISM (DS3)	MANSWTOINT (NE-SREF)	SW-MISMATCH (EQPT)
ETH-LINKLOSS (NE)	MANSWTOPRI (EXT-SREF)	SWTOPRI (EXT-SREF)
EXERCISE-RING-FAIL (STMN)	MANSWTOPRI (NE-SREF)	SWTOPRI (NE-SREF)
EXERCISE-SPAN-FAIL (STMN)	MANSWTOSEC (EXT-SREF)	SWTOSEC (EXT-SREF)
FAILTOSW (EQPT)	MANSWTOSEC (NE-SREF)	SWTOSEC (NE-SREF)
FAILTOSW (ESCON)	MANSWTOTHIRD (EXT-SREF)	SWTOTHIRD (EXT-SREF)
FAILTOSW (FC)	MANSWTOTHIRD (NE-SREF)	SWTOTHIRD (NE-SREF)
FAILTOSW (GE)	MANUAL-REQ-RING (STMN)	SYNC-FREQ (E1)
FAILTOSW (ISC)	MANUAL-REQ-SPAN (ESCON)	SYNC-FREQ (STMN)
FAILTOSW (STMN)	MANUAL-REQ-SPAN (FC)	SYNC-FREQ (TRUNK)
FAILTOSW (TRUNK)	MANUAL-REQ-SPAN (GE)	TEMP-MISM (NE)
FAILTOSW-HO (VCMON-HP)	MANUAL-REQ-SPAN (ISC)	TX-RAI (DS1)
FAILTOSW-LO (VCMON-LP)	MANUAL-REQ-SPAN (STMN)	TX-RAI (E1)
FAILTOSWR (STMN)	MANUAL-REQ-SPAN (TRUNK)	TX-RAI (E3)
FAILTOSWS (STMN)	NO-CONFIG (EQPT)	UNC-WORD (TRUNK)
FE-AIS (E3)	OCHNC-INC (OCHNC-CONN)	VCG-DEG (VCG)
FE-E1-MULTLOS (E3)	ODUK-SD-PM (TRUNK)	VCG-DOWN (VCG)
FE-E1-NSA (E3)	ODUK-SF-PM (TRUNK)	VOLT-MISM (PWR)
FE-E1-SA (E3)	OOU-TPT (VCTRM-HP)	WKSWPR (EQPT)
FE-E1-SNGLLOS (E3)	OOU-TPT (VCTRM-LP)	WKSWPR (ESCON)
FE-E3-NSA (E3)	OSRION (AOTS)	WKSWPR (FC)
FE-E3-SA (E3)	OSRION (OTS)	WKSWPR (GE)
FE-EQPT-NSA (E3)	OTUK-SD (TRUNK)	WKSWPR (ISC)
FE-FRCDWKSWBK-SPAN (STMN)	OTUK-SF (TRUNK)	WKSWPR (STMN)
FE-FRCDWKSWPR-RING (STMN)	OUT-OF-SYNC (ISC)	WKSWPR (TRUNK)
FE-FRCDWKSWPR-SPAN (STMN)	PARAM-MISM (OCH)	WKSWPR (VCMON-HP)
FE-IDLE (E3)	PARAM-MISM (OMS)	WKSWPR (VCMON-LP)

Table 2-4 ONS 15454 SDH Not Alarmed Conditions List (continued)

FE-LOCKOUTOFPR-SPAN (STMN)	PARAM-MISM (OTS)	WTR (EQPT)
FE-LOF (E3)	—	WTR (ESCON)
FE-LOS (E3)	PORT-MISMATCH (FCMR)	WTR (FC)
FE-MANWKSWBK-SPAN (STMN)	RAI (DS1)	WTR (GE)
FE-MANWKSWPR-RING (STMN)	RAI (DS3)	WTR (ISC)
FE-MANWKSWPR-SPAN (STMN)	RAI (E1)	WTR (STMN)
FORCED-REQ (EQPT)	RFI-V (VCMON-LP)	WTR (TRUNK)
FORCED-REQ (VCMON-HP)	RING-SW-EAST (STMN)	WTR (VCMON-HP)
FORCED-REQ (VCMON-LP)	RING-SW-WEST (STMN)	WTR (VCMON-LP)
FORCED-REQ-RING (STMN)	ROLL (VCMON-HP)	—

2.1.5 Not Reported Conditions (NR)

Table 2-5 alphabetically lists ONS 15454 SDH Not Reported (NR) conditions.

Table 2-5 ONS 15454 SDH Not Reported Conditions List

AIS (BITS)	AUTOSW-AIS-SNCP (VCMON-LP)	ODUK-OCI-PM (TRUNK)
AIS (DS1)	HP-RFI (VCMON-HP)	OTUK-AIS (TRUNK)
AIS (DS3)	LP-RFI (VCTRM-LP)	OTUK-BDI (TRUNK)
AIS (E1)	MS-AIS (STM1E)	RFI (TRUNK)
AIS (E3)	MS-AIS (STMN)	ROLL-PEND (VCTRM-HP)
AIS (E4)	MS-RFI (STM1E)	TU-AIS (VCMON-LP)
AIS (FUDC)	ODUK-1-AIS-PM (TRUNK)	TU-AIS (VCTRM-LP)
AIS (MSUDC)	ODUK-2-AIS-PM (TRUNK)	TX-AIS (DS1)
AIS (TRUNK)	ODUK-3-AIS-PM (TRUNK)	TX-AIS (DS3)
AIS-L (TRUNK)	ODUK-4-AIS-PM (TRUNK)	TX-AIS (E1)
AU-AIS (VCMON-HP)	ODUK-AIS-PM (TRUNK)	TX-AIS (E3)
AU-AIS (VCTRM-HP)	ODUK-BDI-PM (TRUNK)	TX-LOF (DS1)
AUTOSW-AIS-SNCP (VCMON-HP)	ODUK-LCK-PM (TRUNK)	TX-LOF (E1)

2.2 Alarms and Conditions Listed By Alphabetical Entry

Table 2-6 alphabetically lists all ONS 15454 SDH alarms and conditions.

Table 2-6 ONS 15454 SDH Alarm and Condition Alphabetical List

AIS (BITS)	GFP-LFD (MLFX)	OPWR-LFAIL (OCH)
AIS (DS1)	GFP-NO-BUFFERS (FCMR)	OPWR-LFAIL (OMS)

Table 2-6 ONS 15454 SDH Alarm and Condition Alphabetical List (continued)

AIS (DS3)	GFP-NO-BUFFERS (GFP-FAC)	OPWR-LFAIL (OTS)
AIS (E1)	GFP-UP-MISMATCH (CE100T)	OSRION (AOTS)
AIS (E3)	GFP-UP-MISMATCH (FCMR)	OSRION (OTS)
AIS (E4)	GFP-UP-MISMATCH (GFP-FAC)	OTUK-AIS (TRUNK)
AIS (FUDC)	GFP-UP-MISMATCH (ML1000)	OTUK-BDI (TRUNK)
AIS (MSUDC)	GFP-UP-MISMATCH (ML100T)	OTUK-IAE (TRUNK)
AIS (TRUNK)	GFP-UP-MISMATCH (MLFX)	OTUK-LOF (TRUNK)
AIS-L (TRUNK)	HELLO (STMN)	OTUK-SD (TRUNK)
ALS (2R)	HI-LASERBIAS (2R)	OTUK-SF (TRUNK)
ALS (AOTS)	HI-LASERBIAS (EQPT)	OTUK-TIM (TRUNK)
ALS (FC)	HI-LASERBIAS (ESCON)	OUT-OF-SYNC (FC)
ALS (GE)	HI-LASERBIAS (FC)	OUT-OF-SYNC (GE)
ALS (ISC)	HI-LASERBIAS (GE)	OUT-OF-SYNC (ISC)
ALS (STMN)	HI-LASERBIAS (ISC)	OUT-OF-SYNC (TRUNK)
ALS (TRUNK)	HI-LASERBIAS (PPM)	PARAM-MISM (AOTS)
AMPLI-INIT (AOTS)	HI-LASERBIAS (STMN)	PARAM-MISM (OCH)
APC-CORRECTION-SKIPPED (AOTS)	HI-LASERBIAS (TRUNK)	PARAM-MISM (OMS)
APC-CORRECTION-SKIPPED (OCH)	HI-LASERTEMP (EQPT)	PARAM-MISM (OTS)
APC-CORRECTION-SKIPPED (OMS)	HI-LASERTEMP (PPM)	—
APC-CORRECTION-SKIPPED (OTS)	HI-LASERTEMP (STMN)	PEER-NORESPONSE (EQPT)
APC-DISABLED (NE)	HI-RXPOWER (2R)	PORT-ADD-PWR-DEG-HI (OCH)
APC-END (NE)	HI-RXPOWER (ESCON)	PORT-ADD-PWR-DEG-LOW (OCH)
APC-OUT-OF-RANGE (AOTS)	HI-RXPOWER (FC)	PORT-ADD-PWR-FAIL-HIGH (OCH)
APC-OUT-OF-RANGE (OCH)	HI-RXPOWER (GE)	PORT-ADD-PWR-FAIL-LOW (OCH)
APC-OUT-OF-RANGE (OMS)	HI-RXPOWER (ISC)	PORT-FAIL (OCH)
APC-OUT-OF-RANGE (OTS)	HI-RXPOWER (STMN)	PORT-MISMATCH (FCMR)
APSB (STMN)	HI-RXPOWER (TRUNK)	PRC-DUPID (STMN)
APSCDFLTK (STMN)	HITEMP (EQPT)	PROTNA (EQPT)
APSC-IMP (STMN)	HITEMP (NE)	PROV-MISMATCH (PPM)
APSCINCON (STMN)	HI-TXPOWER (2R)	PTIM (TRUNK)
APSCM (STMN)	HI-TXPOWER (EQPT)	PWR-FAIL-A (EQPT)
APSCNMIS (STMN)	HI-TXPOWER (ESCON)	PWR-FAIL-B (EQPT)
APSIMP (STMN)	HI-TXPOWER (FC)	PWR-FAIL-RET-A (EQPT)
APS-INV-PRIM (STMN)	HI-TXPOWER (GE)	PWR-FAIL-RET-B (EQPT)
APSMM (STMN)	HI-TXPOWER (ISC)	RAI (DS1)
APS-PRIM-FAC (STMN)	HI-TXPOWER (PPM)	RAI (DS3)
APS-PRIM-SEC-MISM (STMN)	HI-TXPOWER (STMN)	RAI (E1)

Table 2-6 ONS 15454 SDH Alarm and Condition Alphabetical List (continued)

AS-CMD (2R)	HI-TXPOWER (TRUNK)	RCVR-MISS (DS1)
AS-CMD (AOTS)	HLDOVRSYNC (NE-SREF)	RCVR-MISS (E1)
AS-CMD (BPLANE)	HP-ENCAP-MISMATCH (VCTRM-HP)	RFI (TRUNK)
AS-CMD (CE100T)	HP-RFI (VCMON-HP)	RFI-V (VCMON-LP)
AS-CMD (DS1)	HP-TIM (VCMON-HP)	RING-ID-MIS (OSC-RING)
AS-CMD (DS3)	HP-TIM (VCTRM-HP)	RING-ID-MIS (STMN)
AS-CMD (E1)	HP-UNEQ (VCMON-HP)	RING-MISMATCH (STMN)
AS-CMD (E1000F)	HP-UNEQ (VCTRM-HP)	RING-SW-EAST (STMN)
AS-CMD (E100T)	I-HITEMP (NE)	RING-SW-WEST (STMN)
AS-CMD (E3)	IMPROPRMVL (EQPT)	ROLL (VCMON-HP)
AS-CMD (E4)	IMPROPRMVL (PPM)	ROLL (VCMON-LP)
AS-CMD (EQPT)	INC-ISD (DS3)	ROLL (VCTRM-HP)
AS-CMD (ESCON)	INC-ISD (E3)	ROLL-PEND (VCMON-HP)
AS-CMD (FC)	INHSWPR (EQPT)	ROLL-PEND (VCMON-LP)
AS-CMD (FCMR)	INHSWWKG (EQPT)	ROLL-PEND (VCTRM-HP)
AS-CMD (G1000)	INTRUSION-PSWD (NE)	RPRW (ML1000)
AS-CMD (GE)	INVMACADR (BPLANE)	RPRW (ML100T)
AS-CMD (ISC)	IOSCFGCOPY (EQPT)	RPRW (MLFX)
AS-CMD (ML1000)	ISIS-ADJ-FAIL (STMN)	RS-TIM (STMN)
AS-CMD (ML100T)	KB-PASSTHR (STMN)	RUNCFG-SAVENEED (EQPT)
AS-CMD (MLFX)	KBYTE-APS-CHANNEL-FAILURE (STMN)	SD (DS1)
AS-CMD (NE)	LAN-POL-REV (NE)	SD (DS3)
AS-CMD (OCH)	LASER-APR (AOTS)	SD (E1)
AS-CMD (OMS)	LASERBIAS-DEG (AOTS)	SD (E3)
AS-CMD (OTS)	LASERBIAS-DEG (OTS)	SD (E4)
AS-CMD (PPM)	LASERBIAS-FAIL (AOTS)	SD (STM1E)
AS-CMD (PWR)	LASERTEMP-DEG (AOTS)	SD (STMN)
AS-CMD (STM1E)	LCAS-CRC (VCTRM-HP)	SD (TRUNK)
AS-CMD (STMN)	LCAS-CRC (VCTRM-LP)	SDBER-EXCEED-HO (VCMON-HP)
AS-CMD (TRUNK)	LCAS-RX-FAIL (VCTRM-HP)	SDBER-EXCEED-HO (VCTRM-HP)
AS-CMD (GFP-FAC)	LCAS-RX-FAIL (VCTRM-LP)	SDBER-EXCEED-LO (VCMON-LP)
AS-MT (2R)	LCAS-TX-ADD (VCTRM-HP)	SDBER-EXCEED-LO (VCTRM-LP)
AS-MT (AOTS)	LCAS-TX-ADD (VCTRM-LP)	SD-L (STM1E)
AS-MT (CE100T)	LCAS-TX-DNU (VCTRM-HP)	SF (DS1)
AS-MT (DS1)	LCAS-TX-DNU (VCTRM-LP)	SF (DS3)
AS-MT (DS3)	LKOUTPR-S (STMN)	SF (E1)

Table 2-6 ONS 15454 SDH Alarm and Condition Alphabetical List (continued)

AS-MT (E1)	LOA (VCG)	SF (E3)
AS-MT (E3)	LOCKOUT-REQ (2R)	SF (E4)
AS-MT (E4)	LOCKOUT-REQ (EQPT)	SF (STMN)
AS-MT (EQPT)	LOCKOUT-REQ (ESCON)	SF (TRUNK)
AS-MT (ESCON)	LOCKOUT-REQ (FC)	SFBER-EXCEED-HO (VCMON-HP)
AS-MT (FC)	LOCKOUT-REQ (GE)	SFBER-EXCEED-HO (VCTRM-HP)
AS-MT (FCMR)	LOCKOUT-REQ (ISC)	SFBER-EXCEED-LO (VCMON-LP)
AS-MT (G1000)	LOCKOUT-REQ (STMN)	SFBER-EXCEED-LO (VCTRM-LP)
AS-MT (GE)	LOCKOUT-REQ (TRUNK)	SF-L (STM1E)
AS-MT (GFP-FAC)	LOCKOUT-REQ (VCMON-HP)	SFTWDOWN (EQPT)
AS-MT (ISC)	LOCKOUT-REQ (VCMON-LP)	SH-INS-LOSS-VAR-DEG-HIGH (OTS)
AS-MT (ML1000)	LOF (BITS)	SH-INS-LOSS-VAR-DEG-LOW (OTS)
AS-MT (ML100T)	LOF (DS1)	SHUTTER-OPEN (OTS)
AS-MT (MLFX)	LOF (DS3)	SIGLOSS (FC)
AS-MT (OCH)	LOF (E1)	SIGLOSS (FCMR)
AS-MT (OMS)	LOF (E4)	SIGLOSS (GE)
AS-MT (OTS)	LOF (STM1E)	SIGLOSS (ISC)
AS-MT (PPM)	LOF (STMN)	SIGLOSS (TRUNK)
AS-MT (STM1E)	LOF (TRUNK)	SNTP-HOST (NE)
AS-MT (STMN)	LO-LASERBIAS (EQPT)	SPAN-SW-EAST (STMN)
AS-MT (TRUNK)	LO-LASERBIAS (PPM)	SPAN-SW-WEST (STMN)
AS-MT-OOG	LO-LASERBIAS (STMN)	SQM (VCTRM-HP)
AS-MT-OOG (VCTRM-LP)	LO-LASERTEMP (EQPT)	SQM (VCTRM-LP)
AU-AIS (VCMON-HP)	LO-LASERTEMP (PPM)	SQUELCH (STMN)
AU-AIS (VCTRM-HP)	LO-LASERTEMP (STMN)	SQUELCHED (2R)
AUD-LOG-LOSS (NE)	LOM (TRUNK)	SQUELCHED (ESCON)
AUD-LOG-LOW (NE)	LOM (VCMON-HP)	SQUELCHED (FC)
AU-LOF (VCTRM-HP)	LOM (VCTRM-HP)	SQUELCHED (GE)
AU-LOP (VCMON-HP)	LOM (VCTRM-LP)	SQUELCHED (ISC)
AU-LOP (VCTRM-HP)	LO-RXPOWER (2R)	SQUELCHED (STMN)
AUTOLSROFF (STMN)	LO-RXPOWER (ESCON)	SQUELCHED (TRUNK)
AUTOLSROFF (TRUNK)	LO-RXPOWER (FC)	SSM-DUS (BITS)
AUTORESET (EQPT)	LO-RXPOWER (GE)	SSM-DUS (E1)
AUTOSW-AIS-SNCP (VCMON-HP)	LO-RXPOWER (ISC)	SSM-DUS (STMN)
AUTOSW-AIS-SNCP (VCMON-LP)	LO-RXPOWER (STMN)	SSM-DUS (TRUNK)
AUTOSW-LOP-SNCP (VCMON-HP)	LO-RXPOWER (TRUNK)	SSM-FAIL (BITS)
AUTOSW-LOP-SNCP (VCMON-LP)	LOS (2R)	SSM-FAIL (E1)

Table 2-6 ONS 15454 SDH Alarm and Condition Alphabetical List (continued)

—	LOS (BITS)	SSM-FAIL (STMN)
AUTOSW-SDBER-SNCP (VCMON-HP)	LOS (DS1)	SSM-FAIL (TRUNK)
AUTOSW-SFBER-SNCP (VCMON-HP)	LOS (DS3)	SSM-LNC (BITS)
AUTOSW-UNEQ-SNCP (VCMON-HP)	LOS (E1)	SSM-LNC (NE-SREF)
AUTOSW-UNEQ-SNCP (VCMON-LP)	LOS (E3)	SSM-LNC (STMN)
AWG-DEG (OTS)	LOS (E4)	SSM-LNC (TRUNK)
AWG-FAIL (OTS)	LOS (ESCON)	SSM-OFF (BITS)
AWG-OVERTEMP (OTS)	LOS (FUDC)	SSM-OFF (E1)
AWG-WARM-UP (OTS)	LOS (ISC)	SSM-OFF (STMN)
BAT-FAIL (PWR)	LOS (MSUDC)	SSM-OFF (TRUNK)
BKUPMEMP (EQPT)	LOS (OTS)	SSM-PRC (BITS)
CARLOSS (CE100T)	LOS (STM1E)	SSM-PRC (NE-SREF)
CARLOSS (E1000F)	LOS (STMN)	SSM-PRC (STMN)
CARLOSS (E100T)	LOS (TRUNK)	SSM-PRC (TRUNK)
CARLOSS (EQPT)	LOS-O (OCH)	SSM-PRS (E1)
CARLOSS (FC)	LOS-O (OMS)	SSM-PRS (TRUNK)
CARLOSS (G1000)	LOS-O (OTS)	SSM-RES (E1)
CARLOSS (GE)	LOS-P (OCH)	SSM-RES (TRUNK)
CARLOSS (ISC)	LOS-P (OMS)	SSM-SDH-TN (BITS)
CARLOSS (ML1000)	LOS-P (OTS)	SSM-SDH-TN (NE-SREF)
CARLOSS (ML100T)	LOS-P (TRUNK)	SSM-SDH-TN (STMN)
CARLOSS (MLFX)	LO-TXPOWER (2R)	SSM-SDH-TN (TRUNK)
CARLOSS (TRUNK)	LO-TXPOWER (EQPT)	SSM-SETS (BITS)
CASETEMP-DEG (AOTS)	LO-TXPOWER (ESCON)	SSM-SETS (NE-SREF)
CLDRESTART (EQPT)	LO-TXPOWER (FC)	SSM-SETS (STMN)
COMIOXC (EQPT)	LO-TXPOWER (GE)	SSM-SETS (TRUNK)
COMM-FAIL (EQPT)	LO-TXPOWER (ISC)	SSM-SMC (E1)
CONTBUS-A-18 (EQPT)	LO-TXPOWER (PPM)	SSM-SMC (TRUNK)
CONTBUS-B-18 (EQPT)	LO-TXPOWER (STMN)	SSM-ST2 (E1)
CONTBUS-DISABLED (EQPT)	LO-TXPOWER (TRUNK)	SSM-ST2 (TRUNK)
CONTBUS-IO-A (EQPT)	LPBKDS1FEAC-CMD (DS1)	SSM-ST3 (E1)
CONTBUS-IO-B (EQPT)	LPBKDS3FEAC (DS3)	SSM-ST3 (TRUNK)
CTNEQPT-MISMATCH (EQPT)	LPBKDS3FEAC-CMD (DS3)	SSM-ST3E (E1)
CTNEQPT-PBPROT (EQPT)	LPBKDS3FEAC-CMD (E3)	SSM-ST3E (TRUNK)
CTNEQPT-PBWORK (EQPT)	LPBKE1FEAC (E3)	SSM-ST4 (E1)
DATAFLT (NE)	LPBKE3FEAC (E3)	SSM-ST4 (STMN)
DBOSYNC (NE)	LPBKFACILITY (CE100T)	SSM-ST4 (TRUNK)

Table 2-6 ONS 15454 SDH Alarm and Condition Alphabetical List (continued)

DS3-MISM (DS3)	LPBKFACILITY (DS1)	SSM-STU (BITS)
DSP-COMM-FAIL (TRUNK)	LPBKFACILITY (DS3)	SSM-STU (E1)
DSP-FAIL (TRUNK)	LPBKFACILITY (E1)	SSM-STU (NE-SREF)
DUP-IPADDR (NE)	LPBKFACILITY (E3)	SSM-STU (STMN)
DUP-NODEME (NE)	LPBKFACILITY (E4)	SSM-STU (TRUNK)
EHIBATVG (PWR)	LPBKFACILITY (ESCON)	SSM-TNC (STMN)
ELWBATVG (PWR)	LPBKFACILITY (FC)	SSM-TNC (TRUNK)
EOC (STMN)	LPBKFACILITY (FCMR)	SW-MISMATCH (EQPT)
EOC (TRUNK)	LPBKFACILITY (G1000)	SWMTXMOD-PROT (EQPT)
EOC-L (TRUNK)	LPBKFACILITY (GE)	SWMTXMOD-WORK (EQPT)
EQPT (AICI-AEP)	LPBKFACILITY (ISC)	SWTOPRI (EXT-SREF)
EQPT (AICI-AIE)	LPBKFACILITY (STM1E)	SWTOPRI (NE-SREF)
EQPT (EQPT)	LPBKFACILITY (STMN)	SWTOSEC (EXT-SREF)
EQPT (PPM)	LPBKFACILITY (TRUNK)	SWTOSEC (NE-SREF)
EQPT-MISS (FAN)	LPBKCRS (VCMON-HP)	SWTOTHIRD (EXT-SREF)
ERROR-CONFIG (EQPT)	LPBKCRS (VCTRM-HP)	SWTOTHIRD (NE-SREF)
ETH-LINKLOSS (NE)	LPBKTERMINAL (STM1E)	SYNC-FREQ (E1)
E-W-MISMATCH (STMN)	LPBKTERMINAL (STMN)	SYNC-FREQ (STMN)
EXCCOL (EQPT)	LPBKTERMINAL (CE100T)	SYNC-FREQ (TRUNK)
EXERCISE-RING-FAIL (STMN)	LPBKTERMINAL (DS1)	SYNCLOSS (FC)
EXERCISE-SPAN-FAIL (STMN)	LPBKTERMINAL (DS3)	SYNCLOSS (FCMR)
EXT (ENVALRM)	LPBKTERMINAL (E1)	SYNCLOSS (GE)
EXTRA-TRAF-PREEMPT (STMN)	LPBKTERMINAL (E3)	SYNCLOSS (ISC)
FAILTOSW (2R)	LPBKTERMINAL (E4)	SYNCLOSS (TRUNK)
FAILTOSW (EQPT)	LPBKTERMINAL (ESCON)	SYNCPRI (EXT-SREF)
FAILTOSW (ESCON)	LPBKTERMINAL (FC)	SYNCPRI (NE-SREF)
FAILTOSW (FC)	LPBKTERMINAL (FCMR)	SYNCSEC (EXT-SREF)
FAILTOSW (GE)	LPBKTERMINAL (G1000)	SYNCSEC (NE-SREF)
FAILTOSW (ISC)	LPBKTERMINAL (GE)	SYNCTHIRD (EXT-SREF)
FAILTOSW (STMN)	LPBKTERMINAL (ISC)	SYNCTHIRD (NE-SREF)
FAILTOSW (TRUNK)	LPBKTERMINAL (TRUNK)	SYSBOOT (NE)
FAILTOSW-HO (VCMON-HP)	LP-ENCAP-MISMATCH (VCTRM-LP)	TEMP-MISM (NE)
FAILTOSW-LO (VCMON-LP)	LP-PLM (VCTRM-LP)	TIM (STM1E)
FAILTOSWR (STMN)	LP-RFI (VCTRM-LP)	TIM (STMN)
FAILTOSWS (STMN)	LP-TIM (VCTRM-LP)	TIM (TRUNK)
FAN (FAN)	LP-UNEQ (VCMON-LP)	TIM-MON (STMN)

Table 2-6 ONS 15454 SDH Alarm and Condition Alphabetical List (continued)

FC-NO-CREDITS (FC)	LP-UNEQ (VCTRM-LP)	TIM-MON (TRUNK)
FC-NO-CREDITS (FCMR)	MANRESET (EQPT)	TPTFAIL (CE100T)
FC-NO-CREDITS (TRUNK)	MAN-REQ (EQPT)	TPTFAIL (FCMR)
FE-AIS (E3)	MAN-REQ (VCMON-HP)	TPTFAIL (G1000)
FEC-MISM (TRUNK)	MAN-REQ (VCMON-LP)	TPTFAIL (ML1000)
FE-E1-MULTLOS (E3)	MANSWTOINT (NE-SREF)	TPTFAIL (ML100T)
FE-E1-NSA (E3)	MANSWTOPRI (EXT-SREF)	TPTFAIL (MLFX)
FE-E1-SA (E3)	MANSWTOPRI (NE-SREF)	TRMT (DS1)
FE-E1-SNGLLOS (E3)	MANSWTOSEC (EXT-SREF)	TRMT (E1)
FE-E3-NSA (E3)	MANSWTOSEC (NE-SREF)	TRMT-MISS (DS1)
FE-E3-SA (E3)	MANSWTOTHIRD (EXT-SREF)	TRMT-MISS (E1)
FE-EQPT-NSA (E3)	MANSWTOTHIRD (NE-SREF)	TU-AIS (VCMON-LP)
FE-FRCDWKSWBK-SPAN (STMN)	MANUAL-REQ-RING (STMN)	TU-AIS (VCTRM-LP)
FE-FRCDWKSWPR-RING (STMN)	MANUAL-REQ-SPAN (2R)	TU-LOP (VCMON-LP)
FE-FRCDWKSWPR-SPAN (STMN)	MANUAL-REQ-SPAN (ESCON)	TU-LOP (VCTRM-LP)
FE-IDLE (E3)	MANUAL-REQ-SPAN (FC)	TX-AIS (DS1)
FE-LOCKOUTOFPR-SPAN (STMN)	MANUAL-REQ-SPAN (GE)	TX-AIS (DS3)
FE-LOF (E3)	MANUAL-REQ-SPAN (ISC)	TX-AIS (E1)
FE-LOS (E3)	MANUAL-REQ-SPAN (STMN)	TX-AIS (E3)
FE-MANWKSWBK-SPAN (STMN)	MANUAL-REQ-SPAN (TRUNK)	TX-LOF (DS1)
FE-MANWKSWPR-RING (STMN)	MEA (BIC)	TX-LOF (E1)
FE-MANWKSWPR-SPAN (STMN)	MEA (EQPT)	TX-RAI (DS1)
FEPRLF (STMN)	MEA (FAN)	TX-RAI (E1)
FIBERTEMP-DEG (AOTS)	MEA (PPM)	TX-RAI (E3)
FORCED-REQ (EQPT)	MEM-GONE (EQPT)	UNC-WORD (TRUNK)
FORCED-REQ (VCMON-HP)	MEM-LOW (EQPT)	UNREACHABLE-TARGET-POWER (OCH)
FORCED-REQ (VCMON-LP)	MFGMEM (AICI-AEP)	UT-COMM-FAIL (TRUNK)
FORCED-REQ-RING (STMN)	MFGMEM (AICI-AIE)	UT-FAIL (TRUNK)
FORCED-REQ-SPAN (2R)	MFGMEM (BPLANE)	VCG-DEG (VCG)
FORCED-REQ-SPAN (ESCON)	MFGMEM (FAN)	VCG-DOWN (VCG)
FORCED-REQ-SPAN (FC)	MFGMEM (PPM)	VOA-HDEG (AOTS)
FORCED-REQ-SPAN (GE)	MS-AIS (STM1E)	VOA-HDEG (OCH)
FORCED-REQ-SPAN (ISC)	MS-AIS (STMN)	VOA-HDEG (OMS)
FORCED-REQ-SPAN (STMN)	MS-EOC (STMN)	VOA-HDEG (OTS)
FORCED-REQ-SPAN (TRUNK)	MS-RFI (STM1E)	VOA-HFAIL (AOTS)
FRCDSWTOINT (NE-SREF)	MS-RFI (STMN)	VOA-HFAIL (OCH)

Table 2-6 ONS 15454 SDH Alarm and Condition Alphabetical List (continued)

FRCDSWTOPRI (EXT-SREF)	MSSP-OOSYNC (STMN)	VOA-HFAIL (OMS)
FRCDSWTOPRI (NE-SREF)	MSSP-SW-VER-MISM (STMN)	VOA-HFAIL (OTS)
FRCDSWTOSEC (EXT-SREF)	NO-CONFIG (EQPT)	VOA-LDEG (AOTS)
FRCDSWTOSEC (NE-SREF)	NOT-AUTHENTICATED	VOA-LDEG (OCH)
FRCDSWTOTHIRD (EXT-SREF)	OCHNC-INC (OCHNC-CONN)	VOA-LDEG (OMS)
FRCDSWTOTHIRD (NE-SREF)	ODUK-1-AIS-PM (TRUNK)	VOA-LDEG (OTS)
FRNGSYNC (NE-SREF)	ODUK-2-AIS-PM (TRUNK)	VOA-LFAIL (AOTS)
FSTSYNC (NE-SREF)	ODUK-3-AIS-PM (TRUNK)	VOA-LFAIL (OCH)
FULLPASSTHR-BI (STMN)	ODUK-4-AIS-PM (TRUNK)	VOA-LFAIL (OMS)
GAIN-HDEG (AOTS)	ODUK-AIS-PM (TRUNK)	VOA-LFAIL (OTS)
GAIN-HFAIL (AOTS)	ODUK-BDI-PM (TRUNK)	VOLT-MISM (PWR)
GAIN-LDEG (AOTS)	ODUK-LCK-PM (TRUNK)	WKSWPR (2R)
GAIN-LFAIL (AOTS)	ODUK-OCI-PM (TRUNK)	WKSWPR (EQPT)
GCC-EOC (TRUNK)	ODUK-SD-PM (TRUNK)	WKSWPR (ESCON)
GE-OOSYNC (FC)	ODUK-SF-PM (TRUNK)	WKSWPR (FC)
GE-OOSYNC (GE)	ODUK-TIM-PM (TRUNK)	WKSWPR (GE)
GE-OOSYNC (ISC)	OOU-TPT (VCTRM-HP)	WKSWPR (ISC)
GE-OOSYNC (TRUNK)	OOU-TPT (VCTRM-LP)	WKSWPR (STMN)
GFP-CSF (CE100T)	OPTNTWMIS (NE)	WKSWPR (TRUNK)
GFP-CSF (FCMR)	OPWR-HDEG (AOTS)	WKSWPR (VCMON-HP)
GFP-CSF (GFP-FAC)	OPWR-HDEG (OCH)	WKSWPR (VCMON-LP)
GFP-CSF (ML1000)	OPWR-HDEG (OMS)	WTR (2R)
GFP-CSF (ML100T)	OPWR-HDEG (OTS)	WTR (EQPT)
GFP-CSF (MLFX)	OPWR-HFAIL (AOTS)	WTR (ESCON)
GFP-DE-MISMATCH (FCMR)	OPWR-HFAIL (OCH)	WTR (FC)
GFP-DE-MISMATCH (GFP-FAC)	OPWR-HFAIL (OMS)	WTR (GE)
GFP-EX-MISMATCH (FCMR)	OPWR-HFAIL (OTS)	WTR (ISC)
GFP-EX-MISMATCH (GFP-FAC)	OPWR-LDEG (AOTS)	WTR (STMN)
GFP-LFD (CE100T)	OPWR-LDEG (OCH)	WTR (TRUNK)
GFP-LFD (FCMR)	OPWR-LDEG (OMS)	WTR (VCMON-HP)
GFP-LFD (GFP-FAC)	OPWR-LDEG (OTS)	WTR (VCMON-LP)
GFP-LFD (ML1000)	OPWR-LFAIL (AOTS)	WVL-MISMATCH (TRUNK)
GFP-LFD (ML100T)	—	—

2.3 Alarm 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 SDH 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 (STM-N) or the optical transport layer overhead (OTN) as well as other objects. Therefore, both STM-N: LOS and OTN: LOS appear in the list (as well as the other objects).

Alarm profile list objects are defined in Table 2-7.

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

Table 2-7 Alarm Logical Object Type Definitions

Object Type	Definition
2R	Reshape and retransmit (used for transponder [TXP] cards).
AICI-AEP	Alarm Interface Controller–International—Alarm expansion panel.
AIP	Alarm Interface Panel.
AOTS	Amplified optical transport section.
BIC	Backplane interface connector.
BITS	Building integrated timing supply incoming references (BITS-1, BITS-2).
BPLANE	The backplane.
DS3	A DS-3 signal on a DS3i-N-12 card.
E1	E1-42 card.
E3	E3-12 card.
E4	Line type supported by the STM1E card.
E1000F	An E1000-2-G card.
E100T	An E100T-G card.
ENVALRM	An environmental alarm port.
EQPT	A card, its physical objects, and 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, STM, and VC.
ESCON	Enterprise System Connection fiber optic technology, referring to the following TXP cards: TXP_MR_2.5G, TXPP_MR_2.5G.
EXT-SREF	BITS outgoing references (SYNC-BITS1, SYNC-BITS2).
FAN	Fan-tray assembly.
FC	Fibre Channel data transfer architecture, referring to the following muxponder (MXP) or TXP cards: MXP_MR_2.5G, MXPP_MR_2.5G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E.
FCMR	An FC_MR-4 Fibre Channel card.

Table 2-7 Alarm Logical Object Type Definitions (continued)

Object Type	Definition
FUDC	SDH F1 byte user data channel for ONS 15454 SDH ML-Series Ethernet cards.
G1000	The ONS 15454 SDH G-Series card.
GE	Gigabit Ethernet, referring to the following MXP or TXP cards: MXP_MR_2.5G, MXPP_MR_2.5G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, TXP_MR_10G.
GFP-FAC	Generic framing procedure facility port, referring to all MXP and TXP cards.
ISC	Inter-service channel referring to MXP and TXP cards.
ML1000	The ONS 15454 SDH ML1000-2 card.
ML100T	The ONS 15454 SDH ML100T-2 or ML100T-8 card.
MLFX	An MLFX Ethernet card.
MSUDC	Multiplex section user data channel.
NE	The entire network element.
NE-SREF	The timing status of the NE.
OCH	The optical channel, referring to a dense wavelength division multiplexing (DWDM) cards.
OCHNC-CONN	The optical channel network connection, referring to DWDM cards.
OMS	Optical multiplex section.
OTS	Optical transport section.
PWR	Power equipment.
PPM	Pluggable port module (PPM), referring to all MXP and TXP cards, MRC-12 cards, and OC192-XFP/STM64-XFP cards.
STM1E	Synchronous transfer mode 1 (speed) electrical interface
STMN	An STM-N line on an STM-N card.
VCTRM-HP	VT alarm detection at termination (downstream from the cross-connect).
TRUNK	The optical or DWDM card carrying the high-speed signal; referring to MXP, TXP, or ML-Series cards.
UCP-CKT	Unified control plane circuit.
UCP-IPCC	Unified control plane IP control channel.
UCP-NBR	Unified control plane neighbor.
VCG	ONS 15454 SDH virtual concatenation group of virtual tributaries (VT).
VCMON-HP	High-order path virtual concatenation monitoring.
VCMON-LP	VT1 alarm detection at the monitor point (upstream from the cross-connect).
VCTRM-HP	Low-order path virtual concatenation monitoring.
VCTRM-LP	VC alarm detection at termination (downstream from the cross-connect).

2.4 Alarm List by Logical Object Type

Table 2-8 lists all ONS 15454 SDH Release 6.0 alarms and logical objects as they are given in the system alarm profile. The list entries are organized by logical object name and then by alarm or condition name. Where appropriate, the alarm entries also contain troubleshooting procedures.

Note In a mixed network containing different types of nodes (such as ONS 15310-CL, ONS 15454 SDH, and ONS 15600), the initially displayed alarm list in the Provisioning > Alarm Profiles > Alarm Profile Editor tab lists all conditions that are applicable to all nodes in the network. However, when you load the default severity profile from a node, only applicable alarms will display severity levels. Nonapplicable alarms can display "use default" or "unset."

Note In some cases this list does not follow alphabetical order, but it does reflect the order shown in CTC.

Table 2-8 Alarm List by Logical Object Type in Alarm Profile

2R: ALS	FAN: MFGMEM	STM1E: MS-AIS
2R: AS-CMD	FC: ALS	STM1E: MS-RFI
2R: AS-MT	FC: AS-CMD	STM1E: SD
2R: FAILTOSW	FC: AS-MT	STM1E: SD-L
2R: FORCED-REQ-SPAN	FC: CARLOSS	STM1E: SF-L
2R: HI-LASERBIAS	FC: FAILTOSW	STM1E: TIM
2R: HI-RXPOWER	FC: FC-NO-CREDITS	STMN: ALS
2R: HI-TXPOWER	FC: FORCED-REQ-SPAN	STMN: APS-INV-PRIM
2R: LO-RXPOWER	FC: GE-OOSYNC	STMN: APS-PRIM-FAC
2R: LO-TXPOWER	FC: HI-LASERBIAS	STMN: APS-PRIM-SEC-MISM
2R: LOCKOUT-REQ	FC: HI-RXPOWER	STMN: APSB
2R: LOS	FC: HI-TXPOWER	STMN: APSC-IMP
2R: MANUAL-REQ-SPAN	FC: LO-RXPOWER	STMN: APSCDFLTK
2R: SQUELCHED	FC: LO-TXPOWER	STMN: APSCINCON
2R: WKSWPR	FC: LOCKOUT-REQ	STMN: APSCM
2R: WTR	FC: LPBKFACILITY	STMN: APSCNMIS
AICI-AEP: EQPT	FC: LPBKTERMINAL	STMN: APSIMP
AICI-AEP: MFGMEM	FC: MANUAL-REQ-SPAN	STMN: APSMM
AICI-AIE: EQPT	FC: OUT-OF-SYNC	STMN: AS-CMD
AICI-AIE: MFGMEM	FC: SIGLOSS	STMN: AS-MT
AOTS: ALS	FC: SQUELCHED	STMN: AUTOLSROFF
AOTS: AMPLI-INIT	FC: SYNCLOSS	STMN: E-W-MISMATCH
AOTS: APC-CORRECTION-SKIPPED	FC: WKSWPR	STMN: EOC
AOTS: APC-OUT-OF-RANGE	FC: WTR	STMN: EXERCISE-RING-FAIL

Table 2-8 Alarm List by Logical Object Type in Alarm Profile (continued)

AOTS: AS-CMD	FCMR: AS-CMD	STMN: EXERCISE-SPAN-FAIL
AOTS: AS-MT	FCMR: AS-MT	STMN: EXTRA-TRAF-PREEMPT
AOTS: CASETEMP-DEG	FCMR: FC-NO-CREDITS	STMN: FAILTOSW
AOTS: FIBERTEMP-DEG	FCMR: GFP-CSF	STMN: FAILTOSWR
AOTS: GAIN-HDEG	FCMR: GFP-DE-MISMATCH	STMN: FAILTOSWS
AOTS: GAIN-HFAIL	FCMR: GFP-EX-MISMATCH	STMN: FE-FRCDWKSWBK-SPAN
AOTS: GAIN-LDEG	FCMR: GFP-LFD	STMN: FE-FRCDWKSWPR-RING
AOTS: GAIN-LFAIL	FCMR: GFP-NO-BUFFERS	STMN: FE-FRCDWKSWPR-SPAN
AOTS: LASER-APR	FCMR: GFP-UP-MISMATCH	STMN: FE-LOCKOUTOFPR-SPAN
AOTS: LASERBIAS-DEG	FCMR: LPBKFACILITY	STMN: FE-MANWKSWBK-SPAN
AOTS: LASERBIAS-FAIL	FCMR: LPBKTERMINAL	STMN: FE-MANWKSWPR-RING
AOTS: LASERTEMP-DEG	FCMR: PORT-MISMATCH	STMN: FE-MANWKSWPR-SPAN
AOTS: OPWR-HDEG	FCMR: SIGLOSS	STMN: FEPRLF
AOTS: OPWR-HFAIL	FCMR: SYNCLOSS	STMN: FORCED-REQ-RING
AOTS: OPWR-LDEG	FCMR: TPTFAIL	STMN: FORCED-REQ-SPAN
AOTS: OPWR-LFAIL	FUDC: AIS	STMN: FULLPASSTHR-BI
AOTS: OSRION	FUDC: LOS	STMN: HELLO
AOTS: PARAM-MISM	G1000: AS-CMD	STMN: HI-LASERBIAS
AOTS: VOA-HDEG	G1000: AS-MT	STMN: HI-LASERTEMP
AOTS: VOA-HFAIL	G1000: CARLOSS	STMN: HI-RXPOWER
AOTS: VOA-LDEG	G1000: LPBKFACILITY	STMN: HI-TXPOWER
AOTS: VOA-LFAIL	G1000: LPBKTERMINAL	STMN: ISIS-ADJ-FAIL
BIC: MEA	G1000: TPTFAIL	STMN: KB-PASSTHR
BITS: AIS	GE: ALS	STMN: KBYTE-APS-CHANNEL-FAILURE
BITS: LOF	GE: AS-CMD	STMN: LKOUTPR-S
BITS: LOS	GE: AS-MT	STMN: LO-LASERBIAS
BITS: SSM-DUS	GE: CARLOSS	STMN: LO-LASERTEMP
BITS: SSM-FAIL	GE: FAILTOSW	STMN: LO-RXPOWER
BITS: SSM-LNC	GE: FORCED-REQ-SPAN	STMN: LO-TXPOWER
BITS: SSM-OFF	GE: GE-OOSYNC	STMN: LOCKOUT-REQ
BITS: SSM-PRC	GE: HI-LASERBIAS	STMN: LOF
BITS: SSM-SDH-TN	GE: HI-RXPOWER	STMN: LOS
BITS: SSM-SETS	GE: HI-TXPOWER	STMN: LPBKFACILITY
BITS: SSM-STU	GE: LO-RXPOWER	STMN: LPBKTERMINAL
BPLANE: AS-CMD	GE: LO-TXPOWER	STMN: MANUAL-REQ-RING
BPLANE: INVMACADR	GE: LOCKOUT-REQ	STMN: MANUAL-REQ-SPAN

Table 2-8 Alarm List by Logical Object Type in Alarm Profile (continued)

BPLANE: MFGMEM	GE: LPBKFACILITY	STMN: MS-AIS
CE100T: AS-CMD	GE: LPBKTERMINAL	STMN: MS-EOC
CE100T: AS-MT	GE: MANUAL-REQ-SPAN	STMN: MS-RFI
CE100T: CARLOSS	GE: OUT-OF-SYNC	STMN: MSSP-OOSYNC
CE100T: GFP-CSF	GE: SIGLOSS	STMN: MSSP-SW-VER-MISM
CE100T: GFP-LFD	GE: SQUELCHED	STMN: PRC-DUPID
CE100T: GFP-UP-MISMATCH	GE: SYNCLOSS	STMN: RING-ID-MIS
CE100T: LPBKFACILITY	GE: WKSWPR	STMN: RING-MISMATCH
CE100T: LPBKTERMINAL	GE: WTR	STMN: RING-SW-EAST
CE100T: TPTFAIL	GFP-FAC: AS-CMD	STMN: RING-SW-WEST
DS1: AIS	GFP-FAC: AS-MT	STMN: RS-TIM
DS1: AS-CMD	GFP-FAC: GFP-CSF	STMN: SD
DS1: AS-MT	GFP-FAC: GFP-DE-MISMATCH	STMN: SF
DS1: LOF	GFP-FAC: GFP-EX-MISMATCH	STMN: SPAN-SW-EAST
DS1: LOS	GFP-FAC: GFP-LFD	STMN: SPAN-SW-WEST
DS1: LPBKDS1FEAC-CMD	GFP-FAC: GFP-NO-BUFFERS	STMN: SQUELCH
DS1: LPBKFACILITY	GFP-FAC: GFP-UP-MISMATCH	STMN: SQUELCHED
DS1: LPBKTERMINAL	ISC: ALS	STMN: SSM-DUS
DS1: RAI	ISC: AS-CMD	STMN: SSM-FAIL
DS1: RCVR-MISS	ISC: AS-MT	STMN: SSM-LNC
DS1: SD	ISC: CARLOSS	STMN: SSM-OFF
DS1: SF	ISC: FAILTOSW	STMN: SSM-PRC
DS1: TRMT	ISC: FORCED-REQ-SPAN	STMN: SSM-SDH-TN
DS1: TRMT-MISS	ISC: GE-OOSYNC	STMN: SSM-SETS
DS1: TX-AIS	ISC: HI-LASERBIAS	STMN: SSM-ST4
DS1: TX-LOF	ISC: HI-RXPOWER	STMN: SSM-STU
DS1: TX-RAI	ISC: HI-TXPOWER	STMN: SSM-TNC
DS3: AIS	ISC: LO-RXPOWER	STMN: SYNC-FREQ
DS3: AS-CMD	ISC: LO-TXPOWER	STMN: TIM
DS3: AS-MT	ISC: LOCKOUT-REQ	STMN: TIM-MON
DS3: DS3-MISM	ISC: LOS	STMN: WKSWPR
DS3: INC-ISD	ISC: LPBKFACILITY	STMN: WTR
DS3: LOF	ISC: LPBKTERMINAL	TRUNK: AIS
DS3: LOS	ISC: MANUAL-REQ-SPAN	TRUNK: AIS-L
DS3: LPBKDS3FEAC	ISC: OUT-OF-SYNC	TRUNK: ALS
DS3: LPBKDS3FEAC-CMD	ISC: SIGLOSS	TRUNK: AS-CMD
DS3: LPBKFACILITY	ISC: SQUELCHED	TRUNK: AS-MT

Table 2-8 Alarm List by Logical Object Type in Alarm Profile (continued)

DS3: LPBKTERMINAL	ISC: SYNCLOSS	TRUNK: AUTOLSROFF
DS3: RAI	ISC: WKSWPR	TRUNK: CARLOSS
DS3: SD	ISC: WTR	TRUNK: DSP-COMM-FAIL
DS3: SF	ML1000: AS-CMD	TRUNK: DSP-FAIL
DS3: TX-AIS	ML1000: AS-MT	TRUNK: EOC
E1000F: AS-CMD	ML1000: CARLOSS	TRUNK: EOC-L
E1000F: CARLOSS	ML1000: GFP-CSF	TRUNK: FAILTOSW
E100T: AS-CMD	ML1000: GFP-LFD	TRUNK: FC-NO-CREDITS
E100T: CARLOSS	ML1000: GFP-UP-MISMATCH	TRUNK: FEC-MISM
E1: AIS	ML1000: RPRW	TRUNK: FORCED-REQ-SPAN
E1: AS-CMD	ML1000: TPTFAIL	TRUNK: GCC-EOC
E1: AS-MT	ML100T: AS-CMD	TRUNK: GE-OOSYNC
E1: LOF	ML100T: AS-MT	TRUNK: HI-LASERBIAS
E1: LOS	ML100T: CARLOSS	TRUNK: HI-RXPOWER
E1: LPBKFACILITY	ML100T: GFP-CSF	TRUNK: HI-TXPOWER
E1: LPBKTERMINAL	ML100T: GFP-LFD	TRUNK: LO-RXPOWER
E1: RAI	ML100T: GFP-UP-MISMATCH	TRUNK: LO-TXPOWER
E1: RCVR-MISS	ML100T: RPRW	TRUNK: LOCKOUT-REQ
E1: SD	ML100T: TPTFAIL	TRUNK: LOF
E1: SF	MLFX: AS-CMD	TRUNK: LOM
E1: SSM-DUS	MLFX: AS-MT	TRUNK: LOS
E1: SSM-FAIL	MLFX: CARLOSS	TRUNK: LOS-P
E1: SSM-OFF	MLFX: GFP-CSF	TRUNK: LPBKFACILITY
E1: SSM-PRS	MLFX: GFP-LFD	TRUNK: LPBKTERMINAL
E1: SSM-RES	MLFX: GFP-UP-MISMATCH	TRUNK: MANUAL-REQ-SPAN
E1: SSM-SMC	MLFX: RPRW	TRUNK: ODUK-1-AIS-PM
E1: SSM-ST2	MLFX: TPTFAIL	TRUNK: ODUK-2-AIS-PM
E1: SSM-ST3	MSUDC: AIS	TRUNK: ODUK-3-AIS-PM
E1: SSM-ST3E	MSUDC: LOS	TRUNK: ODUK-4-AIS-PM
E1: SSM-ST4	NE-SREF: FRCDSWTOINT	TRUNK: ODUK-AIS-PM
E1: SSM-STU	NE-SREF: FRCDSWTOPRI	TRUNK: ODUK-BDI-PM
E1: SYNC-FREQ	NE-SREF: FRCDSWTOSEC	TRUNK: ODUK-LCK-PM
E1: TRMT	NE-SREF: FRCDSWTOTHIRD	TRUNK: ODUK-OCI-PM
E1: TRMT-MISS	NE-SREF: FRNGSYNC	TRUNK: ODUK-SD-PM
E1: TX-AIS	NE-SREF: FSTSYNC	TRUNK: ODUK-SF-PM
E1: TX-LOF	NE-SREF: HLDOVRSYNC	TRUNK: ODUK-TIM-PM
E1: TX-RAI	NE-SREF: MANSWTOINT	TRUNK: OTUK-AIS

Table 2-8 Alarm List by Logical Object Type in Alarm Profile (continued)

E3: AIS	NE-SREF: MANSWTOPRI	TRUNK: OTUK-BDI
E3: AS-CMD	NE-SREF: MANSWTOSEC	TRUNK: OTUK-IAE
E3: AS-MT	NE-SREF: MANSWTOTHIRD	TRUNK: OTUK-LOF
E3: FE-AIS	NE-SREF: SSM-LNC	TRUNK: OTUK-SD
E3: FE-E1-MULTLOS	NE-SREF: SSM-PRC	TRUNK: OTUK-SF
E3: FE-E1-NSA	NE-SREF: SSM-SDH-TN	TRUNK: OTUK-TIM
E3: FE-E1-SA	NE-SREF: SSM-SETS	TRUNK: OUT-OF-SYNC
E3: FE-E1-SNGLLOS	NE-SREF: SSM-STU	TRUNK: PTIM
E3: FE-E3-NSA	NE-SREF: SWTOPRI	TRUNK: RFI
E3: FE-E3-SA	NE-SREF: SWTOSEC	TRUNK: SD
E3: FE-EQPT-NSA	NE-SREF: SWTOTHIRD	TRUNK: SF
E3: FE-IDLE	NE-SREF: SYNCPRI	TRUNK: SIGLOSS
E3: FE-LOF	NE-SREF: SYNCSEC	TRUNK: SQUELCHED
E3: FE-LOS	NE-SREF: SYNCTHIRD	TRUNK: SSM-DUS
E3: INC-ISD	NE: APC-DISABLED	TRUNK: SSM-FAIL
E3: LOS	NE: APC-END	TRUNK: SSM-LNC
E3: LPBKDS3FEAC-CMD	NE: AS-CMD	TRUNK: SSM-OFF
E3: LPBKE1FEAC	NE: AUD-LOG-LOSS	TRUNK: SSM-PRC
E3: LPBKE3FEAC	NE: AUD-LOG-LOW	TRUNK: SSM-PRS
E3: LPBKFACILITY	NE: DATAFLT	TRUNK: SSM-RES
E3: LPBKTERMINAL	NE: DBOSYNC	TRUNK: SSM-SDH-TN
E3: SD	NE: DUP-IPADDR	TRUNK: SSM-SETS
E3: SF	NE: DUP-NODEME	TRUNK: SSM-SMC
E3: TX-AIS	NE: ETH-LINKLOSS	TRUNK: SSM-ST2
E3: TX-RAI	NE: HITEMP	TRUNK: SSM-ST3
E4: AIS	NE: I-HITEMP	TRUNK: SSM-ST3E
E4: AS-CMD	NE: INTRUSION-PSWD	TRUNK: SSM-ST4
E4: AS-MT	NE: LAN-POL-REV	TRUNK: SSM-STU
E4: LOF	NE: OPTNTWMIS	TRUNK: SSM-TNC
E4: LOS	NE: SNTP-HOST	TRUNK: SYNC-FREQ
E4: LPBKFACILITY	NE: SYSBOOT	TRUNK: SYNCLOSS
E4: LPBKTERMINAL	NE: TEMP-MISM	TRUNK: TIM
E4: SD	OCH: APC-CORRECTION-SKIPPED	TRUNK: TIM-MON
E4: SF	OCH: APC-OUT-OF-RANGE	TRUNK: UNC-WORD
ENVALRM: EXT	OCH: AS-CMD	TRUNK: UT-COMM-FAIL
EQPT: AS-CMD	OCH: AS-MT	TRUNK: UT-FAIL
EQPT: AS-MT	OCH: LOS-O	TRUNK: WKSWPR

Table 2-8 Alarm List by Logical Object Type in Alarm Profile (continued)

EQPT: AUTORESET	OCH: LOS-P	TRUNK: WTR
EQPT: BKUPMEMP	OCH: OPWR-HDEG	TRUNK: WVL-MISMATCH
EQPT: CARLOSS	OCH: OPWR-HFAIL	VCG: LOA
EQPT: CLDRESTART	OCH: OPWR-LDEG	VCG: VCG-DEG
EQPT: COMIOXC	OCH: OPWR-LFAIL	VCG: VCG-DOWN
EQPT: COMM-FAIL	OCH: PARAM-MISM	VCMON-HP: AU-AIS
EQPT: CONTBUS-A-18	OCH: PORT-ADD-PWR-DEG-HI	VCMON-HP: AU-LOP
EQPT: CONTBUS-B-18	OCH: PORT-ADD-PWR-DEG-LOW	VCMON-HP: AUTOSW-AIS-SNCP
EQPT: CONTBUS-DISABLED	OCH: PORT-ADD-PWR-FAIL-HIGH	VCMON-HP: AUTOSW-LOP-SNCP
EQPT: CONTBUS-IO-A	OCH: PORT-ADD-PWR-FAIL-LOW	—
EQPT: CONTBUS-IO-B	OCH: PORT-FAIL	VCMON-HP: AUTOSW-SDBER-SNCP
EQPT: CTNEQPT-MISMATCH	OCH: UEACHABLE-TARGET-POWER	VCMON-HP: AUTOSW-SFBER-SNCP
EQPT: CTNEQPT-PBPROT	OCH: VOA-HDEG	VCMON-HP: AUTOSW-UNEQ-SNCP
EQPT: CTNEQPT-PBWORK	OCH: VOA-HFAIL	VCMON-HP: FAILTOSW-HO
EQPT: EQPT	OCH: VOA-LDEG	VCMON-HP: FORCED-REQ
EQPT: ERROR-CONFIG	OCH: VOA-LFAIL	VCMON-HP: HP-RFI
EQPT: EXCCOL	OCHNC-CONN: OCHNC-INC	VCMON-HP: HP-TIM
EQPT: FAILTOSW	OMS: APC-CORRECTION-SKIPPED	VCMON-HP: HP-UNEQ
EQPT: FORCED-REQ	OMS: APC-OUT-OF-RANGE	VCMON-HP: LOCKOUT-REQ
EQPT: HI-LASERBIAS	OMS: AS-CMD	VCMON-HP: LOM
EQPT: HI-LASERTEMP	OMS: AS-MT	VCMON-HP: LPBKCRS
EQPT: HI-TXPOWER	OMS: LOS-O	VCMON-HP: MAN-REQ
EQPT: HITEMP	OMS: LOS-P	—
EQPT: IMPROPRMVL	OMS: OPWR-HDEG	VCMON-HP: ROLL
EQPT: INHSWPR	OMS: OPWR-HFAIL	VCMON-HP: ROLL-PEND
EQPT: INHSWWKG	OMS: OPWR-LDEG	VCMON-HP: SDBER-EXCEED-HO
EQPT: IOSCFGCOPY	OMS: OPWR-LFAIL	VCMON-HP: SFBER-EXCEED-HO
EQPT: LO-LASERBIAS	OMS: PARAM-MISM	VCMON-HP: WKSWPR
EQPT: LO-LASERTEMP	OMS: VOA-HDEG	VCMON-HP: WTR
EQPT: LO-TXPOWER	OMS: VOA-HFAIL	VCMON-LP: AUTOSW-AIS-SNCP
EQPT: LOCKOUT-REQ	OMS: VOA-LDEG	VCMON-LP: AUTOSW-LOP-SNCP
EQPT: MAN-REQ	OMS: VOA-LFAIL	VCMON-LP: AUTOSW-UNEQ-SNCP
EQPT: MAESET	OSC-RING: RING-ID-MIS	VCMON-LP: FAILTOSW-LO
EQPT: MEA	OTS: APC-CORRECTION-SKIPPED	VCMON-LP: FORCED-REQ
EQPT: MEM-GONE	OTS: APC-OUT-OF-RANGE	VCMON-LP: LOCKOUT-REQ
EQPT: MEM-LOW	OTS: AS-CMD	VCMON-LP: LP-UNEQ

Table 2-8 Alarm List by Logical Object Type in Alarm Profile (continued)

EQPT: NO-CONFIG	OTS: AS-MT	VCMON-LP: MAN-REQ
EQPT: PEER-NORESPONSE	OTS: AWG-DEG	VCMON-LP: RFI-V
EQPT: PROT	OTS: AWG-FAIL	VCMON-LP: ROLL
EQPT: PWR-FAIL-A	OTS: AWG-OVERTEMP	VCMON-LP: ROLL-PEND
EQPT: PWR-FAIL-B	OTS: AWG-WARM-UP	VCMON-LP: SDBER-EXCEED-LO
EQPT: PWR-FAIL-RET-A	OTS: LASERBIAS-DEG	VCMON-LP: SFBER-EXCEED-LO
EQPT: PWR-FAIL-RET-B	OTS: LOS	VCMON-LP: TU-AIS
EQPT: RUNCFG-SAVENEED	OTS: LOS-O	VCMON-LP: TU-LOP
EQPT: SFTWDOWN	OTS: LOS-P	VCMON-LP: WKSWPR
EQPT: SW-MISMATCH	OTS: OPWR-HDEG	VCMON-LP: WTR
EQPT: SWMTXMOD-PROT	OTS: OPWR-HFAIL	VCTRM-HP: AS-MT-OOG
EQPT: SWMTXMOD-WORK	OTS: OPWR-LDEG	VCTRM-HP: AU-AIS
EQPT: WKSWPR	OTS: OPWR-LFAIL	VCTRM-HP: AU-LOF
EQPT: WTR	OTS: OSRION	VCTRM-HP: AU-LOP
ESCON: ALS	OTS: PARAM-MISM	VCTRM-HP: HP-ENCAP-MISMATCH
ESCON: AS-CMD	OTS: SH-INS-LOSS-VAR-DEG-HIGH	VCTRM-HP: HP-TIM
ESCON: AS-MT	OTS: SH-INS-LOSS-VAR-DEG-LOW	VCTRM-HP: HP-UNEQ
ESCON: FAILTOSW	OTS: SHUTTER-OPEN	VCTRM-HP: LCAS-CRC
ESCON: FORCED-REQ-SPAN	OTS: VOA-HDEG	VCTRM-HP: LCAS-RX-FAIL
ESCON: HI-LASERBIAS	OTS: VOA-HFAIL	VCTRM-HP: LCAS-TX-ADD
ESCON: HI-RXPOWER	OTS: VOA-LDEG	VCTRM-HP: LCAS-TX-DNU
ESCON: HI-TXPOWER	OTS: VOA-LFAIL	VCTRM-HP: LOM
ESCON: LO-RXPOWER	PPM: AS-CMD	VCTRM-HP: LPBKCRS
ESCON: LO-TXPOWER	PPM: AS-MT	VCTRM-HP: OOU-TPT
ESCON: LOCKOUT-REQ	PPM: EQPT	VCTRM-HP: ROLL
ESCON: LOS	PPM: HI-LASERBIAS	VCTRM-HP: ROLL-PEND
ESCON: LPBKFACILITY	PPM: HI-LASERTEMP	VCTRM-HP: SDBER-EXCEED-HO
ESCON: LPBKTERMINAL	PPM: HI-TXPOWER	VCTRM-HP: SFBER-EXCEED-HO
ESCON: MANUAL-REQ-SPAN	PPM: IMPROPRMVL	VCTRM-HP: SQM
ESCON: SQUELCHED	PPM: LO-LASERBIAS	VCTRM-LP: AS-MT-OOG
ESCON: WKSWPR	PPM: LO-LASERTEMP	VCTRM-LP: LCAS-CRC
ESCON: WTR	PPM: LO-TXPOWER	VCTRM-LP: LCAS-RX-FAIL
EXT-SREF: FRCDSWTOPRI	PPM: MEA	VCTRM-LP: LCAS-TX-ADD
EXT-SREF: FRCDSWTOSEC	PPM: MFGMEM	VCTRM-LP: LCAS-TX-DNU
EXT-SREF: FRCDSWTOTHIRD	PPM: PROV-MISMATCH	VCTRM-LP: LOM
EXT-SREF: MANSWTOPRI	PWR: AS-CMD	VCTRM-LP: LP-ENCAP-MISMATCH
EXT-SREF: MANSWTOSEC	PWR: BAT-FAIL	VCTRM-LP: LP-PLM

Table 2-8 Alarm List by Logical Object Type in Alarm Profile (continued)

EXT-SREF: MANSWTOTHIRD	PWR: EHIBATVG	VCTRM-LP: LP-RFI
EXT-SREF: SWTOPRI	PWR: ELWBATVG	VCTRM-LP: LP-TIM
EXT-SREF: SWTOSEC	PWR: VOLT-MISM	VCTRM-LP: LP-UNEQ
EXT-SREF: SWTOTHIRD	STM1E: AS-CMD	VCTRM-LP: OOU-TPT
EXT-SREF: SYNCPRI	STM1E: AS-MT	VCTRM-LP: SDBER-EXCEED-LO
EXT-SREF: SYNCSEC	STM1E: LOF	VCTRM-LP: SFBER-EXCEED-LO
EXT-SREF: SYNCTHIRD	STM1E: LOS	VCTRM-LP: SQM
FAN: EQPT-MISS	STM1E: LPBKFACILITY	VCTRM-LP: TU-AIS
FAN: FAN	STM1E: LPBKTERMINAL	VCTRM-LP: TU-LOP
FAN: MEA	—	—

2.5 Trouble Notifications

The ONS 15454 SDH system reports trouble by utilizing standard alarm and condition characteristics, and standard severities following the rules in ITU-T x.733, and graphical user interface (GUI) state indicators. These notifications are described in the following paragraphs.

The ONS 15454 SDH uses standard 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 address, such as a loss of signal. Conditions do not necessarily require troubleshooting.

2.5.1 Alarm Characteristics

The ONS 15454 SDH uses standard alarm entities to identify what is causing trouble. All alarms stem from hardware, software, environment, or operator-originated problems whether or not they affect service. Current alarms for the network, CTC session, node, or card are listed in the Alarms tab. (In addition, cleared alarms are also found in the History tab.)

2.5.2 Condition Characteristics

Conditions include any problem detected on an ONS 15454 SDH shelf. They could 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.)

Note ONS 15454 SDH condition reporting is not ITU-compliant.

2.5.3 Severities

The ONS 15454 SDH uses ITU-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 (SA) trouble that needs immediate correction, such as an LOS on a trunk port or STM signal.
- A Major (MJ) alarm is a serious alarm, but the trouble has less impact on the network. For example, an automatic protection switching (APS) channel mismatch (APSCNMIS) alarm occurs when working and protect channels have been inadvertently switched so that a working channel is expected at the receive end, but a protect channel is received instead.
- Minor (MN) alarms generally are those that do not affect service. For example, the 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 a free-running synchronization (FRNGSYNC) state or a forced-switch to primary timing (FRCSWTOPRI) 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 (MS-AIS), with severity NR, is inserted by a downstream node when an LOS (CR or MJ) alarm occurs upstream. These conditions do not in themselves require troubleshooting, but are to be expected in the presence of primary alarms.

Severities can be customized for an entire network or for single nodes, from the network level down to the port level by changing or downloading customized alarm profiles. These custom severities are subject to the standard severity-demoting rules given in Telcordia GR-474-CORE and shown in the 2.5.4 Alarm Hierarchy section. Procedures for customizing alarm severities are located in the "Manage Alarms" chapter of the *Cisco ONS 15454 SDH Procedure Guide*.

2.5.4 Alarm Hierarchy

All alarm, condition, and unreported event severities listed in this manual are default profile settings. However in situations when traffic is not lost, such as when the alarm occurs on protected ports or circuits, alarms having Critical (CR) or Major (MJ) default severities can be demoted to lower severities such as Minor (MN) or Non-Service-Affecting (NSA) as defined in Telcordia GR-474-CORE.

A path alarm can be demoted if a higher-ranking alarm is raised for the same object. For example, If an high-order path trace identifier mismatch (HP-TIM) is raised on a circuit path and then an administrative unit (AU) loss of pointer (LOP) is raised on it, the AU-LOP alarm stands and the HP-TIM closes. The path alarm hierarchy used in the ONS 15454 SDH system is shown in Table 2-9.

Table 2-9 Path Alarm Hierarchy

Priority	Condition Type
Highest	AU-AIS
—	AU-LOP
—	HP-UNEQ
Lowest	HP-TIM

Facility (port) alarms also follow a hierarchy, which means that lower-ranking alarms are closed by higher-ranking alarms. The facility alarm hierarchy used in the ONS 15454 SDH system is shown in Table 2-10.

Table 2-10 Facility Alarm Hierarchy

Priority	Condition Type
Highest	LOS
—	LOF
—	MS-AIS
—	MS-EXC[1]
—	MS-DEG[1]
—	MS-RDI[1]
—	RS-TIM
—	AU-AIS
—	AU-LOP
—	HP-EXC[1]
—	HP-DEG[1]
—	HP-UNEQ
—	HP-TIM
Lowest	HP-PLM[1]

1. This alarm is not currently used in the platform.

Near-end failures and far-end failures follow different hierarchies. Near-end failures stand according to whether they are for the entire signal (LOS, LOF), facility (MS-AIS), path (AU-AIS, etc.) or VT (TU-AIS, etc.). The full hierarchy for near-end failures is shown in Table 2-11. This table is taken from Telcordia GR-253-CORE.

Table 2-11 Near-End Alarm Hierarchy

Priority	Condition Type
Highest	LOS
—	LOF
—	MS-AIS
—	AU-AIS[1]
—	AU-LOP[2]
—	HP-UNEQ
—	HP-TIM
—	HP-PLM
—	TU-AIS[1]
—	TU-LOP[2]
—	LP-UNEQ[3]
—	LP-PLM[3]
Lowest	DS-N AIS (if reported for outgoing DS-N signals)

1. Although it is not defined as a defect or failure, all-ones VT pointer relay is also higher priority than AU-LOP. Similarly, all-ones VC pointer relay is higher priority than TU-LOP.
2. AU-LOP is also higher priority than the far-end failure MS-RFI, which does not affect the detection of any near-end failures. Similarly, TU-LOP is higher priority than LP-RF.
3. This alarm is not used in this platform in this release.

The far-end failure alarm hierarchy is shown in Table 2-12, as given in Telcordia GR-253-CORE.

Table 2-12 Far-End Alarm Hierarchy

Priority	Condition Type
Highest	MS-RDI[1]
—	HP-RFI
Lowest	LP-RFI[1]

1. This condition is not used in this platform in this release.

2.5.5 Service Effect

The ITU also provides service effect standards. Service-Affecting (SA) alarms—those that interrupt service—could be Critical (CR), Major (MJ), or Minor (MN) severity alarms.
Non-Service-Affecting (NSA) alarms always have a Minor (MN) default severity.

2.5.6 States

The Alarms and History tab State (ST) column indicate the disposition of the alarm or condition as follows:

- A raised (R) event is one that is active.
- A cleared (C) event is one that is no longer active.
- A transient (T) event is one that is automatically raised and cleared in CTC during system changes such as user login, logout, loss of connection to node view, etc. Transient events do not require user action. These are listed in the “Transient Conditions” chapter.

2.6 Safety Summary

This section covers safety considerations designed to ensure safe operation of the ONS 15454 SDH. Do not perform any procedures in this chapter unless you understand all safety precautions, practices, and warnings for the system equipment. Some troubleshooting procedures require installation or removal of cards; in these instances 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 STM-64 cards. In these instances, pay close attention to the following warnings.

Warning **On the OC192 LR/STM64 LH 1550 card, the laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. The laser is off when the safety key is off (labeled 0).** Statement 293

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

Warning **Use of controls, adjustments, or performing procedures other than those specified could result in hazardous radiation exposure.** Statement 1057

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

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

Warning **Do not reach into a vacant slot or chassis while you install or remove a module or a fan. Exposed circuitry could constitute an energy hazard.** Statement 206

Warning **The power supply circuitry for the equipment can constitute an energy hazard. Before you install or replace the equipment, remove all jewelry (including rings, necklaces, and watches). Metal objects can come into contact with exposed power supply wiring or circuitry inside the DSLAM equipment. This could cause the metal objects to heat up and cause serious burns or weld the metal object to the equipment.** Statement 207

2.7 Alarm Procedures

This section list alarms alphabetically and includes some conditions commonly encountered when troubleshooting alarms. The severity, description, and troubleshooting procedure accompany each alarm and condition.

Note When you check the status of alarms for cards, ensure that the alarm filter icon in the lower right corner of the GUI is not indented. If it is, click it to turn it off. When you're done checking for alarms, click the alarm filter icon again to turn filtering back on. For more information about alarm filtering, refer to the "Manage Alarms" chapter of the *Cisco ONS 15454 SDH Procedure Guide*.

Note When checking alarms, ensure that alarm suppression is not enabled on the card or port. For more information about alarm suppression, refer to the "Manage Alarms" chapter in the *Cisco ONS 15454 SDH Procedure Guide*.

2.7.1 AIS

Not Reported (NR), Non-Service-Affecting (NSA)

SDH Logical Objects: BITS, DS1, DS3, E1, E3, E4, FUDC, MSUDC

DWDM Logical Object: TRUNK

The Alarm Indication Signal (AIS) condition indicates that this node is detecting an alarm indication signal in the incoming signal SDH overhead.

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.

Note DS3i-N-12 card DS3 facility and terminal loopbacks do not transmit DS3 AIS in the direction away from the loopback. Instead of DS3 AIS, a continuance of the signal transmitted to the loopback is provided.

Clear the AIS Condition

Step 1 Determine whether there are alarms on the upstream nodes and equipment, especially the "LOS (STM1E, STMN)" alarm on page 2-147, or if there are locked (locked,maintenance or locked,disabled) ports.

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

Step 3 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or 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.

2.7.2 ALS

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.3 AMPLI-INIT

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.4 APC-CORRECTION-SKIPPED

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.5 APC-DISABLED

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.6 APC-END

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.7 APC-OUT-OF-RANGE

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.8 APSB

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

SDH Logical Object: 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 SDH nodes not manufactured by Cisco send invalid APS codes if they are configured in a 1+1 protection group with newer SDH nodes, such as the ONS 15454 SDH. These invalid codes cause an APSB alarm on an ONS 15454 SDH node.

Clear the APSB Alarm

Step 1 Use an optical test set to examine the incoming SDH 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 ONS 15454 SDH.

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 Traffic Card" procedure on page 2-242.

Caution For the ONS 15454 SDH, removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-230 for commonly used alarm troubleshooting procedures.

Note When you replace a card with the identical type of card, you do not need to make any changes to the database.

Step 3 If the alarm does not clear, log into 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.

2.7.9 APSCDFLTK

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

SDH Logical Object: STMN

The APS Default K Byte Received alarm occurs when a multiplex section-shared protection ring (MS-SPRing) is not properly configured—for example, when a four-node MS-SPRing has one node configured as a subnetwork connection protection (SNCP) ring. When this misconfiguration occurs, a node in an SNCP ring or 1+1 configuration does not send the two valid K1/K2 APS bytes anticipated by a system configured for MS-SPRing. One of the bytes sent is considered invalid by the MS-SPRing configuration. The K1/K2 byte is monitored by receiving equipment for link-recovery information.

Troubleshooting for APSCDFLTK is often similar to troubleshooting for the "MSSP-OOSYNC" alarm on page 2-175.

Clear the APSCDFLTK Alarm

Step 1 Complete the "Identify an MS-SPRing Ring Name or Node ID Number" procedure on page 2-229 to verify that each node has a unique node ID number.

Step 2 Repeat Step 1 for all nodes in the ring.

Step 3 If two nodes have the same node ID number, complete the "Change an MS-SPRing Node ID Number" procedure on page 2-230 to change one node ID number so that each node ID is unique.

Step 4 If the alarm does not clear, verify correct configuration of east port and west port optical fibers. (See the "EXCCOL" alarm on page 2-85.) West port fibers must connect to east port fibers and east port fibers must connect to west port fibers. The "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15454 SDH Procedure Guide* provides a procedure for fibering MS-SPRings.

Step 5 If the alarm does not clear and if the network is a four-fiber MS-SPRing, ensure that each protect fiber is connected to another protect fiber and each working fiber is connected to another working fiber. The software does not report any alarm if a working fiber is incorrectly attached to a protect fiber.

Step 6 If the alarm does not clear, complete the "Verify Node Visibility for Other Nodes" procedure on page 2-230.

Step 7 If nodes are not visible, complete the "Verify or Create Node RS-DCC Terminations" procedure on page 2-244 to ensure that regenerator section data communications channel (RS-DCC) terminations exist on each node.

Step 8 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.

2.7.10 APSC-IMP

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

SDH Logical Object: STMN

An Improper SDH APS Code alarm indicates bad or invalid K bytes. The APSC-IMP alarm occurs on STM-N cards in a MS-SPRing configuration and can occur during MS-SPRing configuration.

The receiving equipment monitors K bytes or K1 and K2 APS bytes for an indication to switch from the working card to the protect card or from the protect card to the working one. K1/K2 bytes also contain bits that tell the receiving equipment whether the K byte is valid. The alarm clears when the node receives valid K bytes.

Note This alarm can occur on a VC_LO_PATH_TUNNEL tunnel when it does not have lower order circuits provisioned on it. It can also occur when the exercise command or a lockout is applied to a span. An externally switched span does not raise this alarm because the traffic is preempted.

Note The APSC-IMP alarm may be raised on a BLSR or MS-SPRing when a drop connection is part of a cross-connect loopback.

Note The APSC-IMP alarm may be momentarily raised on BLSR spans during PCA circuit creation or deletion across multiple nodes using CTC.

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 APSC-IMP Alarm

Step 1 Use an optical test set to determine the validity of the K byte signal by examining the received signal. For specific procedures to use the test set equipment, consult the manufacturer.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454 SDH. Plug the wristband cable into the ESD jack located on the on the middle-right outside edge of the shelf assembly.

If the K byte is invalid, the problem lies with upstream equipment and not with the reporting ONS 15454 SDH. Troubleshoot the upstream equipment using the procedures in this chapter, as applicable. If the upstream nodes are not ONS 15454 SDHs, consult the appropriate user documentation.

Step 2 If the K byte is valid, verify that each node has a ring name that matches the other node ring names. Complete the "Identify an MS-SPRing Ring Name or Node ID Number" procedure on page 2-229.

Step 3 Repeat Step 2 for all nodes in the ring.

Step 4 If a node has a ring name that does not match the other nodes, make that node's ring name identical to the other nodes. Complete the "Change an MS-SPRing Ring Name" procedure on page 2-229.

Step 5 If the condition does not clear, log into the Cisco 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.

2.7.11 APSCINCON

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

SDH Logical Object: STMN

An Inconsistent APS Code alarm indicates that the APS code contained in the SDH overhead is inconsistent. The SDH overhead contains K1/K2 APS bytes that notify receiving equipment, such as the ONS 15454 SDH, to switch the SDH signal from a working to a protect path when necessary. An inconsistent APS code occurs when three consecutive frames contain nonidentical APS bytes, which in turn give the receiving equipment conflicting commands about switching.

Clear the APSCINCON Alarm on an STM-N Card in an MS-SPRing

Step 1 Look for other alarms, especially the "LOS (STM1E, STMN)" alarm on page 2-147, the "LOF (DS1, DS3, E1, E4, STM1E, STMN)" alarm on page 2-138, or the "APSB" alarm on page 2-32. Clearing these alarms clears the APSCINCON alarm.

Step 2 If an APSINCON alarm occurs with no other alarms, log into the Cisco 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.

2.7.12 APSCM

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

SDH Logical Object: STMN

An Improper SDH APS Code alarm indicates three consecutive, identical frames containing:

- Unused code in bits 6 through 8 of byte K2.
- Codes that are irrelevant to the specific protection switching operation being requested.
- Requests that are irrelevant to the ring state of the ring (such as a span protection switch request in a two-fiber ring NE).
- ET code in K2 bits 6 through 8 received on the incoming span, but not sourced from the outgoing span.

Warning **On the OC192 LR/STM64 LH 1550 card, the laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. The laser is off when the safety key is off (labeled 0).** Statement 293

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

Warning **Use of controls, adjustments, or performing procedures other than those specified could result in hazardous radiation exposure.** Statement 1057

Clear the APSCM Alarm

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

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454 SDH. Plug the wristband cable into the ESD jack located on the middle-right outside edge of the shelf assembly.

Step 2 If the alarm does not clear, verify that the protection-card channel fibers are physically connected directly to the adjoining node's protection-card channel fibers.

Step 3 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.

2.7.13 APSCNMIS

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

SDH Logical Object: STMN

The APS Node ID Mismatch alarm occurs when the source node ID contained in the incoming APS channel K2 byte is not present in the ring map. APSCNMIS could occur and clear when an MS-SPRing is being provisioned. If so, the user can disregard the temporary occurrence. If the APSCNMIS occurs and stays, the alarm clears when a K byte with a valid source node ID is received.

Clear the APSCNMIS Alarm

Step 1 Complete the "Identify an MS-SPRing Ring Name or Node ID Number" procedure on page 2-229 for each node to verify that each node has a unique node ID number.

Step 2 If the Node ID column contains any two nodes with the same node ID listed, record the repeated node ID.

Step 3 Click **Close** in the Ring Map dialog box.

Step 4 If two nodes have the same node ID number, complete the "Change an MS-SPRing Node ID Number" procedure on page 2-230 to change one node ID number so that each node ID is unique.

Note If the node names shown in the network view do not correlate with the node IDs, log into each node and click the **Provisioning > MS-SPRing** tabs. The MS-SPRing window shows the node ID of the login node.

Note Applying and removing a lockout on a span causes the ONS node to generate a new K byte. The APSCNMIS alarm clears when the node receives a K byte containing the correct node ID.

Step 5 If the alarm does not clear, use the "Initiate a Lockout on an MS-SPRing Protect Span" procedure on page 2-237 to lock out the span.

Step 6 Complete the "Clear an MS-SPRing External Switching Command" procedure on page 2-238 to clear the lockout.

Step 7 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.

2.7.14 APSIMP

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

SDH Logical Object: STMN

The APS Invalid Mode condition 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 SNCP or MS-SPRing 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 condition is superseded by an APSCM alarm, but not by an AIS condition. It clears when the port receives a valid code for 10 ms.

Clear the APSIMP Condition

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. For procedures, refer to the "Turn Up Node" chapter in the *Cisco ONS 15454 SDH Procedure Guide*.

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 SDH.

Step 4 If the condition 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.

2.7.15 APS-INV-PRIM

The APS-INV-PRIM alarm is not used in this platform in this release. It is reserved for future development.

2.7.16 APSMM

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

SDH Logical Object: STMN

An APS Mode Mismatch failure alarm occurs on STM-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 another vendor's equipment is provisioned as 1:N and the ONS 15454 SDH is provisioned as 1+1.

If one end is provisioned for 1+1 protection switching and the other is provisioned for SNCP protection switching, an APSMM alarm occurs in the ONS 15454 SDH that is provisioned for 1+1 protection switching.

Clear the APSMM Alarm

Step 1 For the reporting ONS 15454 SDH, display node view and verify the protection scheme provisioning by completing the following steps:

- **a.** Click the **Provisioning > Protection** tabs.
- **b.** Click the 1+1 protection group configured for the STM-N cards.

  The chosen protection group is the protection group optically connected (with data communications channel [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 STM-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. If not, change it to match.

Step 5 Click **Apply**.

Step 6 If the condition 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.

2.7.17 APS-PRIM-FAC

The APS-PRIM-FAC condition is not used in this platform in this release. It is reserved for future development.

2.7.18 APS-PRIM-SEC-MISM

The APS-PRIM-SEC-MISM condition is not used in this platform in this release. It is reserved for future development.

2.7.19 AS-CMD

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

SDH Logical Objects: BPLANE, CE100T, DS1, DS3, E1, E100T, E1000F, E3, E4, EQPT, FCMR, G1000, GFP-FAC, ML100T, ML1000, MLFX, NE, PWR, STM1E, STMN

DWDM Logical Objects: 2R, AOTS, ESCON, FC, GE, ISC, OCH, OMS, OTS, PPM, TRUNK

The Alarms Suppressed by User Command condition applies to the network element (NE object), backplane, a single card, or a port on a card. 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 SDH Procedure Guide*.

Clear the AS-CMD Condition

Step 1 For all nodes, in node view, click the **Conditions** tab.

Step 2 Click **Retrieve**. If you have already retrieved conditions, look under the Object column and Eqpt Type column and note what entity the condition is reported against—such as a port, slot, or shelf.

If the condition is reported against an STM-N card and slot, alarms were either suppressed for the entire card or for one of the ports. Note the slot number and continue with Step 3.

If the condition is reported against the backplane, go to Step 8.

If the condition is reported against the NE object, go to Step 9.

Step 3 If the AS-CMD condition is reported for an STM-N card, determine whether alarms are suppressed for a port and if so, raise the suppressed alarms by completing the following steps:

a. Double-click the card to display the card view.

b. Click the **Provisioning > Alarm Profiles > Alarm Behavior** tabs an d 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, click **View > Go to Previous View**.

Step 4 If the AS-CMD condition is reported for an amplifier, combiner, or other DWDM card, determine whether alarms are suppressed for a port and if so, raise the suppressed alarms by completing the following steps:

a. Double-click the card to display the card view.

b. Click the **Provisioning > Optical Line > Alarm Profiles** 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, click **View > Go to Previous View**.

Step 5 In node view, if the AS-CMD condition is reported for a card and not an individual port, click the **Provisioning > Alarm Profiles > Alarm Behavior** tabs.

Step 6 Locate the row for the reported card slot.

Step 7 Click the **Suppress Alarms** column check box to deselect the option for the card row.

Step 8 If the condition is reported for the backplane, the alarms are suppressed for cards such as the AIP that are not in the optical or electrical slots. To clear the alarm, complete the following steps:

a. In node view, click the **Provisioning > Alarm Profiles > Alarm Behavior** tabs.

b. In the backplane row, uncheck the Suppress Alarms column check box.

c. Click **Apply**.

Step 9 If the condition is reported for the shelf, cards and other equipment are affected. To clear the alarm, complete the following steps:

a. In node view, click the **Provisioning > Alarm Profiles > Alarm Behavior** tabs.

b. Click the **Suppress Alarms** check box located at the bottom of the window to deselect the option.

c. Click **Apply**.

Step 10 If the condition 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.

2.7.20 AS-MT

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

SDH Logical Objects: CE100T, DS1, DS3, E1, E3, E4, EQPT, FCMR, G1000, GFP-FAC, ML100T, ML1000, MLFX, STM1E, STMN

DWDM Logical Objects: 2R, AOTS, ESCON, FC, GE, ISC, OCH, OMS, OTS, PPM, TRUNK

The Alarms Suppressed for Maintenance Command condition applies to STM-N and electrical cards and occurs when a port is placed in the Locked-Enabled, loopback & maintenance service state for loopback testing operations.

Clear the AS-MT Condition

Step 1 Complete the "Clear an STM-N Card Facility or Terminal Loopback Circuit" procedure on page 2-244.

Step 2 If the condition 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.

2.7.21 AS-MT-OOG

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

SDH Logical Objects: VCTRM-HP, VCTRM-LP

The Alarms Suppressed on an Out-Of-Group VCAT Member condition is raised on a VC whenever the member is in the IDLE (AS-MT-OOG) admin state. This condition can be raised when a member is initially added to a group. In IDLE (AS-MT-OOG) state, all other alarms for the VC are suppressed.

Clear the AS-MT-OOG Condition

Step 1 The AS-MT-OOG condition clears when a VC member transitions to a different state from IDLE (AS-MT-OOG) or when it is removed completely from the group. It does not require troubleshooting unless it does not clear.

Step 2 If the condition 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.

2.7.22 AU-AIS

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

SDH Logical Objects: 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

Step 1 Complete the "Clear the AIS Condition" procedure on page 2-31.

Step 2 If the condition does not clear, complete the "Clear the APSB Alarm" procedure on page 2-32.

Step 3 If the condition 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.

2.7.23 AUD-LOG-LOSS

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

SDH Logical Object: NE

The Audit Trail Log Loss condition occurs when the log is 100 percent full and that the oldest entries are being replaced as new entries are generated. The log capacity is 640 entries. You must off-load (save) the log to make room for more entries.

Clear the AUD-LOG-LOSS Condition

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

Step 2 Click **Retrieve**.

Step 3 Click **Archive**.

Step 4 In the Archive Audit Trail dialog box, navigate to the directory (local or network) where you want to save the file.

Step 5 Enter a name in the File Name field.

You do not need to assign an extension to the file. The file is readable in any application that supports text files, such as WordPad, Microsoft Word (imported), etc.

Step 6 Click **Save**.

The 640 entries are saved in this file. New entries continue with the next number in the sequence, rather than starting over.

Step 7 If the condition 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.

2.7.24 AUD-LOG-LOW

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

SDH Logical Object: NE

The Audit Trail Log Low condition occurs when the audit trail log is 80 percent full.

Note AUD-LOG-LOW is an informational condition. The condition does not require troubleshooting.

2.7.25 AU-LOF

Critical (CR), Service-Affecting (SA)

SDH Logical Object: VCTRM-HP

The AU Loss of Frame (LOF) alarm indicates that the ONS 15454 SDH detects frame loss in the regenerator section of the SDH overhead.

Clear the AU-LOF Alarm

Step 1 Complete the "Clear the LOF (DS1, DS3, E1, E4, STM1E, STMN) Alarm" procedure on page 2-138.

Step 2 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 to report a Service-Affecting (SA) problem.

2.7.26 AU-LOP

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

SDH 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 SONET 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

Note For more information about MXP and TXP cards, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Clear the AU-LOP Alarm

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" procedure on page 2-243.

Step 5 Recreate the circuit for the correct size. For procedures, refer to the "Create Circuits and Tunnels" chapter in the *Cisco ONS 15454 SDH Procedure Guide*.

Step 6 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or 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.

2.7.27 AUTOLSROFF

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

SDH Logical Object: STMN

DWDM Logical Object: TRUNK

The Auto Laser Shutdown alarm occurs when the STM-64 card temperature exceeds 194 degrees F (90 degrees C). The internal equipment automatically shuts down the STM-64 laser when the card temperature rises to prevent the card from self-destructing.

Warning **On the OC192 LR/STM64 LH 1550 card, the laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. The laser is off when the safety key is off (labeled 0).** Statement 293.

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

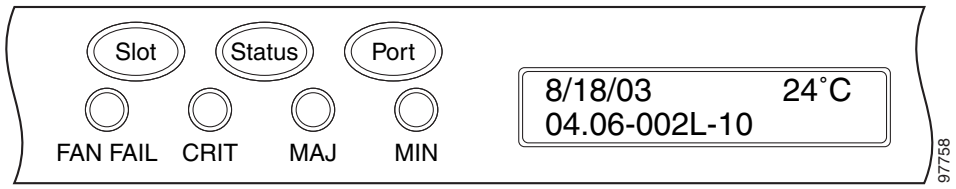
Warning **Use of controls, adjustments, or performing procedures other than those specified could result in hazardous radiation exposure.** Statement 1057

Clear the AUTOLSROFF Alarm

Step 1 View the temperature displayed on the ONS 15454 SDH LCD front panel (Figure 2-1).

Figure 2-1 shows the shelf LCD panel.

Figure 2-1 Shelf LCD Panel



Step 2 If the temperature of the shelf exceeds 194 degrees F (90 degrees C), the alarm should clear if you solve the ONS 15454 SDH temperature problem. Complete the "Clear the HITEMP Alarm" procedure on page 2-117.

Step 3 If the temperature of the shelf is under 194 degrees F (90 degrees C), the HITEMP alarm is not the cause of the AUTOLSROFF alarm. Complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the STM-64 card.

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. See the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-230 for commonly used troubleshooting procedures.

Note When you replace a card with the identical type of card, you do not need to make any changes to the database.

Step 4 If card replacement does not clear the alarm, 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.

2.7.28 AUTORESET

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

SDH Logical Object: EQPT

The Automatic System Reset alarm occurs when a card is performing an automatic warm reboot. An AUTORESET occurs when you change an IP address or perform any other operation that causes an automatic card-level reboot.

Clear the AUTORESET Alarm

Step 1 Determine whether there are additional alarms that could have triggered an automatic reset. If there are, troubleshoot these alarms using the applicable section of this chapter.

Step 2 If the card automatically resets more than once a month with no apparent cause, complete the "Physically Replace a Traffic Card" procedure on page 2-242.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454 SDH. Plug the wristband cable into the ESD jack located on the middle-right outside edge of the shelf assembly.

Caution For the ONS 15454 SDH, removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-230 for commonly used traffic-switching procedures.

Note When you replace a card with the identical type of card, you do not need to make any changes to the database.

Step 3 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.

2.7.29 AUTOSW-AIS-SNCP

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

SDH Logical Objects: VCMON-HP, VCMON-LP

The Automatic SNCP Switch Caused by an AIS condition indicates that automatic SNCP protection switching occurred because of the "TU-AIS" condition on page 2-221. If the SNCP ring is configured for revertive switching, it switches back to the working path after the fault clears. The AUTOSW-AIS-SNCP clears when you clear the primary alarm on the upstream node.

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 AUTOSW-AIS-SNCP Condition

Step 1 Complete the "Clear the AIS Condition" procedure on page 2-31.

Step 2 If the condition 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.

2.7.30 AUTOSW-LOP-SNCP

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

SDH Logical Objects: VCMON-HP, VCMON-LP

An Automatic SNCP Switch Caused by LOP alarm indicates that an automatic SNCP protection switching occurred because of the "AU-LOP" alarm on page 2-43. If the SNCP ring is configured for revertive switching, it switches back to the working path after the fault clears.

Clear the AUTOSW-LOP-SNCP Alarm

Step 1 Complete the "Clear the AU-LOP Alarm" procedure on page 2-44.

Step 2 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.

2.7.31 AUTOSW-SDBER-SNCP

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

SDH Logical Object: VCMON-HP

The Automatic SNCP Switch Caused by Signal Degrade Bit Error Rate (SDBER) condition indicates that a signal degrade [see the "SD (DS1, DS3, E1, E3, E4, STM1E, STMN)" condition on page 2-192] caused automatic SNCP protection switching to occur. If the SNCP ring is configured for revertive switching, it reverts to the working path when the SD is resolved.

Clear the AUTOSW-SDBER-SNCP Condition

Step 1 Complete the "Clear the SD (DS3, E1, E3, E4, STM1E, STM-N) Condition" procedure on page 2-193.

Step 2 If the condition 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.

2.7.32 AUTOSW-SFBER-SNCP

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

SDH Logical Object: VCMON-HP

The Automatic SNCP Switch Caused by Signal Fail Bit Error Rate (SFBER) condition indicates that a signal fail [see the "SF (DS1, DS3, E1, E3, E4, STMN)" condition on page 2-196] caused automatic SNCP protection switching to occur. If the SNCP ring is configured for revertive switching, it reverts to the working path when the SF is resolved.

Clear the AUTOSW-SFBER-SNCP Condition

Step 1 Complete the "Clear the SF (DS3, E1, E3, E4, STMN) Condition" procedure on page 2-197.

Step 2 If the condition 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.

2.7.33 AUTOSW-UNEQ-SNCP (VCMON-HP)

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

SDH Logical Object: VCMON-HP

The Automatic SNCP Switch Caused by an Unequipped condition indicates that an HP-UNEQ alarm caused automatic SNCP protection switching to occur (see the "HP-UNEQ" alarm on page 2-122). If the SNCP 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

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

Step 1 Complete the "Clear the HP-UNEQ Alarm" procedure on page 2-122.

Step 2 If the condition 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.

2.7.34 AUTOSW-UNEQ-SNCP (VCMON-LP)

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

SDH Logical Object: VCMON-LP

AUTOSW-UNEQ-SNCP for VCMON-LP indicates that the "LP-UNEQ" alarm on page 2-163 caused automatic SNCP protection switching to occur. If the SNCP 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

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

Step 1 Display the CTC network view and right-click the span reporting AUTOSW-UNEQ. Select **Circuits** from the shortcut menu.

Step 2 If the specified circuit is a low-order path tunnel, determine whether low-order paths are assigned to the tunnel.

Step 3 If the low-order path tunnel does not have assigned low-order paths, delete the low-order path tunnel from the list of circuits.

Step 4 If you have complete visibility to all nodes, determine whether there are incomplete circuits such as stranded bandwidth from circuits that were not completely deleted.

Step 5 If you find incomplete circuits, determine whether they are working circuits and if they are still passing traffic.

Step 6 If the incomplete circuits are not needed or are not passing traffic, delete them and log out of CTC. Log back in and search for incomplete circuits again. Recreate any needed circuits.

Step 7 If the condition does not clear, verify that all circuits terminating in the reporting card are active by completing the following steps:

a. In node view, click the **Circuits** tab.

b. Verify that the **Status** column lists the port as active.

c. If the Status column lists the port as incomplete, and the incomplete does not change after a full initialization, 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.

Step 8 After you determine that the port is active, verify the signal source received by the card reporting the alarm.

Step 9 If the condition does not clear, verify that the far-end STM-N card providing payload to the card is working properly.

Step 10 If the condition does not clear, verify the far-end cross-connect between the STM-N card and the E-N card.

Step 11 If the condition does not clear, clean the far-end optical fiber cable ends according to site practice. If no site practice exists, complete the procedure for cleaning optical connectors in the "Maintain the Node" chapter of the *Cisco ONS 15454 SDH Procedure Guide*.

Warning **On the OC192 LR/STM64 LH 1550 card, the laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. The laser is off when the safety key is off (labeled 0).** Statement 293

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

Warning **Use of controls, adjustments, or performing procedures other than those specified could result in hazardous radiation exposure.** Statement 1057

Step 12 If the condition 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.

2.7.35 AWG-DEG

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.36 AWG-FAIL

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.37 AWG-OVERTEMP

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.38 AWG-WARM-UP

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.39 BAT-FAIL

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

SDH Logical Object: PWR

The Battery Fail alarm occurs when one of the two power supplies (A or B) is not detected. This could be because the supply is removed or is not operational. The alarm does not distinguish between the individual power supplies, so onsite information about the conditions is necessary for troubleshooting.

Clear the BATFAIL Alarm

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

Step 2 Remove the power cable from the faulty supply.

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 to report a Service-Affecting (SA) problem.

2.7.40 BLSROSYNC

The BLSROSYNC alarm is not used in this platform in this release. It is reserved for future development.

2.7.41 BKUPMEMP

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

Note The severity is Minor (MN), Non-Service-Affecting (NSA) for SBY TCC2/TCC2P card.

SDH Logical Object: EQPT

The Primary Nonvolatile Backup Memory Failure alarm refers to a problem with the TCC2/TCC2P card flash memory. This alarm is raised on ACT/SBY TCC2/TCC2P cards. The alarm occurs when the TCC2/TCC2P card is in active or standby state and has one of four problems:

- Failure to format a flash partition.
- Failure to write a file to a flash partition.
- Problem at the driver level.
- Code volume fails cyclic redundancy checking (CRC, a method to verify for errors in data transmitted to the TCC2/TCC2P card).

The BKUPMEMP alarm can also cause the "EQPT" alarm on page 2-79. If the EQPT alarm is caused by BKUPMEMP, complete the following procedure to clear the BKUPMEMP and the EQPT alarm.

Clear the BKUPMEMP Alarm

Step 1 Verify that both TCC2/TCC2P cards are powered and enabled by confirming lighted ACT/SBY LEDs on the TCC2/TCC2P cards.

Step 2 Determine whether the active or standby TCC2/TCC2P card has the alarm.

Step 3 If both cards are powered and enabled, reset the TCC2/TCC2P card where the alarm is raised. If the card is the active TCC2/TCC2P card, complete the "Reset an ActiveTCC2/TCC2P Card and Activate the Standby Card" procedure on page 2-239.
Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card. The ACT/STBY LED of this card should be amber and the newly active TCC2/TCC2P card LED should be green.
If the card is the standby TCC2/TCC2P card, complete the "Reset the Standby TCC2/TCC2P Card" procedure on page 2-239.

Step 4 If the reset TCC2/TCC2P card has not rebooted successfully, or the alarm has not cleared, log into the Cisco 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. If the Technical Support technician tells you to reseat the card, complete the "Remove and Reinsert (Reseat) Any Card" procedure on page 2-241. If the Technical Support technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Traffic Card" procedure on page 2-242.

2.7.42 CARLOSS (CE100T)

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

SDH Logical Object: CE100T

The Carrier Loss alarm is raised on CE-100T-8 cards in Mapper mode when there is a circuit failure due to link integrity. It does not get raised when a user simply puts the port in the Unlocked state. It has to be Unlocked with a circuit or loopback.

Note For more information about Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.

Clear the CARLOSS (CE100T) Alarm

Step 1 Complete the "Clear the CARLOSS (G1000) Alarm" procedure on page 2-57. However, rather than checking for a TPTFAIL (G1000) at the end of the procedure, check for a "TPTFAIL (CE100T)" alarm on page 2-217.

Step 2 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.

2.7.43 CARLOSS (E100T, E1000F)

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

SDH Logical Objects: E100T, E1000F

A Carrier Loss alarm on the LAN E-Series Ethernet card is the data equivalent of the "LOS (STM1E, STMN)" alarm on page 2-147. The Ethernet card has lost its link and is not receiving a valid signal. The most common causes of the CARLOSS alarm are a disconnected cable, an Ethernet Gigabit Interface Converter (GBIC) fiber connected to an optical card rather than an Ethernet device, or an improperly installed Ethernet card. Ethernet card ports must be enabled for CARLOSS to occur. CARLOSS is declared after no signal is received for approximately 2.5 seconds.

CARLOSS also occurs after the restoration of a node database. In this instance, the alarm clears approximately 30 seconds after the node reestablishes Spanning Tree Protocol (STP). Reestablishment applies to the E-Series Ethernet cards but not to the G-Series card. The G-Series card does not use STP and is not affected by STP reestablishment.

Note For more information about Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.

Clear the CARLOSS (E100T, E1000F) Alarm

Step 1 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 Cable" chapter in the *Cisco ONS 15454 SDH Procedure Guide*.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454 SDH. Plug the wristband cable into the ESD jack located on the middle-right outside edge of the shelf assembly.

Step 2 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 STM-N card. For more information about fiber connections and terminations, refer to the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15454 SDH Procedure Guide*.

Step 3 If no misconnection to an STM-N card exists, verify that the transmitting device is operational. If not, troubleshoot the device.

Step 4 If the alarm does not clear, use an Ethernet test set to determine whether a valid signal is coming into the Ethernet port. For specific procedures to use the test set equipment, consult the manufacturer.

Step 5 If a valid Ethernet signal is not present and the transmitting device is operational, replace the fiber cable connecting the transmitting device to the Ethernet port. To do this, refer to the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15454 SDH Procedure Guide*.

Step 6 If a valid Ethernet signal is present, complete the "Remove and Reinsert (Reseat) Any Card" procedure on page 2-241 for the Ethernet card.

Step 7 If the alarm does not clear, complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the Ethernet card.

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. See the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-230 for commonly used traffic-switching procedures.

Note When you replace a card with the identical type of card, you do not need to make any changes to the database.

Step 8 If a CARLOSS alarm repeatedly appears and clears, use the following steps to examine the layout of your network to determine whether the Ethernet circuit is part of an Ethernet manual cross-connect.

An Ethernet manual cross-connect is used when another vendor's equipment sits between ONS 15454 SDHs, and the open systems interconnect/target identifier address resolution protocol (OSI/TARP)-based equipment does not allow tunneling of the ONS 15454 SDH TCP/IP-based DCC. To circumvent a lack of continuous DCC, the Ethernet circuit is manually cross connected to a channel riding through the non-ONS network.

If the reporting Ethernet circuit is part of an Ethernet manual cross-connect, then the reappearing alarm could be a result of mismatched circuit sizes in the set up of the manual cross-connect. Determine this by completing the following steps. If the Ethernet circuit is not part of a manual cross-connect, the following steps do not apply.

a. Right-click anywhere in the row of the CARLOSS alarm.

b. Click **Select Affected Circuits** in the shortcut menu that appears.

c. Record the information in the type and size columns of the highlighted circuit.

d. From the examination of the layout of your network, determine which ONS 15454 SDH node and card are hosting the Ethernet circuit at the other end of the Ethernet manual cross-connect and complete the following substeps:

- Log into the ONS 15454 SDH at the other end of the Ethernet manual cross-connect.
- Double-click the Ethernet card that is part of the Ethernet manual cross-connect.
- Click the **Circuits** tab.
- Record the information in the type and size columns of the circuit that is part of the Ethernet manual cross-connect. The Ethernet manual cross-connect circuit connects the Ethernet card to an STM-N card at the same node.

e. Use the information you recorded to determine whether the two Ethernet circuits on each side of the Ethernet manual cross-connect have the same circuit size.

If one of the circuit sizes is incorrect, complete the "Delete a Circuit" procedure on page 2-243 and reconfigure the circuit with the correct circuit size. For procedures, refer to the "Create Circuits and Tunnels" chapter in the *Cisco ONS 15454 SDH Procedure Guide*.

Step 9 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.

2.7.44 CARLOSS (EQPT)

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

SDH Logical Object: EQPT

The Carrier Loss Equipment alarm occurs when the ONS 15454 SDH and the workstation hosting CTC do not have a TCP/IP connection. CARLOSS is a problem involving the LAN or data circuit used by the RJ-45 connector on the TCC2/TCC2P card or the LAN backplane pin connection on the back of the ONS 15454 SDH. The alarm does not involve an Ethernet circuit connected to a port on an Ethernet (traffic) card. The problem is in the connection (usually a LAN problem) and not the CTC or the ONS 15454 SDH.

On TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, and MXP_2.5G_10G cards, CARLOSS is also raised against trunk ports when ITU-T G.709 monitoring is turned off.

A TXP_MR_2.5G card can raise a CARLOSS alarm when the payload is incorrectly configured for the 10 Gigabit Ethernet or 1 Gigabit Ethernet payload data types.

Note For more information about provisioning MXP or TXP PPMs, refer to the "Provision Transponder and Muxponder Cards" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For more information about the cards themselves, refer to the "Card Reference" chapter. For more information about MRC-12 and OC192-XFP/STM64-XFP cards, refer to the "Change Card Settings" chapter of the *Cisco ONS 15454 SDH Procedure Guide*. For more information about Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.

Clear the CARLOSS (EQPT) Alarm

Step 1 If the reporting card is an MXP, TXP, MRC-12, or OC192-XVP/STM64-XFP card in an ONS 15454 SDH node, verify the data rate configured on the PPM by completing the following steps:

- **a.** Double-click the reporting card.
- **b.** Click the **Provisioning > Pluggable Port Modules** tabs.
- **c.** View the Pluggable Port Modules area port listing in the **Actual Equipment Type** column for the card and compare this with the Selected PPM area Rate column contents.
- **d.** If the rate does not match the actual equipment, you must delete and recreate the selected PPM. Select the PPM, click **Delete**, then click **Create** and choose the correct rate for the port rate.

Step 2 If the reporting card is an STM-N card, verify connectivity by pinging the ONS 15454 SDH that is reporting the alarm by completing the procedure in the "1.9.8 Verify PC Connection to the ONS 15454 SDH (ping)" section on page 1-109.

Step 3 If the ping is successful, it demonstrates that an active TCP/IP connection exists. Restart CTC by completing the following steps:

- **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 specific procedures to use the test set equipment, consult the manufacturer.)

Step 5 Verify that the optical LAN cable is properly connected and attached to the correct port. For more information about fiber connections and terminations, refer to the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15454 SDH Procedure Guide*

Step 6 If the fiber cable is properly connected and attached to the port, verify that the cable connects the card to another Ethernet device and is not misconnected to an STM-N card. For more information about fiber connections and terminations, refer to the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15454 SDH Procedure Guide*.

Step 7 If you are unable to establish connectivity, replace the fiber cable with a new known-good cable. To do this, refer to the "Install Cards and Fiber-Optic Cable" chapter of the *Cisco ONS 15454 SDH Procedure Guide* for procedures.

Step 8 If you are unable to establish connectivity, perform standard network or LAN diagnostics. For example, trace the IP route, verify cable continuity, and troubleshoot any routers between the node and CTC. To verify cable continuity, follow site practices.

Step 9 If you are unable to establish connectivity, perform standard network/LAN diagnostics. For example, trace the IP route, verify cable continuity, and troubleshoot any routers between the node. 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 to report a Service-Affecting (SA) problem.

2.7.45 CARLOSS (FC)

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.46 CARLOSS (G1000)

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

SDH Logical Object: G1000

A Carrier Loss alarm on the LAN G-Series Ethernet card is the data equivalent of the "LOS (STM1E, STMN)" alarm on page 2-147. The Ethernet card has lost its link and is not receiving a valid signal.

CARLOSS on the G-Series card can be caused by one of two situations:

- The G-Series port reporting the alarm is not receiving a valid signal from the attached Ethernet device. The CARLOSS can be caused by an improperly connected Ethernet cable or a problem with the signal between the Ethernet device and the G-Series port.
- If a problem exists in the end-to-end path (including possibly the far-end G-Series card), the problem causes the reporting G-Series to turn off the Gigabit Ethernet transmitter. Turning off the transmitter typically causes the attached device to turn off its link laser, which results in a CARLOSS on the reporting G-Series card. The root cause is the problem in the end-to-end path. When the root cause is cleared, the far-end G-Series port turns the transmitter laser back on and clears the CARLOSS on the reporting card. If a turned-off transmitter causes the CARLOSS alarm, it is normally accompanied by a "TPTFAIL (G1000)" alarm on page 2-218 or STM-N alarms or conditions on the end-to-end path.

Refer to the *Cisco ONS 15454 SDH Reference Manual* for a description of the G-Series card's end-to-end Ethernet link integrity capability. Also see the "TRMT" alarm on page 2-220 for more information about alarms that occur when a point-to-point circuit exists between two G-Series cards.

Ethernet card ports must be unlocked for CARLOSS to occur. CARLOSS is declared after no signal is received for approximately 2.5 seconds.

Note For more information about Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.

Clear the CARLOSS (G1000) Alarm

Step 1 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 Cable" chapter in the *Cisco ONS 15454 SDH Procedure Guide*.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454 SDH. Plug the wristband cable into the ESD jack located on the middle-right outside edge of the shelf assembly.

Step 2 If the fiber cable is correctly connected and attached, verify that the cable connects the card to another Ethernet device and is not misconnected to an STM-N card.

Step 3 If no misconnection to the STM-N card exists, verify that the attached transmitting Ethernet device is operational. If not, troubleshoot the device.

Step 4 Verify that optical receive levels are within the normal range. These are listed in the "1.12.3 Optical Card Transmit and Receive Levels" section on page 1-135.

Step 5 If the alarm does not clear, use an Ethernet test set to determine whether a valid signal is coming into the Ethernet port. For specific procedures to use the test set equipment, consult the manufacturer.

Step 6 If a valid Ethernet signal is not present and the transmitting device is operational, replace the fiber cable connecting the transmitting device to the Ethernet port. To do this, refer to the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15454 SDH Procedure Guide* for procedures.

Step 7 If the alarm does not clear, and link autonegotiation is enabled on the G-Series port but the autonegotiation process fails, the card turns off its transmitter laser and reports a CARLOSS alarm. If link autonegotiation has been enabled for the port, determine whether there are conditions that could cause autonegotiation to fail by completing the following steps:

a. Confirm that the attached Ethernet device has autonegotiation enabled and is configured for compatibility with the asymmetric flow control on the card.

b. Confirm that the attached Ethernet device configuration allows reception of flow control frames.

Step 8 If the alarm does not clear, disable and reenable the Ethernet port to attempt to remove the CARLOSS condition. (The autonegotiation process restarts.)

Step 9 If the alarm does not clear and the "TPTFAIL (G1000)" alarm on page 2-218 is also reported, complete the "Clear the TPTFAIL (G1000) Alarm" procedure on page 2-219. If the TPTFAIL alarm is not raised, continue to the next step.

Note When the CARLOSS and the TPTFAIL alarms are reported, the condition could be caused by the G-Series card's end-to-end link integrity feature taking action on a remote failure indicated by the TPTFAIL alarm.

Step 10 If the TPTFAIL alarm was not raised, determine whether a terminal (inward) loopback has been provisioned on the port by completing the following steps:

a. In node view, click the card to go to card view.

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

c. If the port Admin State is listed as Locked, maintenance, a loopback could be provisioned. Go to Step 11.

Step 11 If a loopback was provisioned, complete the "Clear a Non-STM Card Facility or Terminal Loopback Circuit" procedure on page 2-245.

On the G-Series, provisioning a terminal (inward) loopback causes the transmit laser to turn off. If an attached Ethernet device detects the loopback as a loss of carrier, the attached Ethernet device shuts off the transmit laser to the G-Series card. Terminating the transmit laser could raise the CARLOSS alarm because the looped-back G-Series port detects the termination.

If the card does not have a loopback condition, continue to Step 12.

Step 12 If a CARLOSS alarm repeatedly appears and clears, the reappearing alarm could be a result of mismatched circuit sizes in the setup of the manual cross-connect. Perform the following steps if the Ethernet circuit is part of a manual cross-connect by completing the following steps:

Note An ONS 15454 SDH Ethernet manual cross-connect is used when another vendor's equipment sits between ONS nodes, and the OSI/TARP-based equipment does not allow tunneling of the ONS 15454 SDH TCP/IP-based DCC. To circumvent a lack of continuous DCC, the Ethernet circuit is manually cross connected to a channel riding through the non-ONS network.

a. Right-click anywhere in the row of the CARLOSS alarm.

b. Right-click or left-click **Select Affected Circuits** in the shortcut menu that appears.

c. Record the information in the type and size columns of the highlighted circuit.

d. Examine the layout of your network and determine which ONS 15454 SDH and card are hosting the Ethernet circuit at the other end of the Ethernet manual cross-connect by completing the following substeps:

- Log into the node at the other end of the Ethernet manual cross-connect.
- Double-click the Ethernet card that is part of the Ethernet manual cross-connect.
- Click the **Circuits** tab.
- Record the information in the type and size columns of the circuit that is part of the Ethernet manual cross-connect. The cross-connect circuit connects the Ethernet card to an STM-N card at the same node.

e. Determine whether the two Ethernet circuits on each side of the Ethernet manual cross-connect have the same circuit size from the circuit size information you recorded.

f. If one of the circuit sizes is incorrect, complete the "Delete a Circuit" procedure on page 2-243 and reconfigure the circuit with the correct circuit size. Refer to the "Create Circuits and Tunnels" chapter in the *Cisco ONS 15454 SDH Procedure Guide* for detailed procedures to create circuits.

Step 13 If a valid Ethernet signal is present, complete the "Remove and Reinsert (Reseat) Any Card" procedure on page 2-241.

Step 14 If the alarm does not clear, complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the Ethernet card.

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. See the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-230 for commonly used traffic-switching procedures.

Note When you replace a card with the identical type of card, you do not need to make any changes to the database.

Step 15 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.

2.7.47 CARLOSS (GE)

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.48 CARLOSS (ISC)

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.49 CARLOSS (ML100T, ML1000, MLFX)

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

SDH Logical Objects: ML100T, ML1000, MLFX

A Carrier Loss alarm on the ML-Series Ethernet card is the data equivalent of the "LOS (STM1E, STMN)" alarm on page 2-147. The Ethernet port has lost its link and is not receiving a valid signal.

A CARLOSS alarm occurs when the Ethernet port has been configured from the Cisco IOS command-line interface (CLI) as a no-shutdown port and one of the following problems also occurs:

- The cable is not properly connected to the near or far port.
- Autonegotiation is failing.
- The speed (10/100 ports only) is set incorrectly.

Note For information about provisioning ML-Series Ethernet cards from the Cisco IOS interface, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.*

Clear the CARLOSS (ML100T, ML1000, MLFX) Alarm

Step 1 Verify that the LAN cable is properly connected and attached to the correct port on the ML-Series card and on the peer Ethernet port. For more information about fiber connections and terminations, refer to the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15454 SDH Procedure Guide*.

Step 2 If the alarm does not clear, verify that autonegotiation is set properly on the ML-Series card port and the peer Ethernet port.

Step 3 If the alarm does not clear, verify that the speed is set properly on the ML-Series card port and the peer Ethernet port if you are using 10/100 ports.

Step 4 If the alarm does not clear, the Ethernet signal is not valid, but the transmitting device is operational, replace the LAN cable connecting the transmitting device to the Ethernet port.

Step 5 If the alarm does not clear, disable and reenable the Ethernet port by performing a "shutdown" and then a "no shutdown" on the Cisco IOS CLI. Autonegotiation restarts.

Step 6 If the problem persists with the loopback installed, complete the "Remove and Reinsert (Reseat) Any Card" procedure on page 2-241.

Step 7 If the alarm does not clear, complete the "Physically Replace a Traffic Card" procedure on page 2-242.

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. See the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-230 for commonly used traffic-switching procedures.

Note When you replace a card with the identical type of card, you do not need to make any changes to the database.

Step 8 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.

2.7.50 CARLOSS (TRUNK)

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.51 CASETEMP-DEG

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.52 CKTDOWN

The CKTDOWN alarm is not used in this platform in this release. It is reserved for future development.

2.7.53 CLDRESTART

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

SDH Logical Object: EQPT

The Cold Restart condition occurs when a card is physically removed and inserted, replaced, or when the ONS 15454 SDH power is initialized.

Clear the CLDRESTART Condition

Step 1 Complete the "Remove and Reinsert (Reseat) the Standby TCC2/TCC2P Card" procedure on page 2-241.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454 SDH. Plug the wristband cable into the ESD jack located on the middle-right outside edge of the shelf assembly.

Step 2 If the condition fails to clear after the card reboots, complete the "Remove and Reinsert (Reseat) Any Card" procedure on page 2-241.

Step 3 If the condition does not clear, complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the card.

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. See the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-230 for commonly used traffic-switching procedures.

Note When you replace a card with the identical type of card, you do not need to make any changes to the database.

Step 4 If the condition 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.

2.7.54 COMIOXC

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

SDH Logical Object: EQPT

The Input/Output Slot To Cross-Connect Communication Failure alarm can be caused by the cross-connect card when there is a communication failure for a traffic slot.

Clear the COMIOXC Alarm

Step 1 Complete the "Reset a Traffic Card in CTC" procedure on page 2-238 on the card in which the alarm is reported. For the LED behavior, see the "2.9.2 Typical Traffic Card LED Activity During Reset" section on page 2-228.

Step 2 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

Step 3 If the CTC reset does not clear the alarm, move traffic off the reporting cross-connect card. Complete the "Side Switch the Active and Standby Cross-Connect Cards" procedure on page 2-240.

Step 4 Complete the "Remove and Reinsert (Reseat) Any Card" procedure on page 2-241 on the card in which the alarm is reported.

Step 5 If the alarm does not clear, complete the "Physically Replace an In-Service Cross-Connect Card" procedure on page 2-242 for the reporting cross-connect card or complete the "Physically Replace a Traffic Card" procedure on page 2-242 on the card in which the alarm is reported.

Note When you replace a card with the identical type of card, you do not need to make any changes to the database.

Step 6 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.

2.7.55 COMM-FAIL

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

SDH Logical Object: EQPT

The Plug-In Module (card) Communication Failure alarm indicates that there is a communication failure between the TCC2/TCC2P card and the card. The failure could indicate a broken card interface.

Clear the COMM-FAIL Alarm

Step 1 Complete the "Reset a Traffic Card in CTC" procedure on page 2-238 for the reporting card.

Step 2 If the alarm does not clear, complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the card.

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. See the "2.10.3 CTC Card Resetting and Switching" section on page 2-238 for commonly used traffic-switching procedures.

Note When you replace a card with the identical type of card, you do not need to make any changes to the database.

Step 3 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.

2.7.56 CONTBUS-A-18

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

SDH Logical Object: EQPT

A Communication Failure from Controller Slot to Controller Slot alarm for the TCC2/TCC2P card slot to TCC2/TCC2P card slot occurs when the main processor on the TCC2/TCC2P card in the first slot (TCC A) loses communication with the coprocessor on the same card. This applies to the Slot 7 TCC2/TCC2P card.

Clear the CONTBUS-A-18 Alarm

Step 1 Complete the "Remove and Reinsert (Reseat) the Standby TCC2/TCC2P Card" procedure on page 2-241 to make the Slot 11 TCC2/TCC2P card active.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454 SDH. Plug the wristband cable into the ESD jack located on the middle-right outside edge of the shelf assembly.

Step 2 Wait approximately 10 minutes for the Slot 7 TCC2/TCC2P card to reset as the standby TCC2/TCC2P card. Verify that the ACT/SBY LED is correctly illuminated before proceeding to the next step. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

Step 3 Position the cursor over the Slot 11 TCC2/TCC2P card and complete the "Reset an ActiveTCC2/TCC2P Card and Activate the Standby Card" procedure on page 2-239 to return the card to the active state.

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/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. If the Technical Support technician tells you to reseat the card, complete the "Remove and Reinsert (Reseat) Any Card" procedure on page 2-241. If the Technical Support technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Traffic Card" procedure on page 2-242.

2.7.57 CONTBUS-B-18

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

SDH Logical Object: EQPT

A Communication Failure from Controller Slot to Controller Slot alarm for the TCC2/TCC2P card slot to TCC2/TCC2P card slot occurs when the main processor on the TCC2/TCC2P card in the second slot (TCC B) loses communication with the coprocessor on the same card. This applies to the Slot 11 TCC2/TCC2P card.

Clear the CONTBUS-B-18 Alarm

Step 1 Complete the "Reset an ActiveTCC2/TCC2P Card and Activate the Standby Card" procedure on page 2-239 to make the Slot 7 TCC2/TCC2P card active.

Step 2 Wait approximately 10 minutes for the Slot 11 TCC2/TCC2P card to reset as the standby TCC2/TCC2P card. Verify that the ACT/SBY LED is correctly illuminated before proceeding to the next step. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

Step 3 Position the cursor over the Slot 7 TCC2/TCC2P card and complete the "Reset an ActiveTCC2/TCC2P Card and Activate the Standby Card" procedure on page 2-239 to return the Slot 11 TCC2/TCC2P card to the active state.

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/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. If the Technical Support technician tells you to reseat the card, complete the "Remove and Reinsert (Reseat) Any Card" procedure on page 2-241. If the Technical Support technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Traffic Card" procedure on page 2-242.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454 SDH. Plug the wristband cable into the ESD jack located on the middle-right outside edge of the shelf assembly.

2.7.58 CONTBUS-DISABLED

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

SDH Logical Object: EQPT

The CONTBUS-DISABLED alarm is a function of the Release 6.0 enhanced cell bus verification feature. This alarm occurs when a card is defective upon insertion into the chassis or when a card already present in the chassis becomes defective. (That is, the card fails the enhanced cell bus verification test.) The alarm persists as long as the defective card remains in the chassis. When the card is removed, CONTBUS-DISABLED will remain raised for a one-minute wait time. This wait time is designed as a guard period so that the system can distinguish this outage from a briefer card reset communication outage.

If no card is reinserted into the original slot during the wait time, the alarm clears. After this time, a different, nondefective card (not the original card) should be inserted.

When CONTBUS-DISABLED is raised, no message-oriented communication is allowed to or from this slot to the TCC2/TCC2P card (thus avoiding node communication failure).

Caution CONTBUS-DISABLED clears only when the faulty card is removed for one minute. If any card at all is reinserted before the one-minute guard period expires, the alarm does not clear.

CONTBUS-DISABLED overrides the IMPROPRMVL alarm during the one-minute wait period, but afterward IMPROPRMVL can be raised because it is no longer suppressed. IMPROPRMVL is raised after CONTBUS-DISABLED clears if the card is in the node database. If CONTBUS-DISABLED has cleared but IMPROPRMVL is still active, inserting a card will clear the IMPROPRMVL alarm.

Clear the CONTBUS-DISABLED Alarm

Step 1 If the IMPROPRMVL alarm is raised, complete the "Physically Replace a Traffic Card" procedure on page 2-242. (For general information about card installation, refer to the "Install Cards and Fiber-Optic Cable" chapter of the *Cisco ONS 15454 SDH Procedure Guide*.)

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or 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.

2.7.59 CONTBUS-IO-A

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

SDH Logical Object: EQPT

A TCCA to Shelf A Slot Communication Failure alarm occurs when the active Slot 7 TCC2/TCC2P card (TCC A) has lost communication with another card in the shelf. The other card is identified by the Object column in the CTC alarm window.

The CONTBUS-IO-A alarm can appear briefly when the ONS 15454 SDH switches to the protect TCC2/TCC2P card. In the case of a TCC2/TCC2P card protection switch, the alarm clears after the other cards establish communication with the newly active TCC2/TCC2P card. If the alarm persists, the problem lies with the physical path of communication from the TCC2/TCC2P card to the reporting card. The physical path of communication includes the TCC2/TCC2P card, the other card, and the backplane.

Clear the CONTBUS-IO-A Alarm

Step 1 Ensure that the reporting card is physically present in the shelf. Record the card type. Click the **Inventory** tab and view the Eqpt Type column to reveal the provisioned type.

If the actual card type and the provisioned card type do not match, see the "MEA (EQPT)" alarm on page 2-168 for the reporting card.

Step 2 If the alarm object is any single card slot other than the standby Slot 11 TCC2/TCC2P card, perform a CTC reset of the object card. Complete the "Reset a Traffic Card in CTC" procedure on page 2-238. For the LED behavior, see the "2.9.2 Typical Traffic Card LED Activity During Reset" section on page 2-228.

Step 3 If the alarm object is the standby Slot 11 TCC2/TCC2P card, complete the "Reset a Traffic Card in CTC" procedure on page 2-238 for it. The procedure is similar.

Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card. (A reset standby card remains standby.)

Step 4 If CONTBUS-IO-A is raised on several cards at once, complete the "Reset an ActiveTCC2/TCC2P Card and Activate the Standby Card" procedure on page 2-239.

Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card.

Step 5 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

Step 6 If the CTC reset does not clear the alarm, complete the "Remove and Reinsert (Reseat) Any Card" procedure on page 2-241 for the reporting card.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454 SDH. Plug the wristband cable into the ESD jack located on the middle-right outside edge of the shelf assembly.

Step 7 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/techsupport for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of toll-free TAC numbers for your country. If the Technical Support technician tells you to reseat the card, complete the "Remove and Reinsert (Reseat) the Standby TCC2/TCC2P Card" procedure on page 2-241. If the Technical Support technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Traffic Card" procedure on page 2-242.

2.7.60 CONTBUS-IO-B

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

SDH Logical Object: EQPT

A TCC B to Shelf Communication Failure alarm occurs when the active Slot 11 TCC2/TCC2P card (TCC B) has lost communication with another card in the shelf. The other card is identified by the Object column in the CTC alarm window.

The CONTBUS-IO-B alarm could appear briefly when the ONS 15454 SDH switches to the protect TCC2/TCC2P card. In the case of a TCC2/TCC2P card protection switch, the alarm clears after the other cards establish communication with the newly active TCC2/TCC2P card. If the alarm persists, the problem lies with the physical path of communication from the TCC2/TCC2P card to the reporting card. The physical path of communication includes the TCC2/TCC2P card, the other card, and the backplane.

Clear the CONTBUS-IO-B Alarm

Step 1 Ensure that the reporting card is physically present in the shelf. Record the card type. Click the **Inventory** tab and view the Eqpt Type column to reveal the provisioned type.

If the actual card type and the provisioned card type do not match, see the "MEA (EQPT)" alarm on page 2-168 for the reporting card.

Step 2 If the alarm object is any single card slot other than the standby Slot 7 TCC2/TCC2P card, perform a CTC reset of the object card. Complete the "Reset a Traffic Card in CTC" procedure on page 2-238. For the LED behavior, see the "2.9.2 Typical Traffic Card LED Activity During Reset" section on page 2-228.

Step 3 If the alarm object is the standby Slot 7 TCC2/TCC2P card, complete the "Reset a Traffic Card in CTC" procedure on page 2-238 for it. The procedure is similar.

Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card. (A reset standby card remains standby.)

Step 4 If CONTBUS-IO-B is raised on several cards at once, complete the "Reset an ActiveTCC2/TCC2P Card and Activate the Standby Card" procedure on page 2-239.

Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card.

Step 5 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

Step 6 If the CTC reset does not clear the alarm, complete the "Remove and Reinsert (Reseat) Any Card" procedure on page 2-241 for the reporting card.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454 SDH. Plug the wristband cable into the ESD jack located on the middle-right outside edge of the shelf assembly.

Step 7 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/techsupport for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of toll-free TAC numbers for your country. If the Technical Support technician tells you to reseat the card, complete the "Remove and Reinsert (Reseat) the Standby TCC2/TCC2P Card" procedure on page 2-241. If the Technical Support technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Traffic Card" procedure on page 2-242.

2.7.61 CTNEQPT-MISMATCH

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

SDH 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's 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 in the *Cisco ONS 15454 SDH Procedure Guide*.

Clear the CTNEQPT-MISMATCH Condition

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's 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. For example, Slot 8 could be provisioned for an XCVT card, which is shown in the Eqpt Type column, but a different cross-connect card could be physically present in the slot. (This card would be shown in the Actual Eqpt Type column.)

Step 2 Complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the mismatched card.

Step 3 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or 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.

2.7.62 CTNEQPT-PBPROT

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

SDH Logical Object: EQPT

The Interconnection Equipment Failure Protect Cross-Connect Card Payload Bus Alarm indicates a failure of the main payload between the protect ONS 15454 SDH Slot 10 cross-connect card and the reporting traffic card. The cross-connect card and the reporting card are no longer communicating through the backplane. The problem exists in the cross-connect card and the reporting traffic card, or the TCC2/TCC2P card and the backplane.

Note This alarm automatically raises and clears when the Slot 8 cross-connect card is reseated.

Caution Software update on a standby TCC2/TCC2P card can take up to 30 minutes.

Clear the CTNEQPT-PBPROT Alarm

Step 1 If all traffic cards show CTNEQPT-PBPROT alarm, complete the following steps:

a. Complete the "Remove and Reinsert (Reseat) the Standby TCC2/TCC2P Card" procedure on page 2-241 for the standby TCC2/TCC2P card.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454 SDH. Plug the wristband cable into the ESD jack located on the middle-right outside edge of the shelf assembly.

b. If the reseat fails to clear the alarm, complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the standby TCC2/TCC2P card.

Caution Do not physically reseat an active TCC2/TCC2P card. Doing so disrupts traffic.

Step 2 If not all cards show the alarm, perform a CTC reset on the standby STM-64 card. Complete the "Reset a Traffic Card in CTC" procedure on page 2-238. For the LED behavior, see the "2.9.2 Typical Traffic Card LED Activity During Reset" section on page 2-228.

Step 3 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

If the cross-connect reset is not complete and error-free or if the TCC2/TCC2P card reboots automatically, 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 TAC numbers for your country.

Step 4 If the alarm does not clear, complete the "Remove and Reinsert (Reseat) Any Card" procedure on page 2-241 for the standby STM-64 card.

Step 5 Determine whether the card is an active card or standby card in a protection group. Click the node view **Maintenance > Protection** tabs, then click the protection group. The cards and their status are displayed in the list.

Step 6 If the reporting traffic card is the active card in the protection group, complete the "Initiate a 1:1 Card Switch Command" procedure on page 2-233. After you move traffic off the active card, or if the reporting card is standby, continue with the following steps.

Step 7 Complete the "Reset a Traffic Card in CTC" procedure on page 2-238 on the reporting card. For the LED behavior, see the "2.9.2 Typical Traffic Card LED Activity During Reset" section on page 2-228.

Step 8 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

Step 9 If the alarm does not clear, complete the "Remove and Reinsert (Reseat) Any Card" procedure on page 2-241 for the reporting card.

Step 10 Complete the "Initiate a 1:1 Card Switch Command" procedure on page 2-233 to switch traffic back.

Step 11 If the alarm does not clear, complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the reporting traffic card.

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. See the "2.10.2 Protection Switching, Lock Initiation, and Clearing" procedure on page 2-230 for commonly used traffic-switching procedures.

Note When you replace a card with the identical type of card, you do not need to make any changes to the database.

Step 12 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.

2.7.63 CTNEQPT-PBWORK

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

SDH Logical Object: EQPT

The Interconnection Equipment Failure Working Cross-Connect Card Payload Bus alarm indicates a failure in the main payload bus between the ONS 15454 SDH Slot 8 cross-connect card and the reporting traffic card. The cross-connect card and the reporting card are no longer communicating through the backplane. The problem exists in the cross-connect card and the reporting traffic card, or the TCC2/TCC2P card and the backplane.

Note This alarm automatically raises and clears when the ONS 15454 SDH Slot 10 cross-connect card is reseated.

Clear the CTNEQPT-PBWORK Alarm

Step 1 If all traffic cards show CTNEEQPT-PBWORK alarm, complete the following steps:

a. Complete the "Reset an ActiveTCC2/TCC2P Card and Activate the Standby Card" procedure on page 2-239 for the active TCC2/TCC2P card and then complete the "Remove and Reinsert (Reseat) the Standby TCC2/TCC2P Card" procedure on page 2-241.

b. If the reseat fails to clear the alarm, complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the TCC2/TCC2P card.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454 SDH. Plug the wristband cable into the ESD jack located on the middle-right outside edge of the shelf assembly.

Caution Do not physically reseat an active TCC2/TCC2P card; it disrupts traffic.

Step 2 If not all cards show the alarm, complete the "Side Switch the Active and Standby Cross-Connect Cards" procedure on page 2-240 for the active cross-connect card.

Step 3 Complete the "Reset a Traffic Card in CTC" procedure on page 2-238 for the reporting card. For the LED behavior, see the "2.9.2 Typical Traffic Card LED Activity During Reset" section on page 2-228.

Step 4 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

Step 5 If the alarm does not clear, complete the "Remove and Reinsert (Reseat) Any Card" procedure on page 2-241 for the standby cross-connect card.

Step 6 If the alarm does not clear and the reporting traffic card is the active card in the protection group, complete the "Initiate a 1:1 Card Switch Command" procedure on page 2-233. If the card is standby, or if you have moved traffic off the active card, proceed with the following steps.

Step 7 Complete the "Reset a Traffic Card in CTC" procedure on page 2-238 for the reporting card. For the LED behavior, see the "2.9.2 Typical Traffic Card LED Activity During Reset" section on page 2-228.

Step 8 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

Step 9 If the CTC reset does not clear the alarm, complete the "Remove and Reinsert (Reseat) Any Card" procedure on page 2-241 for the reporting card.

Step 10 If you switched traffic, complete the "Initiate a 1:1 Card Switch Command" procedure on page 2-233 to switch it back.

Step 11 If the alarm does not clear, complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the cross-connect card.

Note When you replace a card with the identical type of card, you do not need to make any changes to the database.

Step 12 If the alarm does not clear, complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the reporting traffic card.

Step 13 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or 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.

2.7.64 DATAFLT

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

SDH Logical Object: NE

The Software Data Integrity Fault alarm occurs when the TCC2/TCC2P card exceeds its flash memory capacity.

Caution When the system reboots, the last configuration entered is not saved.

Clear the DATAFLT Alarm

Step 1 Complete the "Remove and Reinsert (Reseat) the Standby TCC2/TCC2P Card" procedure on page 2-241.

Step 2 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.

2.7.65 DBOSYNC

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

SDH Logical Object: NE

The Standby Database Out Of Synchronization alarm occurs when the standbyTCC2/TCC2P card "To be Active" database does not synchronize with the active database on the active TCC2/TCC2P card.

Caution If you reset the active TCC2/TCC2P card while this alarm is raised, you lose current provisioning.

Clear the DBOSYNC Alarm

Step 1 Save a backup copy of the active TCC2/TCC2P card database. Refer to the "Maintain the Node" chapter in the *Cisco ONS 15454 SDH Procedure Guide* for procedures.

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

a. In node view, 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.

Step 3 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.

2.7.66 DS3-MISM

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

SDH Logical Object: DS3

The DS-3 Frame Format Mismatch condition indicates that a frame format mismatch on a signal transiting the ONS 15454 SDH DS3i-N-12 card. The condition occurs when the provisioned line type and incoming signal frame format type do no match. For example, if the line type for a DS3i-N-12 card is set to C Bit and the incoming signal frame format is detected as M13, then the ONS 15454 SDH reports a DS3-MISM condition.

Clear the DS3-MISM Condition

Step 1 Display the CTC card view for the reporting DS3i-N-12 card.

Step 2 Click the **Provisioning > Line** tabs.

Step 3 For the row on the appropriate port, verify that the Line Type column is set to match the expected incoming signal (C Bit or M13).

Step 4 If the Line Type drop-down list does not match the expected incoming signal, select the correct Line Type in the drop-down list.

Step 5 Click **Apply**.

Step 6 If the condition does not clear after the user verifies that the provisioned line type matches the expected incoming signal, use an optical test set to verify that the actual signal coming into the ONS 15454 SDH matches the expected incoming signal. For specific procedures to use the test set equipment, consult the manufacturer.

Step 7 If the condition 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.

2.7.67 DSP-COMM-FAIL

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.68 DSP-FAIL

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.69 DUP-IPADDR

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

SDH Logical Object: NE

The Duplicate IP Address alarm indicates that the alarmed node IP address is already in use within the same DCC area. When this happens, CTC no longer reliably connects to either node. Depending on how the packets are routed, CTC could connect to either node (having the same IP address). If CTC has connected to both nodes before they shared the same address, it has two distinct NodeModel instances (keyed by the node ID portion of the MAC address).

Clear the DUP-IPADDR Alarm

Step 1 Isolate the alarmed node from the other node having the same address by completing the following steps:

a. Connect to the alarmed node using the Craft port on the ONS 15454 SDH chassis.

b. Begin a CTC session.

c. In the login dialog window, uncheck the **Network Discovery** check box.

Step 2 In node view, click the **Provisioning > Network > General** tabs.

Step 3 In the IP Address field, change the IP address to a unique number.

Step 4 Click **Apply**.

Step 5 Restart any CTC sessions that are logged into either of the formerly duplicated node IDs. (For procedures to log in or log out, refer to the "Set Up PC and Log Into the GUI" chapter in the *Cisco ONS 15454 SDH Procedure Guide*.)

Step 6 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or 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.

2.7.70 DUP-NODENAME

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

SDH Logical Object: NE

The Duplicate Node Name alarm indicates that the alarmed node's alphanumeric name is already being used within the same DCC area.

Clear the DUP-NODENAME Alarm

Step 1 In node view, click the **Provisioning > General > General** tabs.

Step 2 In the Node Name field, enter a unique name for the node.

Step 3 Click **Apply**.

Step 4 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or 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.

2.7.71 EHIBATVG

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

SDH Logical Object: PWR

The Extreme High Voltage Battery alarm occurs in a –48 VDC or –60 VDC environment when the voltage on a battery lead input exceeds the extreme high power threshold. This threshold, with a value of –56.7 VDC in –48 VDC systems or –72 VDC in –60 VDC systems, is user-provisionable. The alarm remains raised until the voltage remains under the threshold for 120 seconds. (For information about changing this threshold, refer to the "Turn Up Node" chapter in the *Cisco ONS 15454 SDH Procedure Guide*.)

Clear the EHIBATVG Alarm

Step 1 The problem is external to the ONS 15454 SDH. Troubleshoot the power source supplying the battery leads.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or 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 to report a Service-Affecting (SA) problem.

2.7.72 ELWBATVG

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

SDH Logical Object: PWR

The Extreme Low Voltage Battery alarm occurs in a –48 VDC environment when the voltage on the battery feeds is extremely low or has been lost, and power redundancy is no longer guaranteed. The threshold for this alarm is –40.5 VDC in –48 VDC systems or –50 VDC in –60 VDC systems. The alarm clears when voltage remains above –40.5 VDC for 120 seconds.

Clear the ELWBATVG Alarm

Step 1 The problem is external to the ONS 15454 SDH. Troubleshoot the power source supplying the battery leads.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or 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 to report a Service-Affecting (SA) problem.

2.7.73 EOC

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

SDH Logical Object: STMN

DWDM Logical Object: TRUNK

The SDH Data Communications Channel (DCC) Termination Failure alarm occurs when the ONS 15454 SDH loses its data communications channel. Although this alarm is primarily SDH, 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 SDH overhead. The bytes convey information about operation, administration, maintenance, and provisioning (OAM&P). The ONS 15454 SDH uses the DCC on the SDH 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 **On the OC192 LR/STM64 LH 1550 card, the laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. The laser is off when the safety key is off (labeled 0).** Statement 293

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

Warning **Use of controls, adjustments, or performing procedures other than those specified could result in hazardous radiation exposure.** Statement 1057

Note If a circuit shows 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.

Note For more information about DWDM cards, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Clear the EOC Alarm

Step 1 If the "LOS (DS1, DS3)" alarm on page 2-143 is also reported, complete the "Clear the LOS (STM1E, STMN) Alarm" procedure on page 2-148.

Step 2 If the "SFTWDOWN" condition on page 2-199 is reported, complete the "Clear the SF (DS3, E1, E3, E4, STMN) Condition" procedure on page 2-197.

Step 3 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. For more information about STM-N fiber connections and terminations, refer to the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15454 SDH Procedure Guide*.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454 SDH. Plug the wristband cable into the ESD jack located on the middle-right outside 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 4 When the LEDs on the cards are correctly illuminated, complete the "Verify or Create Node RS-DCC Terminations" procedure on page 2-244 to verify that the DCC is provisioned for the ports at both ends of the fiber span.

Step 5 Repeat Step 4 at the adjacent nodes.

Step 6 If DCC is provisioned for the ends of the span, verify that the port is active and in service by completing the following steps:

- **a.** Confirm that the card shows a green LED in CTC or on the physical card.

  A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.
- **b.** To determine whether the port is in service, double-click the card in CTC to display the card view.
- **c.** For an STM-N card, click the **Provisioning > Line** tabs. For the OSCM card, click the **Provisioning > STM-1 Line** tabs.
- **d.** Verify that the **Admin State column** lists the port as **Unlocked**.
- **e.** If the **Admin State** column lists the port as locked,maintenance or locked,disabled, click the column and click **Unlocked** from the drop-down list. 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 an STM-N card. It could be necessary to manually switch traffic carrying circuits over to a protection path. Refer to the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-230 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. See the "1.12.3 Optical Card Transmit and Receive Levels" section on page 1-135 for non-DWDM card levels.

Step 9 If budget loss is within parameters, ensure that fiber connectors are securely fastened and properly terminated. For more information refer to "Install Cards and Fiber-Optic Cables" chapter in the *Cisco ONS 15454 SDH Procedure Guide*.

Step 10 If fiber connectors are properly fastened and terminated, complete the "Reset an ActiveTCC2/TCC2P Card and Activate the Standby Card" procedure on page 2-239.

Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card.

Resetting the active TCC2/TCC2P card switches control to the standby TCC2/TCC2P card. If the alarm clears when the ONS 15454 SDH node switches to the standby TCC2/TCC2P card, the user can assume that the previously active card is the cause of the alarm.

Step 11 If the TCC2/TCC2P 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 12 Recreate the RS-DCC termination. Refer to the "Turn Up Network" chapter in the *Cisco ONS 15454 SDH Procedure Guide* for procedures.

Step 13 Verify that both ends of the DCC have been recreated at the optical ports.

Step 14 If the alarm has not cleared, 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. If the Technical Support technician tells you to reseat the card, complete the "Remove and Reinsert (Reseat) Any Card" procedure on page 2-241. If the Technical Support technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Traffic Card" procedure on page 2-242.

2.7.74 EOC-L

The EOC-L alarm is not used in this platform in this release. It is reserved for future development.

2.7.75 EQPT

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

SDH Logical Objects: AICI-AEP, AICI-AIE, EQPT

DWDM Logical Object: PPM

An Equipment Failure alarm indicates that a hardware failure has occurred on the reporting card.

If the EQPT alarm occurs with a BKUPMEMP alarm, see the "2.7.41 BKUPMEMP" section on page 2-52. The BKUPMEMP procedure also clears the EQPT alarm.

Clear the EQPT Alarm

Step 1 If traffic is active on the alarmed port, you could need to switch traffic away from it. See the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-230 for commonly used traffic-switching procedures.

Step 2 Complete the "Reset a Traffic Card in CTC" procedure on page 2-238 for the reporting card. For the LED behavior, see the "2.9.2 Typical Traffic Card LED Activity During Reset" section on page 2-228.

Step 3 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. Verify the LED status. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

Step 4 If the CTC reset does not clear the alarm, complete the "Remove and Reinsert (Reseat) Any Card" procedure on page 2-241 for the reporting card.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454 SDH. Plug the wristband cable into the ESD jack located on the middle-right outside edge of the shelf assembly.

Step 5 If the physical reseat of the card fails to clear the alarm, complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the reporting card.

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. See the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-230 for commonly used traffic-switching procedures.

Note When you replace a card with the identical type of card, you do not need to make any changes to the database.

Step 6 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.

2.7.76 EQPT-DIAG

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

SDH Logical Object: EQPT

An Equipment-Diagnostic Failure 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

Step 1 If traffic is active on the alarmed card, you could need to switch traffic away from it. Refer to the "2.10.5 Generic Signal and Circuit Procedures" section on page 2-243 for procedures.

Step 2 Complete the "Remove and Reinsert (Reseat) Any Card" procedure on page 2-241 for the alarmed card.

Caution If the card carries live traffic, reseating it can affect this traffic.

Step 3 If the alarm does not clear, complete the "Physically Replace a Traffic Card" procedure on page 2-242 if it is raised against a traffic card, or complete the "Physically Replace an In-Service Cross-Connect Card" procedure on page 2-242 if the alarm is raised against the cross-connect card.

Step 4 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.

2.7.77 EQPT-MISS

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

SDH 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 not fully inserted. It could also indicate that the ribbon cable connecting the alarm interface extension (AIE) to the system board is bad.

Clear the EQPT-MISS Alarm

Step 1 If the alarm is reported against the fan, verify that the fan-tray assembly is present.

Step 2 If the fan-tray assembly is present, complete the "Replace the Fan-Tray Assembly" procedure on page 2-247.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454 SDH. Plug the wristband cable into the ESD jack located on the middle-right outside edge of the shelf assembly.

Step 3 If no fan-tray assembly is present, obtain a fan-tray assembly and install it using the "Install the Fan-Tray Assembly," procedure in the "Maintain the Node" chapter in the *Cisco ONS 15454 SDH Procedure Guide*.

Step 4 If the alarm does not clear, replace the ribbon cable from the AIE to the system board with a known-good ribbon cable.

Step 5 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or 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.

2.7.78 ERROR-CONFIG

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

SDH Logical Object: EQPT

The Error in Startup Configuration alarm applies to the ML-Series Ethernet cards. These cards process startup configuration files line by line. If one or more lines cannot be executed, the error causes the ERROR-CONFIG alarm. ERROR-CONFIG is not caused by hardware failure.

The typical reasons for an errored startup file are:

- The user stored the configuration for one type of ML-Series card in the database and then installed another type in its slot.
- The configuration file contained a syntax error on one of the lines.

Note For information about provisioning the ML-Series Ethernet cards from the Cisco IOS interface, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.*

Clear the ERROR-CONFIG Alarm

Step 1 If you have a different type of ML-Series card specified in the startup configuration file than what you have installed, create the correct startup configuration.

Follow the card provisioning instructions in the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.*

Step 2 Upload the configuration file to the TCC2/TCC2P card by completing the following steps:

a. In node view, right-click the ML-Series card graphic.

b. Choose **IOS Startup Config** from the shortcut menu.

c. Click **Local > TCC** and navigate to the file location in the Open dialog box.

Step 3 Complete the "Reset a Traffic Card in CTC" procedure on page 2-238.

Step 4 If the alarm does not clear or if your configuration file was correct according to the installed card, start an Cisco IOS CLI for the card by completing the following steps:

a. Right click the ML-Series card graphic in node view.

b. Choose **Open IOS Connection** from the shortcut menu.

Note Open IOS Connection is not available unless the ML-Series card is physically installed in the shelf.

Follow the card provisioning instructions in the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327* to correct the errored configuration file line.

Step 5 Execute the following CLI command:

```
copy run start
```

The command copies the new card configuration into the database and clears the alarm.

Step 6 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.

2.7.79 ETH-LINKLOSS

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

SDH 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.AlarmMissingBackplane LAN field in NE defaults is enabled.
- The node is configured as a gateway network element (GNE).
- The backplane LAN cable is removed.

Clear the ETH-LINKLOSS Condition

Step 1 To clear this alarm, reconnect the backplane cable. Refer to the "Install the Shelf and FMECS" chapter in the *Cisco ONS 15454 SDH Procedure 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 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.

2.7.80 E-W-MISMATCH

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

SDH Logical Object: STMN

A Procedural Error Misconnect East/West Direction alarm occurs when nodes in a ring have an east slot misconnected to another east slot or a west slot misconnected to another west slot. In most cases, the user did not connect the fibers correctly or the ring provisioning plan was flawed. You can physically reconnect the cable to the correct slots to clear the E-W-MISMATCH alarm. Alternately, you can delete and recreate the span in CTC to change the west line and east line designations. The CTC method clears the alarm, but could change the traditional east-west node connection pattern of the ring.

Note The E-W-MISMATCH alarm also appears during the initial setup of a ring with its east-west slots and ports configured correctly. In this instance, the alarm clears itself shortly after the ring setup is complete.

Note The lower-numbered slot on a node is traditionally labeled the west slot. The higher numbered slot is traditionally labeled the east slot. For example, Slot 1 is West and Slot 14 is East.

Note The physical switch procedure is the recommend method of clearing the E-W-MISMATCH alarm. The physical switch method reestablishes the logical pattern of connection in the ring. However, you can also use CTC to recreate the span and identify the misconnected slots as east and west. The CTC method is useful when the misconnected node is not geographically near the troubleshooter.

Clear the E-W-MISMATCH Alarm with a Physical Switch

Step 1 Diagram the ring setup, including nodes and spans, on a piece of paper or white board.

Step 2 In node view, click **View > Go to Network View**.

Step 3 Label each of the nodes on the diagram with the same name that appears on the network map.

Step 4 Right-click each span to display the node name/slot/port for each end of the span.

Step 5 Label the span ends on the diagram with the same information. For example, with Node 1/Slot 12/Port 1—Node 2/Slot 6/Port 1 (2F MS-SPRing STM-16, Ring Name=0), label the end of the span that connects Node 1 and Node 2 at the Node 1 end as Slot 12/Port 1. Label the Node 2 end of that same span Slot 6/ Port 1.

Step 6 Repeat Steps 4 and 5 for each span on your diagram.

Step 7 Label the highest slot at each node east and the lowest slot at each node west.

Step 8 Examine the diagram. You should see a clockwise pattern of west slots connecting to east slots for each span. Refer to the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15454 SDH Procedure Guide* for more information about configuring the system.

Step 9 If any span has an east-to-east or west-to-west connection, physically switching the fiber connectors from the card that does not fit the pattern to the card that continues the pattern should clear the alarm.

Warning **On the OC192 LR/STM64 LH 1550 card, the laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. The laser is off when the safety key is off (labeled 0).** Statement 293

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

Warning **Use of controls, adjustments, or performing procedures other than those specified could result in hazardous radiation exposure.** Statement 1057

Step 10 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.

Clear the E-W-MISMATCH Alarm in CTC

Step 1 Log into the misconnected node. A misconnected node has both ring fibers connecting it to its neighbor nodes misconnected.

Step 2 Click the **Maintenance > MS-SPRing** tabs.

Step 3 From the row of information for the fiber span, complete the "Identify an MS-SPRing Ring Name or Node ID Number" procedure on page 2-229 to identify the node ID, ring name, and the slot and port in the East Line column and West Line column. Record the above information.

Step 4 Click **View > Go to Network View**.

Step 5 Delete and recreate the MS-SPRing by completing the following steps:

- **a.** Click the **Provisioning > MS-SPRing** tabs.
- **b.** Click the row from Step 3 to select it and click **Delete**.
- **c.** Click **Create**.
- **d.** Fill in the ring name and node ID from the information collected in Step 3.
- **e.** Click **Finish**.

Step 6 Display node view and click the **Maintenance > MS-SPRing** tabs.

Step 7 Change the West Line drop-down list to the slot you recorded for the East Line in Step 3.

Step 8 Change the East Line drop-down list to the slot you recorded for the West Line in Step 3.

Step 9 Click **OK**.

Step 10 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.

2.7.81 EXCCOL

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

SDH Logical Object: EQPT

The Excess Collisions on the LAN alarm indicates that too many collisions are occurring between data packets on the network management LAN, and communications between the ONS 15454 SDH and CTC could be affected. The network management LAN is the data network connecting the workstation running the CTC software to the TCC2/TCC2P card. The problem causing the alarm is external to the ONS 15454 SDH.

Troubleshoot the network management LAN connected to the TCC2/TCC2P 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

Step 1 Verify that the network device port connected to the TCC2/TCC2P card has a flow rate set to 10 Mb, half-duplex.

Step 2 If the alarm does not clear, troubleshoot the network device connected to the TCC2/TCC2P card and the network management LAN.

Step 3 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or 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.

2.7.82 EXERCISE-RING-FAIL

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

SDH Logical Object: STMN

The Exercise Ring command issues ring protection switching of the requested channel without completing the actual bridge and switch. The EXERCISE-RING-FAIL condition is raised if the command was issued and accepted but the exercise did not take place.

Note If the exercise command gets rejected due to the existence of a higher priority condition in the ring, EXERCISE-RING-FAIL is Not Reported (NR).

Clear the EXERCISE-RING-FAIL Condition

Step 1 Look for and clear, if present, the "LOF (DS1, DS3, E1, E4, STM1E, STMN)" alarm on page 2-138, the "LOS (STM1E, STMN)" alarm on page 2-147, or MS-SPRing alarms.

Step 2 Reissue the Exercise Ring command by completing the following steps:

a. Click the **Maintenance > MS-SPRing** tabs.

b. Click the row of the affected ring under the West Switch column.

c. Select **Exercise Ring** in the drop-down list.

Step 3 If the condition does not clear, log into the Cisco 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.

2.7.83 EXERCISE-SPAN-FAIL

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

SDH Logical Object: STMN

The Exercise Span command issues span switching of the requested channel without completing the actual bridge and switch. The EXERCISE-SPAN-FAIL alarm is raised if the command was issued and accepted but the exercise did not take place.

Note If the exercise command gets rejected due to the existence of a higher priority condition in the span or ring, EXERCISE-SPAN-FAIL is Not Reported (NR).

Clear the EXERCISE-SPAN-FAIL Condition

Step 1 Look for and clear, if present, the "LOF (DS1, DS3, E1, E4, STM1E, STMN)" alarm on page 2-138, the "LOS (STM1E, STMN)" alarm on page 2-147, or a MS-SPRing alarm.

Step 2 Complete the "Initiate an Exercise Ring Switch on an MS-SPRing" procedure on page 2-237.

Step 3 If the condition does not clear, log into the Cisco 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.

2.7.84 EXT

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

SDH Logical Object: ENVALRM

An External Facility alarm is detected externally from the node because an environmental alarm is present. For example, an open door or flooding can cause the alarm.

Clear the EXT Alarm

Step 1 In node view, double-click the MIC-A/P card to display the card view.

Step 2 Click the **Maintenance** tab to gather further information about the EXT alarm.

Step 3 Perform your standard operating procedure for this environmental condition.

Step 4 If the alarm does not clear, log into the Cisco 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.

2.7.85 EXTRA-TRAF-PREEMPT

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

SDH Logical Object: STMN

An Extra Traffic Preempted alarm occurs on STM-N cards in two-fiber and four-fiber MS-SPRings because low-priority traffic directed to the protect system has been preempted by a working system protection switch.

Clear the EXTRA-TRAF-PREEMPT Alarm

Step 1 Verify that the protection switch has occurred by verifying that the Conditions window shows the switch.

Step 2 If a ring switch has occurred, clear the alarm on the working system by following the appropriate alarm procedure in this chapter. For more information about protection switches, refer to the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-230.

Step 3 If the alarm does not clear, log into the Cisco 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 to report a Service-Affecting (SA) problem.

2.7.86 FAILTOSW

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

SDH Logical Objects: EQPT, STMN, VCMON-HP

DWDM Logical Objects: 2R, ESCON, FC, GE, ISC, TRUNK

The Failure to Switch to Protection Facility condition occurs when a working or protect electrical or optical 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.

Clear the FAILTOSW Condition

Step 1 Look up and troubleshoot the higher-priority alarm. Clearing the higher-priority condition frees the card and clears the FAILTOSW.

Note A higher-priority alarm is an alarm raised on the working electrical or optical card using the 1:N card protection group. The working electrical or optical card is reporting an alarm but not reporting a FAILTOSW condition.

Step 2 If the condition does not clear, replace the working electrical or optical card that is reporting the higher priority alarm by following the "Physically Replace a Traffic Card" procedure on page 2-242. This card is the working electrical or optical card using the protect card and not reporting FAILTOSW.

Replacing the working electrical or optical 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.

Note Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-230 for commonly used traffic-switching procedures.

Note When you replace a card with the identical type of card, you do not need to make any changes to the database.

Step 3 If the condition does not clear, log into the Cisco 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.

2.7.87 FAILTOSW-HO

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

SDH 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

Step 1 Complete the "Clear the FAILTOSW Condition" procedure on page 2-88.

Step 2 If the condition does not clear, log into the Cisco 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.

2.7.88 FAILTOSW-LO

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

SDH Logical Objects: VCMON-HP

The Low-Order Failure to Switch to Protection condition occurs when a low-order path circuit fails to switch to the working or protect electrical circuit using the MANUAL command.

Clear the FAILTOSW-LO Condition

Step 1 Complete the "Clear the FAILTOSW Condition" procedure on page 2-88.

Step 2 If the condition does not clear, log into the Cisco 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.

2.7.89 FAILTOSWR

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

SDH Logical Object: STMN

The Fail to Switch to Protection Ring condition occurs when a ring switch did not complete because of internal APS problems.

FAILTOSWR clears in any of the following situations:

- A physical card pull of the active TCC2/TCC2P card (done under the supervision of Cisco Technical Support).
- A node power cycle.

- A higher priority event, such as an external switch command.
- The next ring switch succeeds.
- The cause of the APS switch such as the "SD (DS1, DS3, E1, E3, E4, STM1E, STMN)" condition on page 2-192 or the "SF (DS1, DS3, E1, E3, E4, STMN)" condition on page 2-196 clears.

Warning **On the OC192 LR/STM64 LH 1550 card, the laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. The laser is off when the safety key is off (labeled 0).** Statement 293

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

Warning **Use of controls, adjustments, or performing procedures other than those specified could result in hazardous radiation exposure.** Statement 1057

Note If a circuit shows a partial 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 FAILTOSWR Condition on a Four-Fiber MS-SPRing Configuration

Step 1 Perform the EXERCISE RING command on the reporting card by completing the following steps:

a. Click the **Maintenance > MS-SPRing** tabs.

b. Click the row of the affected ring under the West Switch column.

c. Select **Exercise Ring** in the drop-down list.

Step 2 If the condition does not clear, from the view menu, choose **Go to Network View**.

Step 3 Look for alarms on STM-N cards that make up the ring or span and troubleshoot these alarms.

Step 4 If clearing other alarms does not clear the FAILTOSWR condition, log into the near-end node.

Step 5 Click the **Maintenance > MS-SPRing** tabs.

Step 6 Record the STM-N cards listed under West Line and East Line. Ensure that these STM-N cards and ports are active and in service by completing the following steps:

a. Verify the LED status: A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

b. Double-click the card in CTC to display the card view.

c. Click the **Provisioning > Line** tabs.

d. Verify that the **Admin State column** lists the port as **Unlocked**.

e. If the **Admin State** column lists the port as locked,maintenance or locked,disabled, click the column and choose **Unlocked**. Click **Apply**.

Step 7 If the STM-N cards are active and in service, verify fiber continuity to the ports on the recorded cards. To verify fiber continuity, follow site practices.

Step 8 If fiber continuity to the ports is good, 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.

Caution Using an optical test set disrupts service on the STM-N card. It could be necessary to manually switch traffic carrying circuits over to a protection path. Refer to the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-230 for commonly used switching procedures.

Step 9 If the signal is valid, clean the fiber according to site practice. If no site practice exists, complete the procedure for cleaning optical connectors in the "Maintain the Node" chapter of the *Cisco ONS 15454 SDH Procedure Guide*.

Step 10 If cleaning the fiber does not clear the condition, verify that the power level of the optical signal is within the STM-N card receiver specifications. The "1.12.3 Optical Card Transmit and Receive Levels" section on page 1-135 lists these specifications.

Step 11 Repeat Steps 7 through 10 for any other ports on the card.

Step 12 If the optical power level for all STM-N cards is within specifications, complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the protect standby STM-N card.

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. See the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-230 for commonly used traffic-switching procedures.

Note When you replace a card with the identical type of card, you do not need to make any changes to the database.

Step 13 If the condition does not clear after you replace the MS-SPRing cards on the node one by one, repeat Steps 4 through 12 for each of the nodes in the ring.

Step 14 If the condition does not clear, log into the Cisco 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.

2.7.90 FAILTOSWS

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

SDH Logical Object: STMN

The Failure to Switch to Protection Span condition signals an APS span switch failure. For a four-fiber MS-SPRing, a failed span switch initiates a ring switch. If the ring switch occurs, the FAILTOSWS condition does not appear. If the ring switch does not occur, the FAILTOSWS condition appears. FAILTOSWS clears when one of the following situations occurs:

- A physical card pull of the active TCC2/TCC2P card (done under the supervision of Cisco Technical Support).
- A node power cycle.
- A higher priority event such as an external switch command.
- The next span switch succeeds.
- The cause of the APS switch such as the "SD (DS1, DS3, E1, E3, E4, STM1E, STMN)" condition on page 2-192 or the "SF (DS1, DS3, E1, E3, E4, STMN)" condition on page 2-196 clears.

Clear the FAILTOSWS Condition

Step 1 Perform the EXERCISE SPAN command on the reporting card by completing the following steps:

a. Click the **Maintenance > MS-SPRing** tabs.

b. Determine whether the card you would like to exercise is the east card or the west card.

c. Click the row of the affected span under the East Switch or West Switch column.

d. Select **Exercise Span** in the drop-down list.

Step 2 If the condition does not clear, from the view menu, choose **Go to Network View**.

Step 3 Look for alarms on STM-N cards that make up the ring or span and troubleshoot these alarms.

Step 4 If clearing other alarms does not clear the FAILTOSWS condition, log into the near-end node.

Step 5 Click the **Maintenance > MS-SPRing** tabs.

Step 6 Record the STM-N cards listed under West Line and East Line. Ensure that these STM-N cards are active and in service by completing the following steps:

a. Verify the LED status: A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

b. To determine whether the STM-N port is in service, double-click the card in CTC to display the card view.

c. Click the **Provisioning > Line** tabs.

d. Verify that the **Admin State column** lists the port as **Unlocked**.

e. If the **Admin State** column lists the port as locked,maintenance or locked,disabled, click the column and choose **Unlocked**. Click **Apply**.

Step 7 If the STM-N cards are active and in service, verify fiber continuity to the ports on the recorded cards. To verify fiber continuity, follow site practices.

Step 8 If fiber continuity to the ports is good, 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.

Caution Using an optical test set disrupts service on the STM-N card. It could be necessary to manually switch traffic carrying circuits over to a protection path. Refer to the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-230 for commonly used switching procedures.

Step 9 If the signal is valid, clean the fiber according to site practice. If no site practice exists, complete the procedure for cleaning optical connectors in the "Maintain the Node" chapter of the *Cisco ONS 15454 SDH Procedure Guide*.

Step 10 If cleaning the fiber does not clear the condition, verify that the power level of the optical signal is within the STM-N card receiver specifications. The "1.12.3 Optical Card Transmit and Receive Levels" section on page 1-135 lists these specifications.

Step 11 Repeat Steps 7 through 10 for any other ports on the card.

Step 12 If the optical power level for all STM-N cards is within specifications, complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the protect standby STM-N card.

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. See the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-230 for commonly used traffic-switching procedures.

Note When you replace a card with the identical type of card, you do not need to make any changes to the database.

Step 13 If the condition does not clear after you replace the MS-SPRing cards on the node one by one, follow Steps 4 through 12 for each of the nodes in the ring.

Step 14 If the condition does not clear, log into the Cisco 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.

2.7.91 FAN

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

SDH 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 15454 SDH 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 ONS 15454 SDH. 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.

Clear the FAN Alarm

Step 1 Determine whether the air filter needs replacement. Complete the "Inspect, Clean, and Replace the Reusable Air Filter" procedure on page 2-245.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454 SDH. Plug the wristband cable into the ESD jack located on the middle-right outside edge of the shelf assembly.

Step 2 If the filter is clean, complete the "Remove and Reinsert a Fan-Tray Assembly" procedure on page 2-246.

Note The fan-tray assembly should run immediately when correctly inserted.

Step 3 If the fan does not run or the alarm persists, complete the "Replace the Fan-Tray Assembly" procedure on page 2-247.

Step 4 If the replacement fan-tray assembly does not operate correctly, log into the Cisco 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.

2.7.92 FC-NO-CREDITS

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

SDH Logical Object: FCMR

DWDM Logical Objects: FC, TRUNK

The Fibre Channel Distance Extension Credit Starvation alarm occurs on storage access networking (SAN) Fibre Channel/Fiber Connectivity (FICON) FC_MR-4 cards when the congestion prevents the generic framing procedure (GFP) transmitter from sending frames to the FC_MR-4 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.) The alarm is raised in conjunction with the GFP-NO-BUFFERS alarm. For example, if the FC-NO-CREDITS alarm is generated at an FC_MR-4 data port, a GFP-NO-BUFFERS alarm could be raised at the upstream remote FC_MR-4 data port.

Clear the FC-NO-CREDITS Alarm

Step 1 If the port is connected to a Fibre Channel/FICON switch, make sure it is configured for interoperation mode. Follow the manufacturer's instructions for this function.

Step 2 If the port is not connected to a switch, turn off Autodetect credits by completing the following steps:

a. Double-click the FC_MR-4 card to display the card view.

b. Click **Provisioning > Port > General.**

c. Under **Admin State**, click the cell and choose **Locked, maintenance**.

d. Click the **Provisioning > Port > Distance Extension** tabs.

e. Uncheck the **Autodetect Credits** column check box.

f. Click **Apply**.

g. Click **Provisioning > Port > General.**

h. Under Admin State, click the cell and choose **Unlocked**.

i. Click **Apply**.

Step 3 Program the credits available value based on the buffers available on the connected equipment by completing the following steps:

Note NumCredits 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 FC_MR-4 card to display the card view.

b. Click the **Provisioning > Port > Distance Extension** tabs.

c. Enter a new value in the **Credits Available** column.

d. Click **Apply**.

Step 4 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or log into http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of toll-free TAC numbers for your country in order to report a Service-Affecting (SA) problem.

2.7.93 FE-AIS

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

SDH Logical Object: E3

The Far-End AIS condition accompanies the "AIS" condition on page 2-31 at the far-end node. An AIS usually occurs in conjunction with a downstream "LOS (STM1E, STMN)" alarm on page 2-147.

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 FE-AIS Condition

Step 1 Complete the "Clear the AIS Condition" procedure on page 2-31.

Step 2 If the condition does not clear, log into the Cisco 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.

2.7.94 FEC-MISM

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.95 FE-E1-MULTLOS

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

SDH Logical Object: E3

The Far End Multiple E-1 LOS Detected on an E1-42 card condition occurs when multiple E1 inputs detect signal loss on a far-end E1-42 port at the far-end node.

The prefix FE means the main alarm is occurring at the far-end node and not at the node reporting the FE-E1-MULTLOS condition. Troubleshoot the FE alarm or condition by troubleshooting the main alarm at its source. The secondary alarms or conditions clear when the main alarm clears.

Clear the FE-E1-MULTLOS Condition

Step 1 To troubleshoot an FE condition, determine which node and card link 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 links directly to the card reporting the FE condition.

Step 3 Clear the main alarm. Refer to the appropriate alarm section in this chapter for troubleshooting instructions.

Step 4 If the condition does not clear, log into the Cisco 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.

2.7.96 FE-E1-NSA

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

SDH Logical Object: E3

The Far End E1 Equipment Failure Non-Service-Affecting (NSA) condition occurs when a far-end E-1 equipment failure occurs, but does not affect service because the port is protected and traffic is able to switch to the protect port.

Clear the FE-E1-NSA Condition

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-AIS condition from the card in Slot 12 of Node 1 could link to the main AIS 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 Clear the main alarm. Refer to the appropriate alarm section in this chapter for troubleshooting instructions.

Step 4 If the condition does not clear, log into the Cisco 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.

2.7.97 FE-E1-SA

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

SDH Logical Object: E3

The Far End E-1 Equipment Failure Service-Affecting (SA) condition occurs when a far-end E-1 equipment failure occurs and affects service because traffic is unable to switch to the protect port.

Clear the FE-E1-SA Condition

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-AIS condition from the card in Slot 12 of Node 1 could link to the main AIS 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 Clear the main alarm. Refer to the appropriate alarm section in this chapter for troubleshooting instructions.

Step 4 If the condition does not clear, log into the Cisco 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.

2.7.98 FE-E1-SNGLLOS

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

SDH Logical Object: E3

The Far End Single E-1 LOS on the E-3 condition occurs when one of the E3-12 ports on the far end detects an LOS.

Clear the FE-E1-SNGLLOS Condition

Step 1 To troubleshoot an FE condition, determine which node and card link 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 links directly to the card reporting the FE condition.

Step 3 Clear the main alarm. Refer to the appropriate alarm section in this chapter for troubleshooting instructions.

Step 4 If the condition does not clear, log into the Cisco 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.

2.7.99 FE-E3-NSA

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

SDH Logical Object: E3

The Far End E3 Equipment Failure Non-Service-Affecting (NSA) condition occurs when a far-end E-3 equipment failure occurs, but does not affect service because the port is protected and traffic is able to switch to the protect port.

Clear the FE-E3-NSA Condition

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-AIS condition from the card in Slot 12 of Node 1 could link to the main AIS 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 Clear the main alarm. Refer to the appropriate alarm section in this chapter for troubleshooting instructions.

Step 4 If the condition does not clear, log into the Cisco 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.

2.7.100 FE-E3-SA

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

SDH Logical Object: E3

The Far End E3 Equipment Failure Service Affecting condition occurs when a far-end E-3 equipment failure occurs and affects service because traffic is unable to switch to the protect port.

Clear the FE-E3-SA Condition

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-AIS condition from the card in Slot 12 of Node 1 could link to the main AIS 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 Clear the main alarm. Refer to the appropriate alarm section in this chapter for troubleshooting instructions.

Step 4 If the condition does not clear, log into the Cisco 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.

2.7.101 FE-EQPT-NSA

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

SDH Logical Object: E3

The Far End Common Equipment Failure condition occurs when a Non-Service-Affecting (NSA) equipment failure is detected on a far-end DS1i-N-14, DS3i-N-12, or E-N card.

Clear the FE-EQPT-NSA Condition

Step 1 To troubleshoot an FE condition, determine which node and card link 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 links directly to the card reporting the FE condition.

Step 3 Clear the main alarm. Refer to the appropriate alarm section in this chapter for troubleshooting instructions.

Step 4 If the condition does not clear, log into the Cisco 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.

2.7.102 FE-FRCDWKSWBK-SPAN

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

SDH Logical Object: STMN

The Far End Forced Switch Back to Working–Span condition is raised on a far-end 1+1 working port when it is Force switched to the working port.

Note WKSWBK-type conditions apply only to revertive circuits.

Clear the FE-FRCDWKSWBK-SPAN Condition

Step 1 Complete the "Clear a 1+1 Protection Port Force or Manual Switch Command" procedure on page 2-232 for the far-end port.

Step 2 If the condition 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.

2.7.103 FE-FRCDWKSWPR-RING

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

SDH Logical Object: STMN

The Far End Ring Working Facility Forced to Switch to Protection condition occurs from a far-end node when a MS-SPRing is forced from working to protect using the Force Ring command. This condition is only visible on the network view Conditions tab.

Clear the FE-FRCDWKSWPR-RING Condition

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-AIS condition from the STM-16 card in Slot 12 of Node 1 could link to the main AIS condition from an STM-16 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 Clear the main alarm.

Step 4 If the FE-FRCDWKSWPR-RING condition does not clear, complete the "Clear an MS-SPRing External Switching Command" procedure on page 2-238.

Step 5 If the condition does not clear, log into the Cisco 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.

2.7.104 FE-FRCDWKSWPR-SPAN

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

SDH 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 MS-SPRing 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

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-AIS condition from the STM-16 card in Slot 12 of Node 1 could link to the main AIS condition from an STM-16 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 Clear the main alarm.

Step 4 If the FE-FRCDWKSWPR-SPAN condition does not clear, complete the "Clear an MS-SPRing External Switching Command" procedure on page 2-238.

Step 5 If the condition does not clear, log into the Cisco 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.

2.7.105 FE-IDLE

The FE-IDLE condition is not used in this platform in this release. It is reserved for future development.

2.7.106 FE-LOCKOUTOFPR-SPAN

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

SDH Logical Object: STMN

The Far-End Lock Out of Protection Span condition occurs when an MS-SPRing span is locked out of the protection system from a far-end node using the Lockout Protect Span command. This condition is only seen on the network view Conditions tab and is accompanied by LKOUTPR-S. The port where the lockout originated is marked by an "L" on the network view detailed circuit map.

Clear the FE-LOCKOUTOFPR-SPAN Condition

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-AIS condition from the STM-16 card in Slot 12 of Node 1 could link to the main AIS condition from an STM-16 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 Ensure there is no lockout set. Complete the "Clear an MS-SPRing External Switching Command" procedure on page 2-238.

Step 4 If the condition does not clear, log into the Cisco 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.

2.7.107 FE-LOF

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

SDH Logical Object: E3

The Far End LOF condition occurs when a far-end node reports a DS-1 LOF on a DS1i-N-14 card, a DS-3 LOF on a DS3i-N-12 card, or an LOF on an E-N card.

Clear the FE-LOF Condition

Step 1 To troubleshoot an FE condition, determine which node and card link 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 links directly to the card reporting the FE condition.

Step 3 Complete the "2.7.172 LOF (TRUNK)" procedure on page 2-139. The procedure also applies to FE-LOF.

Step 4 If the condition does not clear, log into the Cisco 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.

2.7.108 FE-LOS

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

SDH Logical Object: E3

The Far End LOS condition occurs when a far-end node reports a DS-1 LOF on a DS1i-N-14 card, a DS-3 LOS on a DS3i-N-12 card, or an E-N LOS.

Clear the FE-LOS Condition

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 the LOS (STM1E, STMN) Alarm" procedure on page 2-148.

Step 4 If the condition does not clear, log into the Cisco 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.

2.7.109 FE-MANWKSWBK-SPAN

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

SDH Logical Object: STMN

The Far End Manual Switch Back to Working—Span 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

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 an MS-SPRing External Switching Command" procedure on page 2-238.

Step 4 If the condition 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.

2.7.110 FE-MANWKSWPR-RING

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

SDH Logical Object: STMN

The Far End Ring Manual Switch of Working Facility to Protect condition occurs when an MS-SPRing working ring is switched from working to protect at a far-end node using the Manual Ring command.

Clear the FE-MANWKSWPR-RING Condition

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 an MS-SPRing External Switching Command" procedure on page 2-238.

Step 4 If the condition does not clear, log into the Cisco 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.

2.7.111 FE-MANWKSWPR-SPAN

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

SDH Logical Object: STMN

The Far-End Span Manual Switch Working Facility to Protect condition occurs when a four-fiber MS-SPRing 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

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 an MS-SPRing External Switching Command" alarm on page 2-238.

Step 4 If the condition does not clear, log into the Cisco 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.

2.7.112 FEPRLF

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

SDH Logical Object: STMN

The Far-End Protection Line Failure alarm occurs when there was an APS channel 2.7.308 SF (DS1, DS3, E1, E3, E4, STMN) condition on the protect card coming into the node.

Note The FEPRLF alarm occurs on the ONS 15454 SDH only when bidirectional protection is used on optical (traffic) cards in a 1+1 protection group configuration.

Clear the FEPRLF Alarm on an MS-SPRing

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.

Step 4 If the alarm does not clear, log into the Cisco 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.

2.7.113 FIBERTEMP-DEG

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.114 FORCED-REQ

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

SDH Logical Objects: EQPT, VCMON-HP, VCMON-LP

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.

Clear the FORCED-REQ Condition

Step 1 Complete the "Clear a 1+1 Protection Port Force or Manual Switch Command" procedure on page 2-232.

Step 2 If the condition does not clear, log into the Cisco 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.

2.7.115 FORCED-REQ-RING

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

SDH Logical Object: STMN

The Force Switch Request Ring condition applies to optical trunk cards when the Force Ring command is applied to MS-SPRings to move traffic from working to protect. This condition is visible on the network view Alarms, Conditions, and History tabs and is accompanied by WKSWPR. The port where the FORCE RING command originated is marked with an "F" on the network view detailed circuit map.

Clear the FORCED-REQ-RING Condition

Step 1 Complete the "Clear an MS-SPRing External Switching Command" procedure on page 2-238.

Step 2 If the condition does not clear, log into the Cisco 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.

2.7.116 FORCED-REQ-SPAN

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

SDH Logical Object: STMN

DWDM Logical Objects: 2R, ESCON, FC, GE, ISC, TRUNK

The Force Switch Request Span condition applies to optical trunk cards in two-fiber or four-fiber MS-SPRings when the Force Span command is applied to a MS-SPRing SPAN to force traffic from working to protect or from protect to working. This condition appears on the network view Alarms, Conditions, and History tabs. The port where the FORCE SPAN command was applied is marked with an "F" on the network view detailed circuit map.

This condition can also be raised in 1+1 facility 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 both the facility and the span.

Clear the FORCED-REQ-SPAN Condition

Step 1 Complete the "Clear an MS-SPRing External Switching Command" procedure on page 2-238.

Step 2 If the condition does not clear, log into the Cisco 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.

2.7.117 FRCDSWTOINT

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

SDH 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. The condition does not require troubleshooting.

2.7.118 FRCDSWTOPRI

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

SDH 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. The condition does not require troubleshooting.

2.7.119 FRCDSWTOSEC

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

SDH 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. The condition does not require troubleshooting.

2.7.120 FRCDSWTOTHIRD

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

SDH 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. The condition does not require troubleshooting.

2.7.121 FRNGSYNC

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

SDH Logical Object: NE-SREF

The Free Running Synchronization Mode condition occurs when the reporting ONS 15454 SDH is in free-run synchronization mode. External timing sources have been disabled and the node is using its internal clock, or the ONS 15454 SDH has lost its designated BITS timing source. After the 24-hour holdover period expires, timing slips could begin to occur on an ONS 15454 SDH relying on an internal clock.

Note If the ONS 15454 SDH is configured to operate from its internal clock, disregard the FRNGSYNC condition.

Clear the FRNGSYNC Condition

Step 1 If the ONS 15454 SDH is configured to operate from an external timing source, verify that the BITS timing source is valid. Common problems with a BITS timing source include reversed wiring and bad timing cards. Refer to the "Timing" chapter in the *Cisco ONS 15454 SDH Reference Manual* for more information about it.

Step 2 If the BITS source is valid, clear alarms related to the failures of the primary and secondary reference sources, such as the "SYNCPRI" alarm on page 2-213 and the "SYSBOOT" alarm on page 2-215.

Step 3 If the condition does not clear, log into the Cisco 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.

2.7.122 FSTSYNC

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

SDH Logical Object: NE-SREF

A Fast Start Synchronization Mode condition occurs when the ONS 15454 SDH is choosing a new timing reference. The previous timing reference has failed.

The FSTSYNC condition disappears after approximately 30 seconds. If the condition does not clear, log into the Cisco 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.

Note FSTSYNC is an informational condition. The condition does not require troubleshooting.

2.7.123 FULLPASSTHR-BI

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

SDH Logical Object: STMN

The Bidirectional Full Pass-Through Active condition occurs on a nonswitching node for an MS-SPRing when the protect channels on the node are active and carrying traffic and there is a change in the receive K byte from No Request.

Clear the FULLPASSTHR-BI Condition

Step 1 Complete the "Clear an MS-SPRing External Switching Command" procedure on page 2-238.

Step 2 If the condition does not clear, log into the Cisco 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.

2.7.124 GAIN-HDEG

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.125 GAIN-HFAIL

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.126 GAIN-LDEG

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.127 GAIN-LFAIL

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.128 GCC-EOC

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.129 GE-OOSYNC

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.130 GFP-CSF

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

SDH Logical Objects: CE100T, FCMR, GFP-FAC, ML100T, ML1000, MLFX

The GFP Client Signal Fail Detected 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 FC_MR-4, ML-Series Ethernet, MXP_MR_2.5G, MXPP_MR_2.5G GFP data ports and does not indicate that a Service-Affecting (SA) failure is occurring at the local site, but that a CARLOSS, LOS, or SYNCLOSS alarm caused by an event such as a pulled receive cable is affecting a remote data ports's transmission capability. This alarm can be demoted when a facility loopback is placed on the FC_MR-4 port.

Note For more information about Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.*

Clear the GFP-CSF Alarm

Step 1 Clear the Service-Affecting (SA) alarm at the remote data port.

Step 2 If the GFP-CSF 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.

2.7.131 GFP-DE-MISMATCH

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

SDH Logical Objects: FCMR, GFP-FAC

The GFP Fibre Channel Distance Extension (DE) Mismatch alarm indicates that a port configured for distance extension is connected to a port not operating in Cisco's proprietary Distance Extension mode. It is raised on Fibre Channel and FICON card GFP ports supporting distance extension. The alarm occurs when distance extension is enabled on one side of the transport but not on the other. To clear, distance extension must be enabled on both ports connected by a circuit.

Note For more information about Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.*

Clear the GFP-DE-MISMATCH Alarm

Step 1 Ensure that the distance extension protocol is configured correctly on both sides by completing the following steps:

a. Double-click the card to display the card view.

b. Click the **Provisioning > Port > General** tabs.

c. Under Admin State, click the cell and choose **Locked, maintenance**.

d. Click **Apply**.

e. Click the **Provisioning > Port > Distance Extension** tabs.

f. Check the check box in the **Enable Distance Extension** column.

g. Click **Apply**.

h. Click the **Provisioning > Port > General** tabs.

i. Under Admin State, click the cell and choose **Unlocked**.

j. Click **Apply**.

Step 2 If the GFP-DE-MISMATCH 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.

2.7.132 GFP-EX-MISMATCH

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

SDH Logical Objects: FCMR, GFP-FAC

The GFP Extension Header Mismatch alarm is raised on Fibre Channel/FICON cards when it receives frames with an extension header that is not null. The alarm occurs when a provisioning error causes all GFP frames to be dropped for 2.5 seconds.

The user needs to ensure both end ports are sending null extension headers for a GFP frame. An FC_MR-4 card always sends a null extension header, so if the equipment is connected to other vendors' equipment, those need to be provisioned appropriately.

Note For more information about Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.

Clear the GFP-EX-MISMATCH Alarm

Step 1 Ensure that the vendor equipment is provisioned to send a null extension header in order to interoperate with the FC_MR-4 card. (The FC_MR-4 card always sends a null extension header.)

Step 2 If the GFP-EX-MISMATCH 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.

2.7.133 GFP-LFD

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

SDH Logical Objects: CE100T, FCMR, GFP-FAC, ML100T, ML1000, MLFX

The GFP Loss of Frame Delineation alarm applies to Fibre Channel, FICON GFP, and Ethernet ports. This alarm occurs if there is a bad SDH connection, if SDH 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. The loss is service-affecting.

Note For more information about Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.

Clear the GFP-LFD Alarm

Step 1 Look for and clear any associated SDH path errors such as LOS originating at the transmit node.

Step 2 If the GFP-LFD 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.

2.7.134 GFP-NO-BUFFERS

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

SDH Logical Objects: FCMR, GFP-FAC

The GFP Fibre Channel Distance Extension Buffer Starvation alarm is raised on Fibre Channel/FICON card ports supporting GFP and the distance extension protocol when the GFP transmitter cannot send GFP frames due to lack of remote GFP receiver buffers. This occurs when the remote GFP-T receiver experiences congestion and is unable to send frames over the Fibre Channel/FICON link.

This alarm could be raised in conjunction with the FC-NO-CREDITS alarm. For example, if the FC-NO-CREDITS alarm is generated at an FC_MR-4 data port, a GFP-NO-BUFFERS alarm could be raised at the upstream remote FC_MR-4 data port.

Note For more information about Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.

Clear the GFP-NO-BUFFERS Alarm

Step 1 Complete the "Clear the FC-NO-CREDITS Alarm" procedure on page 2-94.

Step 2 If the GFP-CSF 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.

2.7.135 GFP-UP-MISMATCH

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

SDH Logical Objects: CE100T, FCMR, GFP-FAC, ML100T, ML1000, 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.

Note For more information about Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.

Clear the GFP-UP-MISMATCH Alarm

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 display 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 display 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**.

Step 3 If the GFP-UP-MISMATCH 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.

2.7.136 HELLO

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

SDH Logical Object: STMN

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

Step 1 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**.

Step 2 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.

2.7.137 HI-LASERBIAS

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

SDH Logical Objects: EQPT, STMN

DWDM Logical Objects: 2R, ESCON, FC, GE, ISC, PPM, TRUNK

The Equipment High Transmit Laser Bias Current alarm is raised against TXP, MXP, MRC-12, and OC192-XFP/STM64-XFP card laser performance. The alarm indicates that the card laser has reached the maximum laser bias tolerance.

The laser bias ratio typically starts at about 30 percent of the manufacturer's 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 can no longer be used. If the threshold is set at 90 percent of the maximum, the card is still usable for several weeks or months before it needs to be replaced.

Note For more information about provisioning MXP or TXP PPMs, refer to the "Provision Transponder and Muxponder Cards" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For more information about the cards themselves, refer to the "Card Reference" chapter.

Clear the HI-LASERBIAS Alarm

Step 1 Complete the "Physically Replace a Traffic Card" procedure on page 2-242 during a maintenance window. (Replacement is not urgent.)

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. See the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-230 for commonly used traffic-switching procedures.

Note When you replace a card with the identical type of card, you do not need to make any changes to the database.

Step 2 If the alarm does not clear, log into the Cisco 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.

2.7.138 HI-LASERTEMP

Default Severity: Minor (MN), Non-Service-Affecting (NSA) for 2R, EQPT, FC, GE, ISC, STMN; Not Alarmed (NA), Non-Service-Affecting (NSA) for PPM

SDH Logical Objects: EQPT, STMN

SDH Logical Object: PPM

The Equipment High Laser Optical Transceiver Temperature alarm applies to TXP, MXP, MRC-12, and OC192-XFP/STM64-XFP 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 card raises this alarm, the laser is automatically shut off. The "LOS (STM1E, STMN)" alarm on page 2-147 is raised at the far-end node and the "DSP-FAIL" alarm on page 2-74 is raised at the near end.

Note For more information about provisioning MXP or TXP PPMs, refer to the "Provision Transponder and Muxponder Cards" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For more information about the cards themselves, refer to the "Card Reference" chapter.

Clear the HI-LASERTEMP Alarm

Step 1 In node view, double-click the card to display 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 Traffic Card in CTC" procedure on page 2-238 for the reporting card.

Step 5 If the alarm does not clear, complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the reporting card.

Step 6 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or 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.

2.7.139 HI-RXPOWER

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

SDH Logical Object: STMN

DWDM Logical Objects: 2R, ESCON, FC, GE, ISC, TRUNK

The Equipment High Receive Power alarm is an indicator of the optical signal power that is transmitted to the TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, or MXP_2.5G_10G card. HI-RXPOWER occurs when the measured optical power of the received signal exceeds the threshold. The threshold value is user-provisionable.

Note For more information about MXP or TXP cards, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Note When you upgrade a node to Software Release 6.0 or later, this enables received optical power PMs for the STM1-8, STM64-SR, STM64-IR, STM64-ITU, STM64-XFP, MRC-12, and MRC25G-4 cards. The newly enabled HI-RXPOWER and LO-RXPOWER alarms require that you initialize a site-accepted optical power (OPR0) nominal value after the upgrade. (To do this, refer to the procedure in the "Turn Up a Node" chapter in the *Cisco ONS 15454 SDH Procedure Guide*.) When you apply the value change, CTC uses the new OPR0 value to calculate PM percentage values. If you do not change the nominal value, the HI-RXPOWER or LO-RXPOWER may be raised in response to the unmodified setting.

Clear the HI-RXPOWER Alarm

Step 1 Find out whether the gain (the amplification power) of any amplifiers has been changed. The change also causes channel power to need adjustment.

Step 2 Find out whether channels have been dropped from the fiber. Increasing or decreasing channels can affect power. If channels have been dropped, the power levels of all channels have to be adjusted.

Note If the card is part of an amplified DWDM system, dropping channels on the fiber affects the transmission power of each channel more than it would in an unamplified system.

Step 3 At the transmit end of the errored circuit, decrease the transmit power level within safe limits.

Step 4 If neither of these problems caused the HI-RXPOWER alarm, there is a slight possibility that another wavelength is drifting on top of the alarmed signal. In this case, the receiver gets signals from two transmitters at once and data alarms would be present. If wavelengths are drifting, the data is garbled and receive power increases by about +3 dBm.

Step 5 If the alarm does not clear, add fiber attenuators to the receive ports. Start with low-resistance attenuators and use stronger ones as needed, depending on factors such as the transmission distance according to standard practice.

Step 6 If the alarm does not clear, and no faults are present on the other ports of the transmit or receive card, use a known-good loopback cable to complete the "1.5.1 Perform a Facility (Line) Loopback on a Source-Node MXP/TXP/FC_MR-4 Port" procedure on page 1-79 and test the loopback.

Step 7 If a port is bad and you need to use all the port bandwidth, complete the "Physically Replace a Traffic Card" procedure on page 2-242. If the port is bad but you can move the traffic to another port, replace the card at the next available maintenance window.

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. See the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-230 for commonly used traffic-switching procedures.

Note When you replace a card with the identical type of card, you do not need to make any changes to the database.

Step 8 If the alarm does not clear, log into the Cisco 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.

2.7.140 HITEMP

Default Severity: Critical (CR), Service-Affecting (SA) for NE; Minor (MN), Non-Service-Affecting (NSA) for EQPT

SDH Logical Objects: EQPT, NE

The High Temperature alarm occurs when the temperature of the ONS 15454 SDH is above 50 degrees C (122 degrees F).

Clear the HITEMP Alarm

Step 1 View the temperature displayed on the ONS 15454 SDH LCD front panel. For an illustration of the LCD panel, see Figure 2-1.

Step 2 Verify that the environmental temperature of the room is not abnormally high.

Step 3 If the room temperature is not abnormal, physically ensure that nothing prevents the fan-tray assembly from passing air through the ONS 15454 SDH.

Step 4 If airflow is not blocked, physically ensure that blank faceplates fill the ONS 15454 SDH empty slots. Blank faceplates help airflow.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454 SDH. Plug the wristband cable into the ESD jack located on the middle-right outside edge of the shelf assembly.

Step 5 If faceplates fill the empty slots, determine whether the air filter needs replacement. Complete the "Inspect, Clean, and Replace the Reusable Air Filter" procedure on page 2-245.

Step 6 If the filter is clean, complete the "Remove and Reinsert a Fan-Tray Assembly" procedure on page 2-246.

Note The fan-tray assembly should run immediately when correctly inserted.

Step 7 If the fan does not run or the alarm persists, complete the "Replace the Fan-Tray Assembly" procedure on page 2-247.

Step 8 If the replacement fan-tray assembly does not operate correctly, log into the Cisco Technical Support Website at http://www.cisco.com/techsupport for more information. If the alarm does not clear, 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.

2.7.141 HI-TXPOWER

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

SDH Logical Objects: EQPT, STMN

DWDM Logical Objects: 2R, ESCON, FC, GE, ISC, PPM, TRUNK

The Equipment High Transmit Power alarm is an indicator on TXP, MXP, MRC-12, and OC192-XFP/STM64-XFP card transmitted optical signal power. HI-TXPOWER occurs when the measured optical power of the transmitted signal exceeds the threshold.

Note For more information about provisioning MXP or TXP PPMs, refer to the "Provision Transponder and Muxponder Cards" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For more information about the cards themselves, refer to the "Card Reference" chapter.

Clear the HI-TXPOWER Alarm

Step 1 In node view, display the card view for the reporting card.

Step 2 Click the **Provisioning > Optics Thresholds** tabs **Provisioning > Optics Thresholds > Current Values** tabs as appropriate.

Step 3 Decrease (change toward the negative direction) the OPT-HIGH column value by 0.5 dBm.

Step 4 If the card transmit power setting cannot be lowered without disrupting the signal, complete the "Physically Replace a Traffic Card" procedure on page 2-242.

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. See the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-230 for commonly used traffic-switching procedures.

Note When you replace a card with the identical type of card, you do not need to make any changes to the database.

Step 5 If the alarm does not clear, log into the Cisco 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.

2.7.142 HLDOVRSYNC

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

SDH 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 15454 SDH relying on an internal clock.

Clear the HLDOVRSYNC Alarm

Step 1 Clear additional events that relate to timing, such as:

- 2.7.121 FRNGSYNC, page 2-107
- 2.7.122 FSTSYNC, page 2-108
- 2.7.142 HLDOVRSYNC, page 2-119
- 2.7.171 LOF (DS1, DS3, E1, E4, STM1E, STMN), page 2-138
- 2.7.186 LOS (STM1E, STMN), page 2-147
- 2.7.226 MANSWTOINT, page 2-166
- 2.7.227 MANSWTOPRI, page 2-166
- 2.7.228 MANSWTOSEC, page 2-166
- 2.7.229 MANSWTOTHIRD, page 2-167
- 2.7.351 SYSBOOT, page 2-215
- 2.7.344 SWTOSEC, page 2-211
- 2.7.345 SWTOTHIRD, page 2-212
- 2.7.346 SYNC-FREQ, page 2-212
- 2.7.348 SYNCPRI, page 2-213

- 2.7.351 SYSBOOT, page 2-215

Step 2 Reestablish primary and secondary timing sources according to local site practice. If none exists, refer to the "Change Node Settings" chapter in the *Cisco ONS 15454 SDH Procedure Guide* for procedures.

Step 3 If the alarm does not clear, log into the Cisco 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.

2.7.143 HP-ENCAP-MISMATCH

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

SDH 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**.

Note For more information about the ML-Series Ethernet card, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.*

Clear the HP-ENCAP-MISMATCH Alarm

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**. Refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327* entries on all three of these topics to obtain the full configuration command sequences.

Step 4 If the alarm does not clear, log into the Cisco 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.

2.7.144 HP-RFI

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

SDH 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

Step 1 Log into the node at the far end of the reporting ONS 15454 SDH.

Step 2 Determine whether there are any related alarms, especially the "LOS (STM1E, STMN)" alarm on page 2-147.

Step 3 Clear the main alarm. See the appropriate alarm section in this chapter for procedures.

Step 4 If the condition does not clear, log into the Cisco 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.

2.7.145 HP-TIM

Default Severities: Critical (CR), Service-Affecting (SA) for VCTRM-HP; Minor (MN), Non-Service-Affecting (NSA) for VCMON-HP

SDH 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 SDH path overhead. The error can originate at the transmit end or the receive end.

Clear the HP-TIM Alarm

Step 1 Use an optical test set capable of viewing SDH 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" procedure on page 2-213.

Step 3 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. If the alarm applies to VCTRM-HP, it is a service-affecting problem.

2.7.146 HP-UNEQ

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

SDH Logical ObjectS: 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 SDH path overhead.

Clear the HP-UNEQ Alarm

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.

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" procedure on page 2-243.

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 a through b.

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" procedure on page 2-243.

Step 10 Recreate the circuit with the correct circuit size. Refer to the "Create Circuits and Tunnels" chapter in the *Cisco ONS 15454 SDH Procedure 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 *Cisco ONS 15454 SDH Procedure Guide*.

Warning **On the OC192 LR/STM64 LH 1550 card, the laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. The laser is off when the safety key is off (labeled 0).** Statement 293

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

Warning **Use of controls, adjustments, or performing procedures other than those specified could result in hazardous radiation exposure.** Statement 1057

Step 13 If the alarm does not clear, complete the "Physically Replace a Traffic Card" procedure on page 2-242 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. Refer to the "Maintain the Node" chapter in the *Cisco ONS 15454 SDH Procedure Guide* for information.

Note When you replace a card with the identical type of card, you do not need to make any changes to the database.

Step 14 If the alarm does not clear, log into the Cisco 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.

2.7.147 I-HITEMP

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

SDH Logical Object: NE

The Industrial High Temperature alarm occurs when the temperature of the ONS 15454 SDH is above 149 degrees F (65 degrees C) or below –40 degrees F (–40 degrees C). This alarm is similar to the HITEMP alarm but is used for the industrial environment. If this alarm is used, you can customize your alarm profile to ignore the lower-temperature HITEMP alarm.

Clear the I-HITEMP Alarm

Step 1 Complete the "Clear the HITEMP Alarm" procedure on page 2-117.

Step 2 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 to report a Service-Affecting (SA) problem.

2.7.148 IMPROPRMVL

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

SDH Logical Object: EQPT

DWDM Logical Object: PPM

The Improper Removal alarm for equipment occurs when a card is physically removed from its slot before being deleted from CTC. The card does not need to be in service to cause the IMPROPRMVL alarm; CTC only has to recognize that the card is not present. The alarm does not appear if you delete the card from CTC before you physically remove the card from the node. For PPM, the alarm occurs if you provision a PPM but no physical module is inserted on the port.

Caution Do not remove a card during a card reboot. If CTC begins to reboot a card before you remove it, allow the card to finish rebooting. After the card reboots, delete the card in CTC again and physically remove the card before it begins to reboot.

Note CTC gives the user approximately 15 seconds to physically remove the card before CTC begins a card reboot.

Note It can take up to 30 minutes for software to be updated on a standby TCC2/TCC2P card.

Note When a MIC-A/P card is removed from the shelf, no IMPROPRMVL alarm is reported for that card. The FMEC to the left side of the MIC-A/P also could also disappear from view in CTC. This functions as designed. The MIC-A/P card provides a communication channel to the other FMEC. When the MIC card is removed, the communication channel is no longer available and consequently, the other FMEC is assumed not to be present. The disappeared FMEC is rediscovered when the MIC-A/P is reinserted.

Clear the IMPROPRMVL Alarm

Step 1 In node view, right-click the card reporting the IMPROPRMVL.

Step 2 Choose **Delete** from the shortcut menu.

Note CTC does not allow you to delete the reporting card if the card is in service, does have circuits mapped to it, is paired in a working protection scheme, has DCC enabled, or is used as a timing reference.

Step 3 If any ports on the card are in service, lock them (Locked, maintenance) by completing the following steps:

Caution Before locking a port (locked,maintenance or locked,disabled), ensure that no live traffic is present.

a. In node view, double-click the reporting card to display the card view.

b. Click the **Provisioning > Line** tab or the **Provisioning > Line > SDH** tab as appropriate to the reporting card.

c. Click the **Admin State** column of any Unlocked ports.

d. Choose **Locked, maintenance** to take the ports out of service.

Step 4 If a circuit has been mapped to the card, complete the "Delete a Circuit" procedure on page 2-243.

Caution Before deleting the circuit, ensure that the circuit does not carry live traffic.

Step 5 If the card is paired in a protection scheme, delete the protection group by completing the following steps:

a. Click **View > Go to Previous View** to return to node view.

b. If you are already in node view, click the **Provisioning > Protection** tabs.

c. Click the protection group of the reporting card.

d. Click **Delete**.

Step 6 If the card is provisioned for DCC, delete the DCC provisioning by completing the following steps:

a. Click the ONS 15454 SDH **Provisioning > Comm Channels > RS-DCC** tabs.

b. Click the slots and ports listed in DCC terminations.

c. Click **Delete** and click **Yes** in the dialog box that appears to delete all of the selected terminations.

Step 7 If the card is used as a timing reference, change the timing reference by completing the following steps:

a. Click the **Provisioning > Timing > General** tabs.

b. Under NE Reference, click the drop-down list for Ref-1.

c. Change Ref-1 from the listed STM-N card to **Internal Clock**.

d. Click **Apply**.

Step 8 If the alarm does not clear, log into the Cisco 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.

2.7.149 INC-ISD

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

SDH Logical Objects: DS3, E3

The DS-3 Idle condition indicates that the DS3i-N-12 card is receiving an idle signal, meaning that the payload of the signal contains a repeating pattern of bits. The INC-ISD condition occurs when the transmitting port has a Locked, maintenance Admin State. It is resolved when the Locked, maintenance state ends.

Note INC-ISD is an informational condition. The condition does not require troubleshooting.

2.7.150 INHSWPR

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

SDH 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

Step 1 If the condition is raised against a 1+1 port, complete the "Initiate a 1+1 Protection Port Manual Switch Command" procedure on page 2-231.

Step 2 If it is raised against a 1:1 card, complete the "Initiate a 1:1 Card Switch Command" procedure on page 2-233 to switch it back.

Step 3 If the condition does not clear, log into the Cisco 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.

2.7.151 INHSWWKG

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

SDH 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.

Note For more information about Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.

Clear the INHSWWKG Condition

Step 1 If the condition is raised against a 1+1 port, complete the "Initiate a 1+1 Protection Port Manual Switch Command" procedure on page 2-231.

Step 2 If it is raised against a 1:1 card, complete the "Initiate a 1:1 Card Switch Command" procedure on page 2-233 to switch it back.

Step 3 If the condition does not clear, log into the Cisco 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.

2.7.152 INTRUSION-PSWD

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

SDH 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 lockout is permanent.

Clear the INTRUSION-PSWD Condition

Step 1 Click the **Provisioning > Security > Users** tabs.

Step 2 Click **Clear Security Intrusion Alarm**.

Step 3 If the condition does not clear, log into the Cisco 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.

2.7.153 INVMACADR

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

SDH Logical Object: BPLANE

The Equipment Failure Invalid MAC Layer address alarm occurs when the ONS 15454 SDH MAC address is invalid. The MAC address is permanently assigned to the ONS 15454 SDH chassis during manufacture. Do not attempt to troubleshoot an INVMACADR alarm. Log into the Cisco 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.

2.7.154 IOSCFGCOPY

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

SDH Logical Object: EQPT

The Cisco IOS Configuration Copy in Progress condition occurs on ML-Series Ethernet cards when a Cisco IOS startup configuration file is being uploaded to or downloaded from an ML-Series card. (This condition is very similar to the 2.7.313 SFTWDOWN condition but it applies to ML-Series Ethernet cards rather than to the TCC2/TCC2P card.)

The condition clears after the copy operation is complete. (If it does not complete correctly, the 2.7.245 NO-CONFIG condition could be raised.)

Note IOSCFGCOPY is an informational condition.

Note For more information about Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.*

2.7.155 ISIS-ADJ-FAIL

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

SDH Logical Object: STMN

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. For more information about IS-IS OSI routing and MAA configuration, refer to the "Management Network Connectivity" chapter in the *Cisco ONS 15454 SDH Reference Manual*. For more information about configuring OSI, refer to the "Turn Up Node" chapter in the *Cisco ONS 15454 SDH Procedure Guide* for procedures.

Clear the ISIS-ADJ-FAIL Alarm

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 *Cisco ONS 15454 SDH Procedure Guide* for the procedure.

Step 3 If the nodes use PPP Layer 2, complete the "Clear the EOC Alarm" procedure on page 2-77. If the alarm does not clear, go to Step 7.

Step 4 If both nodes use the LAPD Layer 2 protocol but have different Mode settings, change the incorrect node's 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 *Cisco ONS 15454 SDH Procedure Guide* for procedures to do this.

Step 9 If the condition does not clear, log into the Cisco 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.

2.7.156 KB-PASSTHR

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

SDH Logical Object: STMN

The K Bytes Pass Through Active condition occurs on a nonswitching node in an MS-SPRing when the protect channels on the node are not active and the node is in K Byte pass-through state.

Clear the KB-PASSTHR Condition

Step 1 Complete the "Clear an MS-SPRing External Switching Command" procedure on page 2-238.

Step 2 If the condition does not clear, log into the Cisco 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.

2.7.157 KBYTE-APS-CHANNEL-FAILURE

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

SDH Logical Object: STMN

The APS Channel Failure alarm is raised when a span is provisioned for different APS channels on each side. For example, the alarm is raised if K3 is selected on one end and F1, E2, or Z2 is selected on the other end.

This alarm is also raised during checksum. Failure occurs if the K1 and K2 bytes are overwritten by test equipment. It is not raised in bidirectional full pass-through or K byte pass-through states. The alarm is overridden by MS-AIS, "LOF (DS1, DS3, E1, E4, STM1E, STMN)" alarm on page 2-138, "LOS (STM1E, STMN)" alarm on page 2-147, or SFBER-EXCEED-HO alarms.

Clear the KBYTE-APS-CHANNEL-FAILURE Alarm

Step 1 The alarm is most frequently raised due to mismatched span provisioning. In this case, reprovision one side of the span to match the parameters of the other side. To do this, refer to the "Turn Up Network" chapter in the *Cisco ONS 15454 SDH Procedure Guide* for procedures.

Step 2 If the error is not caused by misprovisioning, it is due to checksum errors within an STM-N, cross-connect, or TCC2/TCC2P card. In this case, complete the "Side Switch the Active and Standby Cross-Connect Cards" procedure on page 2-240 to allow CTC to resolve the issue.

Step 3 If third-party equipment is involved, ensure that it is configured for the same APS channel as the Cisco ONS equipment.

Step 4 If the condition does not clear, log into the Cisco 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.

2.7.158 LAN-POL-REV

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

SDH Logical Object: NE

The LAN Connection Polarity Reversed condition is not raised in shelves that contain TCC2 cards. It is raised during software upgrade when the card detects that a connected Ethernet cable has reversed receive wire pairs. The card automatically compensates for this reversal, but LAN-POL-REV stays active.

Note For more information about Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.*

Clear the LAN-POL-REV Condition

Step 1 Replace the connected Ethernet cable with a cable that has the correct pinout. For correct pin mapping, refer to the "Maintain the Node" chapter in the *Cisco ONS 15454 SDH Procedure Guide*.

Step 2 If the condition does not clear, log into the Cisco 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.

2.7.159 LASER-APR

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.160 LASERBIAS-DEG

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.161 LASERBIAS-FAIL

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.162 LASERTEMP-DEG

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.163 LCAS-CRC

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

SDH Logical Objects: VCTRM-HP, VCTRM-LP

The Link Capacity Adjustment Scheme (LCAS) Control Word CRC Failure condition is raised against ML-Series Ethernet cards and CE-series cards. It occurs when there is an equipment, path, or provisioning error on the virtual concatenation group (VCG) that causes consecutive 2.5 second CRC failures in the LCAS control word.

The condition can occur if an LCAS-enabled node (containing ML-Series cards) transmitting to another LCAS-enabled node delivers faulty traffic due to an equipment or SDH path failure. Transmission errors would also be reflected in CV-P, ES-P, or SES-P performance monitoring statistics. If these errors do not exist, an equipment failure is indicated.

If LCAS is not supported on the peer node, the condition does not clear.

LCAS-CRC can also occur if the VCG source node is not LCAS-enabled, but the receiving node does have the capability enabled. Both source and destination nodes must have LCAS enabled. Otherwise, the LCAS-CRC condition persists on the VCG.

Note For more information about Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.

Clear the LCAS-CRC Condition

Step 1 Look for and clear any associated equipment failures, such as the EQPT alarm, on the receive node or transmit node.

Step 2 Look for and clear any bit error rate alarms at the transmit node.

Step 3 If no equipment or SDH path errors exist, ensure that the remote node has LCAS enabled on the circuit:

Step 4 In node view, click the **Circuits** tab.

Step 5 Choose the VCAT circuit and click **Edit**.

Step 6 In the Edit Circuit window, click the **General** tab.

Step 7 Verify that the Mode column says LCAS.

Step 8 If the column does not say LCAS, complete the "Delete a Circuit" procedure on page 2-243 and recreate it in LCAS mode using the instructions in the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.

Step 9 If the condition 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.

2.7.164 LCAS-RX-FAIL

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

SDH Logical Objects: VCTRM-HP, VCTRM-LP

The LCAS VCG Member Receive-Side-In Fail condition is raised against CE-series cards, FC_MR-4 cards, and ML-Series Ethernet cards with LCAS-enabled VCG.

LCAS VCGs treat failures unidirectionally, meaning that failures of the transmit or receive points occur independently of each other. The LCAS-RX-FAIL condition can occur on the receive side of an LCAS VCG member for the following reasons:

- SDH path failure (a unidirectional failure as seen by the receive side).
- VCAT member is set out of group at the transmit side, but is set in group at the receive side.
- VCAT member does not exist at the transmit side but does exist and is in group at the receive side.

The condition can be raised during provisioning operations on LCAS VCGs but should clear when the provisioning is completed.

Software-enabled LCAS VCGs treat failure bidirectionally, meaning that both directions of a VCG member are considered failed if either transmit or receive fails. The LCAS-RX-FAIL condition is raised on these VCG members when a member receive side fails due to a SDH path failure.

Note For more information about Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.*

Note ML-Series cards are LCAS-enabled. ML-Series and FC-MR-4 cards are SW-LCAS enabled.

Clear the LCAS-RX-FAIL Condition

Step 1 Check for and clear any line or path alarms.

Step 2 If the condition 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.

2.7.165 LCAS-TX-ADD

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

SDH Logical Objects: VCTRM-HP, VCTRM-LP

The LCAS VCG Member Transmit-Side-In Add State condition is raised against ML-Series Ethernet cards and CE-series cards when the transmit side of an LCAS VCG member is in the add state. The condition clears after provisioning is completed. The condition clears after provisioning is completed.

Note LCAS-TX-ADD is an informational condition and does not require troubleshooting.

Note For more information about Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.*

2.7.166 LCAS-TX-DNU

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

SDH Logical Objects: VCTRM-HP, VCTRM-LP

The LCAS VCG Member Transmit Side In Do Not Use condition is raised on FC_MR-4 cards, ML-Series Ethernet cards, and CE-series cards when the transmit side of an LCAS VCG member is in the do-not use state. For a unidirectional failure, this condition is only raised at the source node. The LCAS-TX-DNU condition is raised when the cable is unplugged.

The node reporting this condition likely reports an HP-RFI alarm, and the remote node likely reports a path alarm such as MS-AIS or "HP-UNEQ" alarm on page 2-122.

Note LCAS-TX-DNU is an informational condition and does not require troubleshooting.

Note For more information about Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.

2.7.167 LKOUTPR-S

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

SDH Logical Object: STMN

The Lockout of Protection Span condition occurs when span traffic is locked out of a protect span using the Lockout of Protect command. This condition is visible on the Alarms, Conditions, and History tabs in network view after the lockout has occurred and accompanies the FE-LOCKOUTPR-SPAN condition. The port where the lockout originated is marked by an "L" on the network view detailed circuit map.

Clear the LKOUTPR-S Condition

Step 1 Complete the "Clear an MS-SPRing External Switching Command" procedure on page 2-238.

Step 2 If the condition does not clear, log into the Cisco 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.

2.7.168 LOA

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

SDH Logical Object: VCG

The Loss of Alignment on a VCG is a VCAT member alarm. (VCAT member circuits are independent circuits that are concatenated from different time slots into a higher-rate signal.) The alarm occurs when members of a VCG travel over different paths in the network (due to initial operator provisioning or to protection or restoration events) and the differential delays between the paths cannot be recovered by terminating hardware buffers.

Note This alarm occurs only if you provision circuits outside of CTC, such as by using TL1.

Clear the LOA Alarm

Step 1 In network view, click the **Circuits** tab.

Step 2 Click the alarmed VCG and then click **Edit**.

Step 3 In the Edit Circuit dialog box, view the source and destination circuit slots, ports, and VC4s.

Step 4 Identify whether the circuit travels across different fibers. If it does, complete the "Delete a Circuit" procedure on page 2-243.

Step 5 Recreate the circuit using the procedure in the "Create Circuits and Tunnels" chapter in the *Cisco ONS 15454 SDH Procedure Guide*.

Step 6 If the alarm does not clear, log into the Cisco 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.

2.7.169 LOCKOUT-REQ

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

SDH Logical Objects: EQPT, STMN, VCMON-HP, VCMON-LP

DWDM Logical Objects: 2R, ESCON, FC, GE, ISC, TRUNK

The Lockout Switch Request on Facility or Equipment condition occurs when a user initiates a lockout switch request for an STM-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

Step 1 Complete the "Clear a Card or Port Lock On or Lock Out Command" procedure on page 2-233.

Step 2 If the condition does not clear, log into the Cisco 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.

2.7.170 LOF (BITS)

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

SDH Logical Object: BITS

The Loss of Frame (LOF) BITS alarm occurs when a port on the TCC2/TCC2P card BITS input detects an LOF on the incoming BITS timing reference signal. LOF indicates that the receiving ONS 15454 SDH has lost frame delineation in the incoming data.

Note The procedure assumes that the BITS timing reference signal is functioning properly and that the alarm is not appearing during node turn-up.

Clear the LOF (BITS) Alarm

Step 1 Verify that the line framing and line coding match between the BITS input and the TCC2/TCC2P card by completing the following steps:

a. In node view or card view, note the slot and port reporting the alarm.

b. Find the coding and framing formats of the external BITS timing source. The formats should be in the user documentation for the external BITS timing source or on the timing source itself.

c. Click the **Provisioning > Timing > BITS Facilities** tabs to display the General Timing window.

d. Verify that the value listed in Coding matches the coding of the BITS timing source (either B8ZS or AMI).

e. If the coding does not match, click the BITS-1 or BITS2 Coding field and choose the appropriate coding from the drop-down list.

f. Verify that the value listed in the Framing field matches the framing of the BITS timing source (either ESF or SF).

g. If the framing does not match, click the BITS-1 or BITS-2 Framing field and choose the appropriate framing from the drop-down list.

Note On the timing subtab, the binary 8-zero substitution (B8ZS) coding field is normally paired with Extended Superframe (ESF) in the Framing field and the alternate mark inversion (AMI) coding field is normally paired with SF (D4) in the Framing field.

Step 2 If the alarm does not clear when the line framing and line coding match between the BITS input and the TCC2/TCC2P card, replace the TCC2/TCC2P card by using the "Physically Replace a Traffic Card" procedure on page 2-242.

Caution Always use the supplied ESD wristband when working with a powered ONS 15454 SDH. Plug the wristband cable into the ESD jack located on the middle-right outside edge of the shelf assembly.

Note When you replace a card with the identical type of card, you do not need to make any changes to the database.

Step 3 If the alarm does not clear, log into the Cisco 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.

2.7.171 LOF (DS1, DS3, E1, E4, STM1E, STMN)

Default Severity: Critical (CR), Service-Affecting (SA) for DS3, E4, STMN, STM1E; Default Severity: Major (MJ), Service-Affecting (SA) for DS1, E1

SDH Logical Objects: DS1, DS3, E1, E4, STM1E, STMN

An LOF alarm on a DS1i-N-14, DS3i-N-12, E1-N-14, or E1-42 card for these objects means that the receiving ONS 15454 SDH has lost frame delineation in the incoming data. LOF occurs when the SDH overhead loses a valid framing pattern for three seconds. Receiving two consecutive valid patterns clears the alarm.

Clear the LOF (DS1, DS3, E1, E4, STM1E, STMN) Alarm

Step 1 Verify that the line framing and line coding match between the port and the signal source by completing the following steps:

a. In CTC, note the slot and port reporting the alarm.

b. Find the coding and framing formats of the signal source for the card reporting the alarm. You could need to contact your network administrator for the format information.

c. Display the card view of the reporting card.

d. Click the **Provisioning > Line** tabs.

e. Verify that the line type of the reporting port matches the line type of the signal source.

f. If the signal source line type does not match the reporting port, click **Line Type** and choose the appropriate type from the drop-down list.

g. Verify that the reporting Line Coding matches the signal source's line type.

h. If the signal source line coding does not match the reporting port, click **Line Coding** and choose the appropriate type from the drop-down list.

i. Click **Apply**.

Step 2 If the alarm does not clear when the coding and framing of the ONS 15454 SDH match the coding and framing of the signal source, replace the card.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454 SDH. Plug the wristband cable into the ESD jack located on the middle-right outside edge of the shelf assembly.

Note When replacing a card with the identical type of card, you do not need to change the CTC database.

Step 3 If the alarm does not clear, log into the Cisco 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.

2.7.172 LOF (TRUNK)

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.173 LO-LASERBIAS

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

SDH Logical Objects: EQPT, STMN

DWDM Logical Objects: PPM

The Equipment Low Transmit Laser Bias Current alarm is raised against the TXP, MXP, MRC-12, and OC192-XFP/STM64-XFP card laser performance. The alarm indicates that the card laser has reached the minimum laser bias tolerance.

If the LO-LASERBIAS alarm threshold is set at 0 percent (the default), the laser's usability has ended. If the threshold is set at 5 percent to 10 percent, the card is still usable for several weeks or months before you need to replace it.

Note For more information about provisioning MXP or TXP PPMs, refer to the "Provision Transponder and Muxponder Cards" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For more information about the cards themselves, refer to the "Card Reference" chapter.

Clear the LO-LASERBIAS Alarm

Step 1 Complete the "Physically Replace a Traffic Card" procedure on page 2-242.

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. Consult the *Cisco ONS 15454 SDH Procedure Guide* for procedures.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or 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.

2.7.174 LO-LASERTEMP

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

SDH Logical Objects: EQPT, STMN

DWDM Logical Object: PPM

The Equipment Low Laser Optical Transceiver Temperature alarm applies to the TXP, MXP, MRC-12, and OC192-XFP/STM64-XFP cards. HI-LASERTEMP occurs when the internally measured transceiver temperature falls below the card setting by 35.6 degrees F (2 degrees C). A laser temperature change affects the transmitted wavelength. (Two degrees temperature is equivalent to about 200 picometers in the wavelength.)

When the card raises this alarm, the laser is automatically shut off. The "LOS (STM1E, STMN)" alarm on page 2-147 is raised at the far-end node and the "DSP-FAIL" alarm on page 2-74 is raised at the near end. To verify the card laser temperature level, double-click the card in node view and click the **Performance > Optics PM > Current Values** tabs or the **Performance > Optics PM** tabs as appropriate to the reporting card. Maximum, minimum, and average laser temperatures are shown in the Current column entries in the Laser Temp rows.

Note For more information about provisioning MXP or TXP PPMs, refer to the "Provision Transponder and Muxponder Chapters" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For more information about the cards themselves, refer to the "Card Reference" chapter.

Clear the LO-LASERTEMP Alarm

Step 1 Complete the "Reset a Traffic Card in CTC" procedure on page 2-238 for the reporting MXP or TXP card.

Step 2 If the alarm does not clear, complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the reporting card.

Step 3 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or 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.

2.7.175 LOM

Default Severity: Critical (CR), Service-Affecting (SA) for TRUNK, VCMON-HP; Major (MJ), Service-Affecting (SA) for VCTRM-HP, VCTRM-LP

SDH Logical Objects: VCMON-HP, VCTRM-HP, VCTRM-LP

DWDM Logical Object: TRUNK

The optical transport unit (OTU) Loss of Multiframe is a VCAT member alarm. (VCAT member circuits are independent circuits that are concatenated from different time slots into a higher-rate signal.) The alarm applies to MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, TXP_MR_10E, or TXPP_MR_2.5G cards when the Multi Frame Alignment Signal (MFAS) overhead field is errored for more than five frames and persists for more than three ms.

Note For more information about MXP or TXP cards, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Clear the LOM Alarm

Step 1 Complete the "Clear the SD (DS3, E1, E3, E4, STM1E, STM-N) Condition" procedure on page 2-193.

Step 2 If the alarm does not clear, log into the Cisco 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.

2.7.176 LO-RXPOWER

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

SDH Logical Object: STMN

DWDM Logical Objects: 2R, ESCON, FC, GE, ISC, 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, and MXP_2.5G_10G card received optical signal power. LO-RXPOWER occurs when the measured optical power of the received signal falls below the threshold value, which is user-provisionable.

Note For more information about MXP and TXP cards, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Note When you upgrade a node to Software Release 6.0 or later, this enables received optical power PMs for the STM1-8, STM64-SR, STM64-IR, STM64-ITU, STM64-XFP, MRC-12, and MRC25G-4 cards. The newly enabled HI-RXPOWER and LO-RXPOWER alarms require that you initialize a site-accepted optical power (OPR0) nominal value after the upgrade. (To do this, refer to the procedure in the "Turn Up a Node" chapter in the *Cisco ONS 15454 SDH Procedure Guide*.) When you apply the value change, CTC uses the new OPR0 value to calculate PM percentage values. If you do not change the nominal value, the HI-RXPOWER or LO-RXPOWER may be raised in response to the unmodified setting.

Clear the LO-RXPOWER Alarm

Step 1 At the transmit end of the errored circuit, increase the transmit power level within safe limits.

Step 2 Find out whether new channels have been added to the fiber. Up to 32 channels can be transmitted on the same fiber, but the number of channels affects power. If channels have been added, the power levels of all channels need to be adjusted.

Note If the card is part of an amplified DWDM system, adding channels on the fiber affects the transmission power of each channel more than it would in an unamplified system.

Step 3 Find out whether the gain (amplification power) of any amplifiers has been changed. Changing amplification also causes channel power to need adjustment.

Step 4 If the alarm does not clear, remove any receive fiber attenuators or replace them with lower-resistance attenuators.

Step 5 If the alarm does not clear, inspect and clean the receive and transmit node fiber connections according to site practice. If no site practice exists, complete the procedure in the "Maintain the Node" chapter in the *Cisco ONS 15454 SDH Procedure Guide*.

Step 6 If the alarm does not clear, ensure that the fiber is not broken or damaged by testing it with an optical test set. If no test set is available, use the fiber for a facility (line) loopback on a known-good port. The error reading you get is not as precise, but you generally know whether the fiber is faulty. For specific procedures to use the test set equipment, consult the manufacturer.

Step 7 If the alarm does not clear, and no faults are present on the other ports of the transmit or receive card, do a facility loopback on the transmit and receive ports with known-good loopback cable. Complete the Create the Facility (Line) Loopback on the Source Optical Port, page 1-39 and test the loopback.

Step 8 If a port is bad and you need to use all the port bandwidth, complete the "Physically Replace a Traffic Card" procedure on page 2-242. If the port is bad but you can move the traffic to another port, replace the card at the next available maintenance window.

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. See the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-230 for commonly used traffic-switching procedures.

Note When you replace a card with the identical type of card, you do not need to make any changes to the database.

Step 9 If the alarm does not clear, log into the Cisco 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.

2.7.177 LOS (2R)

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.178 LOS (BITS)

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

SDH Logical Object: BITS

The LOS (BITS) alarm indicates that the TCC2/TCC2P card has an LOS from the BITS timing source. An LOS (BITS) occurs when an SDH receiver detects an all-zero pattern for 10 microseconds or longer. An LOS (BITS) means the BITS clock or the connection to it failed.

Clear the LOS (BITS) Alarm

Step 1 Verify the wiring connection from the BITS pins on the MIC-C/T/P to the timing source.

Caution Always use the supplied ESD wristband when working with a powered ONS 15454 SDH. Plug the wristband cable into the ESD jack located on the middle-right outside edge of the shelf assembly.

Step 2 If wiring is good, verify that the BITS clock is operating properly.

Step 3 If the alarm does not clear, log into the Cisco 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.

2.7.179 LOS (DS1, DS3)

Default Severities: Critical (CR), Service-Affecting (SA) for DS3; Major (MJ), Service-Affecting (SA) for DS1

SDH Logical Objects: DS1, DS3

A LOS (DS3) alarm for a DS1i_N-14 or DS3i-N-12 port occurs when the port on the card is in service but no signal is being received. The cabling might not be correctly connected to the card, or no signal exists on the line.

Clear the LOS (DS1, DS3) Alarm

Step 1 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 *Cisco ONS 15454 SDH Procedure Guide*.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454 SDH. Plug the wristband cable into the ESD jack located on the middle-right outside edge of the shelf assembly.

Step 2 Consult site records to determine whether the port raising the alarm has been assigned.

Step 3 If the port is not currently assigned, place the port out of service using the following steps:

- **a.** Double-click the card to display the card view.
- **b.** Click the **Maintenance > Loopback** tabs.
- **c.** Under **Admin State**, click **locked,disabled**.
- **d.** Click **Apply**.

Step 4 If the port is assigned, verify that the correct port is in service by completing the following steps:

- **a.** To confirm this physically, 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 this virtually, double-click the card in CTC to display the card view and complete the following substeps:

- Click the **Provisioning > Line** tabs.
- Verify that the **Admin State** column lists the port as **Unlocked**.
- If the **Admin State** column lists the port as locked,maintenance or locked,disabled, click the column and choose **Unlocked**. Click **Apply**.

Step 5 Use a test set to confirm that a valid signal exists on the line. Test the line as close to the receiving card as possible. For specific procedures to use the test set equipment, consult the manufacturer.

Step 6 Ensure that the transmit and receive outputs from the DSx panel to your equipment are properly connected. For more information about fiber connections and terminations, refer to the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15454 SDH Procedure Guide*.

Step 7 If there is a valid signal, replace the electrical connector on the ONS 15454 SDH.

Step 8 If a valid signal is not present and the transmitting device is operational, replace the fiber cable connecting the transmitting device to the port. To do this, refer to the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15454 SDH Procedure Guide* for procedures.

Step 9 Repeat Steps 1 to 8 for any other port on the card that reports the LOS.

Step 10 If no other alarms are present that could be the source of the LOS (DS-1 or DS-3), or if clearing an alarm did not clear the LOS, complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the reporting card.

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. See the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-230 for commonly used traffic-switching procedures.

Note When you replace a card with the identical type of card, you do not need to make any changes to the database.

Step 11 If the alarm does not clear, log into the Cisco 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.

2.7.180 LOS (E1, E3, E4)

Default Severity: Critical (CR), Service-Affecting (SA) for E3, E4; Major (MJ), Service-Affecting (SA) for E1

SDH Logical Objects: E1, E3, E4

LOS on an EC-N port occurs when a SDH receiver detects an all-zero pattern for 10 microseconds or longer. An LOS (EC-N) means that the upstream transmitter has failed. If an EC-N LOS alarm is not accompanied by additional alarms, a cabling problem is usually the cause of the alarm. The condition clears when two consecutive valid frames are received.

Note If a circuit shows a partial status 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 LOS (E1, E3, E4) Alarm

Step 1 Verify cabling continuity to the port reporting the alarm. To verify cable continuity, follow site practices.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454 SDH. Plug the wristband cable into the ESD jack located on the middle-right outside edge of the shelf assembly.

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 lit on the physical card.

   A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

b. To determine whether the port is in service, double-click the card in CTC to display the card view.

c. Click the **Provisioning > Line** tabs.

d. Verify that the **Admin State** column lists the port as Unlocked.

e. If the **Admin State** column lists the port as locked,maintenance or locked,disabled, click the column and choose **Unlocked**. Click **Apply**.

Step 3 If the correct port is in service, 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 4 If the signal is valid, ensure that the transmit and receive outputs from the electrical panel to your equipment are properly connected. For more information about fiber connections and terminations, refer to the "Install Cards and Fiber-Optic Cables" chapter in the *Cisco ONS 15454 SDH Procedure Guide*.

Step 5 If a valid signal exists, replace the cable connector on the ONS 15454 SDH.

Step 6 Repeat Steps 1 through 5 for any other port on the card that reports the LOS (EC-N).

Step 7 If the alarm does not clear, look for and troubleshoot any other alarm that could identify the source of the problem.

Step 8 If no other alarms exist that could be the source of the LOS (EC-N), or if clearing an alarm did not clear the LOS, complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the reporting card.

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. See the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-230 for commonly used traffic-switching procedures.

Note When you replace a card with the identical type of card, you do not need to make any changes to the database.

Step 9 If the alarm does not clear, log into the Cisco 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.

2.7.181 LOS (ESCON)

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.182 LOS (FUDC)

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

SDH Logical Object: FUDC

The LOS (FUDC) alarm is raised if there is a UDC circuit created on the AIC-I DCC port but the port is not receiving signal input. The downstream node has an AIS condition raised against AIC-I DCC port transmitting the UDC.

Clear the LOS (FUDC) Alarm

Step 1 Verify cable continuity to the AIC-I UDC port. To verify cable continuity, follow site practices.

Step 2 Verify that there is a valid input signal using a test set. For specific procedures to use the test set equipment, consult the manufacturer.

Step 3 If there is a valid signal, clean the fiber according to site practice. If no site practice exists, complete the procedure for cleaning optical connectors in the "Maintain the Node" chapter of the *Cisco ONS 15454 SDH Procedure Guide*.

Step 4 If the alarm does not clear, verify that the UDC is provisioned by completing the following steps:

- **a.** At the network view, click the **Provisioning > Overhead Circuits** tabs.
- **b.** If no UDC circuit exists, create one. Refer to the "Create Circuits and Tunnels" chapter in the *Cisco ONS 15454 SDH Procedure Guide* for procedures.
- **c.** If a user data circuit exists (shown as User Data F1 under the Type column), check the source and destination ports. These must be located on AIC-I cards to function.

Step 5 If the alarm does not clear, look for and troubleshoot any other alarm that could identify the source of the problem.

Step 6 If no other alarms exist that could be the source of the LOS (FUDC), or if clearing another alarm did not clear the LOS, complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the reporting card.

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. See the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-230 for commonly used traffic-switching procedures.

Note When you replace a card with the identical type of card, you do not need to make any changes to the database.

Step 7 If the alarm does not clear, log into the Cisco 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.

2.7.183 LOS (ISC)

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.184 LOS (MSUDC)

The LOS (MSUDC) alarm is not supported in this release. It is reserved for future development.

2.7.185 LOS (OTS)

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.186 LOS (STM1E, STMN)

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

SDH Logical Objects: STM1E, STMN

A LOS alarm for an STM1E or STM-N port occurs when the port on the card is in service but no signal is being received. The cabling might not be correctly connected to the card, or no signal exists on the line. Possible causes for no signal on the line include upstream equipment failure.

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.

Note For more information about Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.

Clear the LOS (STM1E, STMN) Alarm

Step 1 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 *Cisco ONS 15454 SDH Procedure Guide*.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454 SDH. Plug the wristband cable into the ESD jack located on the middle-right outside edge of the shelf assembly.

If an optical time-division multiplexing (TDM) signal such as an STM-1 or STM-4 is plugged into an E1000-2-G or G1000-4 card GBIC connector, this can trigger an LOS.

Step 2 Consult site records to determine whether the port raising the alarm has been assigned.

Step 3 If the port is assigned, verify that the correct port is in service by completing the following steps:

a. To confirm this physically, confirm that the card shows a green LED on the physical card.

A green LED indicates an active card. An amber LED indicates a standby card.

b. To determine this virtually, double-click the card in CTC to display the card view and complete the following substeps:

- Click the **Provisioning > Line** tabs.
- Verify that the **Admin State** column lists the port as Unlocked.

c. If the **Admin State** column lists the port as locked,maintenance or locked,disabled, click the column and choose **Unlocked.**

d. Click **Apply**.

Step 4 Check the incoming optical power through CTC (if available) or with an optical power meter to ensure that it at the correct level as determined by Cisco MetroPlanner.

Step 5 Use a test set to confirm that a valid signal exists on the line. Test the line as close to the receiving card as possible. For specific procedures to use the test set equipment, consult the manufacturer.

Step 6 Ensure that the transmit and receive outputs from the electrical panel to your equipment are properly connected. For more information about fiber connections and terminations, refer to the *Cisco ONS 15454 SDH Procedure Guide*.

Step 7 If there is a valid signal, replace the electrical connector on the ONS 15454 SDH.

Step 8 If a valid signal is not present and the transmitting device is operational, replace the cable connecting the transmitting device to the port. To do this, refer to the "Install Hardware" chapter in the *Cisco ONS 15454 SDH Procedure Guide*.

Step 9 Repeat Steps 1 to 8 for any other port on the card that reports the LOS.

Step 10 If no other alarms are present that could be the source of the LOS, or if clearing an alarm did not clear the LOS, complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the reporting card.

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. See the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-230 for commonly used traffic-switching procedures.

Note When you replace a card with the identical type of card, you do not need to make any changes to the database.

Step 11 If the alarm does not clear, log into the Cisco 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.

2.7.187 LOS (TRUNK)

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.188 LOS-O

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.189 LOS-P

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.190 LO-TXPOWER

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

SDH Logical Objects: EQPT, STMN

DWDM Logical Objects: 2R, ESCON, FC, GE, ISC, PPM, TRUNK

The Equipment Low Transmit Power alarm is an indicator for TXP, MXP, MRC-12, and OC192-XFP/STM64-XFP card transmitted optical signal power. LO-TXPOWER occurs when the measured optical power of the transmitted signal falls under the threshold. The threshold value is user-provisionable.

Note For more information about provisioning MXP or TXP PPMs, refer to the "Provision Transponder and Muxponder Cards" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For more information about the cards themselves, refer to the "Card Reference" chapter.

Clear the LO-TXPOWER Alarm

Step 1 Display the reporting card view.

Step 2 Click the **Provisioning > Optics Thresholds > Current Values** tabs or the **Provisioning > Optics Thresholds** tabs as appropriate to the reporting card.

Step 3 Increase the TX Power Low column value by 0.5 dBm.

Step 4 If the card transmit power setting cannot be increased without affecting the signal, complete the "Physically Replace a Traffic Card" procedure on page 2-242.

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. See the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-230 for commonly used traffic-switching procedures.

Note When you replace a card with the identical type of card, you do not need to make any changes to the database.

Step 5 If no ports are shown bad and the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or 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.

2.7.191 LPBKCRS

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

SDH Logical Objects: VCMON-HP, VCTRM-HP

The Loopback Cross-Connect condition indicates that there is a software cross-connect loopback active between an optical card and an STM-64 card. A cross-connect loopback test occurs below line speed and does not affect traffic.

For more information on loopbacks, see the "1.2 Troubleshooting Electrical Circuit Paths With Loopbacks" section on page 1-9.

Note Cross-connect loopbacks occur below line speed. They do not affect traffic.

Clear the LPBKCRS Condition

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" procedure on page 2-244.

Step 3 If the condition 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.

2.7.192 LPBKDS1FEAC-CMD

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

SDH Logical Object: DS1

The DS-1 Loopback Command Sent To Far End condition occurs on the near-end node when you send a DS-1 FEAC loopback.

Note LPBKDS1FEAC-CMD is an informational condition and does not require troubleshooting.

Caution CTC permits loopbacks to be performed on an unlocked circuit. Loopbacks are Service-Affecting (SA).

2.7.193 LPBKDS3FEAC

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

SDH Logical Object: DS3

A Loopback Due to FEAC Command DS-3 condition occurs when a DS3i-N-12 port loopback signal is received from the far-end node because of an FEAC command. An FEAC command is often used with loopbacks. LPBKDS3FEAC is only reported by DS3i-N-12 cards. A DS3i-N-12 card generates and reports FEAC alarms or conditions.

Caution CTC permits loopbacks on an unlocked circuit. Loopbacks are Service-Affecting (SA).

Note LPBKDS3FEAC is an informational condition. It does not require troubleshooting.

Clear the LPBKDS3FEAC Condition

Step 1 Complete the "Clear a Non-STM Card Facility or Terminal Loopback Circuit" procedure on page 2-245.

Step 2 If the condition does not clear, log into the Cisco 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.

2.7.194 LPBKDS3FEAC-CMD

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

SDH Logical Objects: DS3, E3

The DS-3 Loopback Command Sent To Far End condition occurs on the near-end node when you send a DS-3 FEAC loopback to a DS3i-N-12 card. For more information about FEAC loopbacks, see the "1.2 Troubleshooting Electrical Circuit Paths With Loopbacks" section on page 1-9.

Note LPBKDS3FEAC-CMD is an informational condition. It does not require troubleshooting.

2.7.195 LPBKE1FEAC

The LPBKE1FEAC condition is not used in this platform in this release. It is reserved for future development.

2.7.196 LPBKE3FEAC

The LPBKE3FEAC condition is not used in this platform in this release. It is reserved for future development.

2.7.197 LPBKFACILITY (CE100T)

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

SDH Logical Object: CE100T

A Loopback Facility condition on a CE-100T-8 port occurs when a software facility (line) loopback is active for a port on the card.

For information about troubleshooting Ethernet circuits with loopbacks, see the "1.4 Troubleshooting Ethernet Circuit Paths With Loopbacks" section on page 1-61.

Note For more information about Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.*

Clear the LPBKFACILITY (CE100T) Condition

Step 1 Complete the "Clear a Non-STM Card Facility or Terminal Loopback Circuit" procedure on page 2-245.

Step 2 If the condition 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.

2.7.198 LPBKFACILITY (DS1, DS3)

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

SDH Logical Objects: DS1, DS3

A Loopback Facility condition for a DS-1 or DS-3 signal occurs when a software facility (line) loopback is active for a DS1 port on a DS1i-N-14 or a DS3 port on the reporting DS3i-N-12 card.

For information about troubleshooting optical circuits with loopbacks, see the "1.2 Troubleshooting Electrical Circuit Paths With Loopbacks" section on page 1-9. Facility loopbacks are described in the "1.1 Troubleshooting Non-DWDM Circuit Paths with Loopbacks" section on page 1-2.

Note CTC permits loopbacks to be performed on an unlocked circuit. Performing a loopback is Service-Affecting (SA). If you did not perform a lockout or Force switch to protect traffic, the LPBKFACILITY condition can be accompanied by a more serious alarms such as LOS.

Note DS-3 facility (line) loopbacks do not transmit an AIS in the direction away from the loopback. Instead of AIS, a continuance of the signal transmitted to the loopback is provided.

Clear the LPBKFACILITY (DS1, DS3) Condition

Step 1 Complete the "Clear a Non-STM Card Facility or Terminal Loopback Circuit" procedure on page 2-245.

Step 2 If the condition 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.

2.7.199 LPBKFACILITY (E1, E3, E4)

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

SDH Logical Objects: E1, E3, E4

A Loopback Facility condition for an E-1, E-3, or E-4 signal occurs when a software facility loopback is active for a port on the reporting E-N card.

For more information on loopbacks, see the "1.1 Troubleshooting Non-DWDM Circuit Paths with Loopbacks" section on page 1-2 or the "1.2 Troubleshooting Electrical Circuit Paths With Loopbacks" section on page 1-9.

Caution CTC permits loopbacks to be performed on an unlocked circuit. Loopbacks are Service-Affecting (SA).

Clear the LPBKFACILITY (E1, E3, E4) Condition

Step 1 Complete the "Clear a Non-STM Card Facility or Terminal Loopback Circuit" procedure on page 2-245.

Step 2 If the condition does not clear, log into the Cisco 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.

2.7.200 LPBKFACILITY (ESCON)

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.201 LPBKFACILITY (FC)

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.202 LPBKFACILITY (FCMR)

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

SDH Logical Object: FCMR

A Loopback Facility for FCMR condition occurs when a facility loopback is provisioned on an FC_MR-4 card.

For information about troubleshooting optical circuits with loopbacks, see the "1.1 Troubleshooting Non-DWDM Circuit Paths with Loopbacks" section on page 1-2.

Clear the LPBKFACILITY (FCMR) Condition

Step 1 Complete the "Clear a Non-STM Card Facility or Terminal Loopback Circuit" procedure on page 2-245.

Step 2 If the condition 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.

2.7.203 LPBKFACILITY (G1000)

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

SDH Logical Object: G1000

A Loopback Facility condition for the G1000 object occurs when a software facility (line) loopback is active for a port on the reporting G-Series Ethernet card.

For information about troubleshooting optical circuits with loopbacks, see the "1.3 Troubleshooting Optical Circuit Paths With Loopbacks" section on page 1-38. Facility loopbacks are described in the "1.1 Troubleshooting Non-DWDM Circuit Paths with Loopbacks" section on page 1-2.

Caution CTC permits loopbacks to be performed on an unlocked circuit. Loopbacks are Service-Affecting (SA).

Note For more information about Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.

Clear the LPBKFACILITY (G1000) Condition

Step 1 Complete the "Clear a Non-STM Card Facility or Terminal Loopback Circuit" procedure on page 2-245.

Step 2 If the condition 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.

2.7.204 LPBKFACILITY (GE)

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.205 LPBKFACILITY (ISC)

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.206 LPBKFACILITY (STM1E, STMN)

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

SDH Logical Objects: STM1E, STMN

A Loopback Facility condition for an STM1E or STM-N occurs when a software facility loopback is active for a port on the reporting card.

For more information on loopbacks, see the "1.1 Troubleshooting Non-DWDM Circuit Paths with Loopbacks" section on page 1-2 or the "1.2 Troubleshooting Electrical Circuit Paths With Loopbacks" section on page 1-9.

Caution CTC permits loopbacks to be performed on an unlocked circuit. Loopbacks are Service-Affecting (SA).

Clear the LPBKFACILITY (STM1E, STMN) Condition

Step 1 Complete the "Clear an STM-N Card Facility or Terminal Loopback Circuit" procedure on page 2-244.

Step 2 If the condition does not clear, log into the Cisco 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.

2.7.207 LPBKFACILITY (TRUNK)

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.208 LPBKTERMINAL (CE100T)

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

SDH Logical Object: CE100T

A Loopback Terminal condition on a CE-100T-8 port occurs when a software terminal loopback is active for a port on the card.

For information about troubleshooting Ethernet circuits with loopbacks, see the "1.4 Troubleshooting Ethernet Circuit Paths With Loopbacks" section on page 1-61.

Note For more information about Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.

Clear the LPBKTERMINAL (CE100T) Condition

Step 1 Complete the "Clear a Non-STM Card Facility or Terminal Loopback Circuit" procedure on page 2-245.

Step 2 If the condition does not clear, log into the Cisco 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.

2.7.209 LPBKTERMINAL (DS1, DS3)

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

SDH Logical Objects: DS1, DS3

A Loopback Terminal condition for a DS-1 or DS-3 signal occurs when a software terminal (inward) loopback is active for a DS-1 port on a DS1i-N-14 card or a DS-3 port on the reporting DS3i-N-12 card.

For more information on loopbacks, see the "1.1 Troubleshooting Non-DWDM Circuit Paths with Loopbacks" section on page 1-2.

Note DS-3 terminal loopbacks do not transmit the "MS-AIS" condition on page 2-173 in the direction away from the loopback. Instead of MS-AIS, a continuance of the signal transmitted into the loopback is provided.

Caution CTC permits loopbacks to be performed on an unlocked circuit. Loopbacks are Service-Affecting (SA).

Clear the LPBKTERMINAL (DS3) Condition

Step 1 Complete the "Clear a Non-STM Card Facility or Terminal Loopback Circuit" procedure on page 2-245.

Step 2 If the condition does not clear, log into the Cisco 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.

2.7.210 LPBKTERMINAL (E1, E3, E4)

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

SDH Logical Objects: E1, E3, E4

A Loopback Terminal for an E-1, E-3, or E-4 signal condition occurs when a software terminal (inward) loopback is active for a port on the reporting E-N card.

For more information on loopbacks, see the "1.1 Troubleshooting Non-DWDM Circuit Paths with Loopbacks" section on page 1-2.

Caution CTC permits loopbacks to be performed on an unlocked circuit. Loopbacks are Service-Affecting (SA).

Clear the LPBKTERMINAL (E1, E3, E4) Condition

Step 1 Complete the "Clear a Non-STM Card Facility or Terminal Loopback Circuit" procedure on page 2-245.

Step 2 If the condition does not clear, log into the Cisco 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.

2.7.211 LPBKTERMINAL (ESCON)

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.212 LPBKTERMINAL (FC)

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.213 LPBKTERMINAL (FCMR)

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

SDH Logical Object: FCMR

A Loopback Terminal for FCMR condition occurs when a terminal loopback is provisioned on an FC_MR-4 card.

For information about troubleshooting optical circuits with loopbacks, see the "1.1 Troubleshooting Non-DWDM Circuit Paths with Loopbacks" section on page 1-2.

Clear the LPBKTERMINAL (FCMR) Condition

Step 1 Complete the "Clear a Non-STM Card Facility or Terminal Loopback Circuit" procedure on page 2-245.

Step 2 If the condition 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.

2.7.214 LPBKTERMINAL (G1000)

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

SDH Logical Object: G1000

A Loopback Terminal condition for the G1000 object occurs when a software terminal (inward) loopback is active for a port on the reporting G-Series Ethernet card.

When a port in terminal (inward) loopback, its outgoing signal is redirected into the receive direction on the same port, and the externally received signal is ignored. On the G-Series card the outgoing signal is not transmitted; it is only redirected in the receive direction.

For more information about troubleshooting optical circuits, see the "1.1 Troubleshooting Non-DWDM Circuit Paths with Loopbacks" section on page 1-2.

Caution CTC permits loopbacks to be performed on an unlocked circuit. Loopbacks are Service-Affecting (SA).

Note For more information about Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.*

Clear the LPBKTERMINAL (G1000) Condition

Step 1 Complete the "Clear a Non-STM Card Facility or Terminal Loopback Circuit" procedure on page 2-245.

Step 2 If the condition 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.

2.7.215 LPBKTERMINAL (GE)

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.216 LPBKTERMINAL (ISC)

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.217 LPBKTERMINAL (STM1E, STMN)

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

SDH Logical Objects: STM1E, STMN

A Loopback Terminal for an STM-1E or STM-N signal condition occurs when a software terminal (inward) loopback is active for a port on the reporting traffic card.

For more information on loopbacks, see the "1.1 Troubleshooting Non-DWDM Circuit Paths with Loopbacks" section on page 1-2.

Caution CTC permits loopbacks to be performed on an unlocked circuit. Loopbacks are Service-Affecting (SA).

Clear the LPBKTERMINAL (STM1E, STMN) Condition

Step 1 Complete the "Clear an STM-N Card Facility or Terminal Loopback Circuit" procedure on page 2-244.

Step 2 If the condition does not clear, log into the Cisco 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.

2.7.218 LPBKTERMINAL (TRUNK)

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.219 LP-ENCAP-MISMATCH

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

SDH Logical Object: VCTRM-LP

The Encapsulation C2 Byte Mismatch Path 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 LP-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 LP-ENCAP-MISMATCH alarm is if a circuit created between two ML-Series cards has GFP framing provisioned on one end and HLDC 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)

Note By default, an LP-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**.

Note For more information about the ML-Series Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.*

Clear the LP-ENCAP-MISMATCH Alarm

Step 1 Ensure that the correct framing mode is in use on the transmit card, and that it is identical to the receive 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 2 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 **IOS** tab and click **Open IOS Connection**. Refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327* entries on all three of these topics to obtain the full configuration command sequences.

Step 3 If the alarm does not clear, log into the Cisco 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.

2.7.220 LP-PLM

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

SDH Logical Object: VCTRM- LP

The SLMF-PLM Low-Order Path Label Mismatch alarm applies to the V5 byte in low-order (VC-2 or VC-1) path overhead. LP-PLM occurs when there is a mismatch between the transmitted and received V5 byte received in the SDH payload overhead.

The LP-PLM alarm occurs when the optical (traffic) cards cannot detect the value of the C2 byte in the payload. The low-order C2 byte would cause the LP-PLM to occur on terminating cards.

Clear the LP-PLM Alarm

Step 1 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 **Admin State** column lists the port as discovered.

c. If the **Admin State** column lists the port as incomplete, wait 10 minutes for the ONS 15454 SDH to initialize fully. If the incomplete state does not change after full initialization, log into the Cisco 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.

Step 2 After verifying that the port is active, verify the signal source to the electrical card reporting the alarm with an optical test set according to site specific practice. For specific procedures to use the test set equipment, consult the manufacturer.

Step 3 If traffic is being affected, complete the "Delete a Circuit" procedure on page 2-243.

Caution Deleting a circuit can affect traffic.

Step 4 Recreate the circuit with the correct circuit size. Refer to the "Create Circuits and Tunnels" chapter in the *Cisco ONS 15454 SDH Procedure Guide* for circuit procedures.

Step 5 If the circuit deletion and re-creation does not clear the alarm, verify the far-end STM-N card that provides the payload to the electrical card.

Step 6 If the alarm does not clear, verify the cross-connect between the STM-N card and the electrical card.

Step 7 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 *Cisco ONS 15454 SDH Procedure Guide*.

Step 8 If the alarm does not clear, complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the reporting traffic card.

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. See the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-230 for commonly used traffic-switching procedures.

Note When you replace a card with the identical type of card, you do not need to make any changes to the database.

Step 9 If the alarm does not clear, log into the Cisco 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.

2.7.221 LP-RFI

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

SDH Logical Object: VCTRM-LP

The Low-Order RFI condition indicates that there is a remote failure indication in the low-order (VC-2 or VC-1) path, and that the failure has persisted beyond the maximum time allotted for transmission system protection. The LP-RFI is sent as the protection switch is initiated. Resolving the fault in the adjoining node clears the LP-RFI condition in the reporting node.

Clear the LP-RFI Condition

Step 1 Log into the far-end node of the reporting ONS 15454 SDH.

Step 2 Determine whether there are other alarms, especially the "LOS (STM1E, STMN)" alarm on page 2-147.

Step 3 Clear the alarms. See the appropriate alarm section in this chapter for the procedure.

Step 4 If the condition does not clear, log into the Cisco 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.

2.7.222 LP-TIM

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

SDH Logical Object: VCTRM-LP

The Low-Order Path Section TIM alarm occurs when the expected J2 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.

LP-TIM also occurs on a port that has previously been operating without alarms if someone switches or removes the electrical cables or optical fibers that connect the ports. TIM is usually accompanied by other alarms, such as the "LOS (STM1E, STMN)" alarm on page 2-147 or the "LP-UNEQ" alarm on page 2-163. If these alarms accompany the "TIM" alarm on page 2-216, reattach or replace the original cables/fibers to clear the alarms.

Clear the LP-TIM Alarm

Step 1 Complete the "Clear the TIM Alarm" procedure on page 2-216 for the J2 byte.

Step 2 If the alarm does not clear, log into the Cisco 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 problem.

2.7.223 LP-UNEQ

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

SDH Logical Objects: VCMON-LP, VCTRM-LP

The SLMF Unequipped Low-Order Path Unequipped alarm applies to the V5 byte in low-order (VC-2 or VC-1) path overhead. LP-UNEQ occurs when no V5 byte is received in the SDH payload overhead.

Clear the LP-UNEQ Alarm

Step 1 In node view, click **View > 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 VCT, which indicates a VC tunnel circuit. A VC tunnel with no VCs assigned could be the cause of an LP-UNEQ alarm.

Step 5 If the Type column does not contain VCT, there are no VC tunnels connected with the alarm. Go to Step 7.

Step 6 If the Type column does contain VCT(s), attempt to delete the row(s) by completing the following steps:

Note The node does not allow you to delete a valid VT tunnel or one with a valid VT circuit inside.

a. Click the VC tunnel circuit row to highlight it. Complete the "Delete a Circuit" procedure on page 2-243.

b. If an error message dialog box appears, the VC tunnel is valid and not the cause of the alarm.

c. If any other columns contain VCT, repeat Steps a and b.

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 PARTIAL 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 partial circuits.

Complete the "Delete a Circuit" procedure on page 2-243.

Step 10 Recreate the circuit with the correct circuit size. Refer to the "Create Circuits and Tunnels" chapter in the *Cisco ONS 15454 SDH Procedure Guide* for circuit creation 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 of the *Cisco ONS 15454 SDH Procedure Guide*.

Warning **On the OC192 LR/STM64 LH 1550 card, the laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. The laser is off when the safety key is off (labeled 0).** Statement 293.

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

Warning **Use of controls, adjustments, or performing procedures other than those specified could result in hazardous radiation exposure.** Statement 1057

Step 13 If the alarm does not clear, complete the "Physically Replace a Traffic Card" procedure on page 2-242 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. See the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-230 for information.

Note When you replace a card with the identical type of card, you do not need to make any changes to the database.

Step 14 If the alarm does not clear, log into the Cisco 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.

2.7.224 MAN-REQ

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

SDH Logical Objects: EQPT, VCMON-HP, VCMON-LP

The Manual Switch Request condition occurs when a user initiates a Manual switch request on an STM-N port. Clearing the Manual switch clears the MAN-REQ condition. You do not need to clear the switch if you want the manual switch to remain.

Clear the MAN-REQ Condition

Step 1 Complete the "Initiate a 1+1 Protection Port Manual Switch Command" procedure on page 2-231.

Step 2 If the condition does not clear, log into the Cisco 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.

2.7.225 MANRESET

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

SDH Logical Object: EQPT

A User-Initiated Manual Reset condition occurs when you right-click a card in CTC and choose Reset. Resets performed during a software upgrade also prompt the condition. The MANRESET condition clears automatically when the card finishes resetting.

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

2.7.226 MANSWTOINT

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

SDH Logical Object: NE-SREF

The Manual Switch To Internal Clock condition occurs when the NE timing source is manually switched to an internal timing source.

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

2.7.227 MANSWTOPRI

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

SDH Logical Objects: EXT-SREF, NE-SREF

The Manual Switch To Primary Reference condition occurs when the NE timing source is manually switched to the primary timing source.

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

2.7.228 MANSWTOSEC

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

SDH Logical Objects: EXT-SREF, NE-SREF

The Manual Switch To Second Reference condition occurs when the NE timing source is manually switched to a second timing source.

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

2.7.229 MANSWTOTHIRD

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

SDH Logical Objects: EXT-SREF, NE-SREF

The Manual Switch To Third Reference condition occurs when the NE timing source is manually switched to the tertiary timing source.

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

2.7.230 MANUAL-REQ-RING

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

SDH Logical Object: STMN

The Manual Switch Request on Ring condition occurs when a user initiates a MANUAL RING command on MS-SPRing rings to switch from working to protect or protect to working. This condition is visible on the network view Alarms, Conditions, and History tabs and is accompanied by WKSWPR. The port where the MANUAL RING command originated is marked with an "M" on the network view detailed circuit map.

Clear the MANUAL-REQ-RING Condition

Step 1 Complete the "Clear an MS-SPRing External Switching Command" procedure on page 2-238.

Step 2 If the condition does not clear, log into the Cisco 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.

2.7.231 MANUAL-REQ-SPAN

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

SDH Logical Object: STMN

DWDM Logical Objects: 2R, ESCON, FC, GE, ISC, TRUNK

The Manual Switch Request on Ring condition occurs on MS-SPRings when a user initiates a Manual Span command to move MS-SPRing 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.

Clear the MANUAL-REQ-SPAN Condition

Step 1 Complete the "Clear an MS-SPRing External Switching Command" procedure on page 2-238.

Step 2 If the condition does not clear, log into the Cisco 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.

2.7.232 MEA (BIC)

The MEA alarm for the BIC object is not used in this platform in this release. It is reserved for future development.

2.7.233 MEA (EQPT)

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

SDH Logical Object: EQPT

The MEA alarm for equipment is reported against a card slot when the physical card inserted into a slot does not match the card type that is provisioned for that slot in CTC.

Note When downgrading the CTC software from R6.0 to R5.0 and the XCVXC cross-connect card to the XCVXL for use in that release, the standby (Slot 8) XCVXL can raise the MEA alarm until the downgrade is complete.

Clear the MEA (EQPT) Alarm

Step 1 Physically verify the type of card that is installed in the slot reporting the MEA alarm. In node view, click the **Inventory** tab and compare it to the actual installed card.

Step 2 If you prefer the card type depicted by CTC, replace the physical card reporting the mismatch with the card type depicted by CTC (provisioned for that slot). Complete the "2.10.6 Air Filter and Fan Procedures" procedure on page 2-245.

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. See the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-230 for commonly used traffic-switching procedures.

Note When you replace a card with the identical type of card, you do not need to make any changes to the database.

Step 3 If you prefer the card that physically occupies the slot and the card is not in service, has no circuits mapped, and is not part of a protection group, place the cursor over the provisioned card in CTC and right-click to choose **Delete Card**.

The card that physically occupies the slot reboots, and CTC automatically provisions the card type into that slot.

Note If the card is in service, has a circuit mapped, is paired in a working/protection scheme, has DCC communications enabled, or is used as a timing reference, CTC does not allow you to delete the card.

Step 4 If any ports on the card are in service, place them out of service (Locked, maintenance) by completing the following steps:

Caution Before placing ports out of service, ensure that no live traffic is present.

a. Double-click the reporting card to display the card view.
b. Click the **Provisioning > Line** tab.
c. Click the **Admin State** column of any Unlocked ports.
d. Choose **Locked, maintenance** to take the ports out of service.

Step 5 If a circuit has been mapped to the card, complete the "Delete a Circuit" procedure on page 2-243.

Caution Before deleting the circuit, ensure that live traffic is not present.

Step 6 If the card is paired in a protection scheme, delete the protection group by completing the following steps:

a. Click the **Provisioning > Protection** tabs.
b. Choose the protection group of the reporting card.
c. Click **Delete**.
d. Click **Yes** in the Delete Protection Group dialog box.

Step 7 Right-click the card reporting the alarm.

Step 8 Choose **Delete**.

The card that physically occupies the slot reboots, and CTC automatically provisions the card type into that slot.

Step 9 If the alarm does not clear, log into the Cisco 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.

2.7.234 MEA (FAN)

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

SDH Logical Object: FAN

The Mismatch of Equipment Attributes alarm is reported against the fan-tray assembly when an older ONS 15454 SDH fan-tray assembly (FTA2) is used with certain cards that require the newer fan-tray assembly (15454E-FTA-48V). The 10-Gbps-compatible shelf assembly (15454E-SA-ETSI) and fan-tray assembly (15454E-FTA-48V) are required with the ONS 15454 SDH OC192 LR/STM64 LH 1550, E1000-2-G, E100T-G, OC48 IR/STM16 SH AS 1310, or OC48 LR/STM16 AS 1550 cards.

Note For more information about Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.*

Clear the MEA (FAN) Alarm

Step 1 Determine whether the ONS 15454 SDH shelf assembly is a newer ETSI 10-Gbps-compatible shelf assembly (15454E-SA-ETSI) or an earlier shelf assembly by completing the following steps:

- **a.** In node view, click the **Inventory** tab.
- **b.** In the HW Part # column, if the number is 800-08708-XX, then you have a 10-Gbps-compatible shelf assembly (15454-SA-HD).
- **c.** In the HW Part # column, if the number is not 800-08708-XX, then you are using an earlier shelf assembly.

Step 2 If you have a 10-Gbps-compatible shelf assembly (15454E-SA-ETSI), the alarm indicates that an older, incompatible fan-tray assembly is installed in the shelf assembly. Obtain a newer fan-tray assembly (15454-FTA3) with a 5 A fuse and complete the "Replace the Fan-Tray Assembly" procedure on page 2-247.

Step 3 If you are using an earlier shelf assembly, the alarm indicates that you are using a newer fan-tray assembly (15454-FTA3), which is incompatible with the earlier version of the shelf assembly. Obtain an earlier version of the fan-tray assembly (15454-FTA2) and complete the "Replace the Fan-Tray Assembly" procedure on page 2-247.

Step 4 If the alarm does not clear, log into the Cisco 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.

2.7.235 MEA (PPM)

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.236 MEM-GONE

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

SDH Logical Object: EQPT

The Memory Gone alarm occurs when data generated by software operations exceeds the memory capacity of the TCC2/TCC2P card. The TCC2/TCC2P cards which exceed the memory capacity reboot to avoid failure of card operations.

Note The alarm does not require user intervention. The MEM-LOW alarm always preceeds the MEM-GONE alarm.

2.7.237 MEM-LOW

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

SDH Logical Object: EQPT

The Free Memory of Card Almost Gone alarm occurs when data generated by software operations is close to exceeding the memory capacity of the TCC2/TCC2P card. The alarm clears when additional memory becomes available. If additional memory is not made available and the memory capacity of the card is exceeded, CTC ceases to function.

Note The alarm does not require user intervention. Log into the Cisco 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.

2.7.238 MFGMEM (AICI-AEP, AICI-AIE, PPM)

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

SDH Logical Objects: AICI-AEP, AICI-AIE

DWDM Logical Object: PPM

The Manufacturing Data Memory Failure (MFGMEM) alarm occurs if the ONS 15454 SDH cannot access the data in the electronically erasable programmable read-only memory (EEPROM). Either the memory module on the component failed or the TCC2/TCC2P card lost the ability to read that module. The EEPROM stores manufacturing data that is needed for both compatibility and inventory issues. Inability to read a valid MAC address disrupts IP connectivity and makes the ONS 15454 SDH icon on the CTC network view unavailable.

Clear the MFGMEM Alarm

Step 1 Complete the "Remove and Reinsert (Reseat) the Standby TCC2/TCC2P Card" procedure on page 2-241.

Wait ten minutes to verify that the standby TCC2/TCC2P card does not reset itself. If the TCC2/TCC2P card reset is not complete and error-free or if the TCC2/TCC2P card reboots itself, log into the Cisco Technical Support Website at http://www.cisco.com/techsupport for more information or log in to http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml to obtain a directory of toll-free Technical Support numbers for your country.

Note If CTC stops responding after performing a reset on the TCC2/TCC2P card, close the browser and start CTC again on the affected node.

Step 2 If the alarm does not clear, complete the "Remove and Reinsert (Reseat) Any Card" procedure on page 2-241.

Step 3 If the alarm does not clear, physically replace the standby TCC2/TCC2P card on the ONS 15454 SDH with a new TCC2/TCC2P card. Complete the "Physically Replace a Traffic Card" procedure on page 2-242.

Note The active TCC2/TCC2P card takes up to 30 minutes to transfer the system software to the newly installed TCC2/TCC2P card. Software transfer occurs in instances where different software versions exist on the two cards. During this operation, the TCC2/TCC2P card LEDs flash to indicate failure and then the active/standby LED flashes. When the transfer completes, the TCC2/TCC2P card reboots and goes into standby mode after approximately three minutes.

Step 4 Reset the active TCC2/TCC2P card. Complete the "Remove and Reinsert (Reseat) the Standby TCC2/TCC2P Card" procedure on page 2-241.

Wait ten minutes to verify that the standby TCC2/TCC2P card does not reset itself. If the TCC2/TCC2P card reset is not complete and error-free or if the TCC2/TCC2P card reboots itself, log into the Cisco 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.

Step 5 Physically replace the remaining TCC2/TCC2P card with the second TCC2/TCC2P card. Complete the "Physically Replace a Traffic Card" procedure on page 2-242.

The ONS 15454 SDH boots up the second TCC2/TCC2P card. The second TCC2/TCC2P card must also copy the system software, which can take up to twenty minutes.

Step 6 If the MFGMEM alarm continues to report after replacing the TCC2/TCC2P cards, the problem lies with the EEPROM.

Step 7 If the alarm does not clear, log into the Cisco 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.

2.7.239 MFGMEM (BPLANE, FAN)

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

SDH Logical Objects: BPLANE, FAN

The Manufacturing Data Memory (EEPROM) failure alarm occurs if the ONS 15454 SDH cannot access the data in the EEPROM. Lack of access occurs when either the memory module on the component fails or the TCC2/TCC2P card loses the ability to read that module. The EEPROM stores manufacturing data that is needed for both compatibility and inventory issues. An inability to read a valid MAC address disrupts IP connectivity and makes the ONS 15454 SDH icon on the CTC network view unavailable.

Clear the MFGMEM (BPLANE, FAN) Alarm

Step 1 Complete the "Remove and Reinsert (Reseat) the Standby TCC2/TCC2P Card" procedure on page 2-241.

Note If CTC stops responding after performing a reset on the TCC2/TCC2P card, close the browser and start CTC again on the affected node.

Step 2 If the alarm does not clear, complete the "Remove and Reinsert (Reseat) Any Card" procedure on page 2-241.

Step 3 Physically replace the remaining TCC2/TCC2P card with the second TCC2/TCC2P card. Complete the "Physically Replace a Traffic Card" procedure on page 2-242.

Note The active TCC2/TCC2P card takes up to 30 minutes to transfer the system software to the newly installed TCC2/TCC2P card. Software transfer occurs in instances where different software versions exist on the two cards. During this operation, the TCC2/TCC2P card LEDs flash to indicate failure and then the active/standby LED flashes. When the transfer completes, the TCC2/TCC2P card reboots and goes into standby mode after approximately three minutes.

Step 4 Perform a CTC reset on the TCC2/TCC2P card. Complete the "Remove and Reinsert (Reseat) the Standby TCC2/TCC2P Card" procedure on page 2-241.

Step 5 Verify that the remaining TCC2/TCC2P card is now in standby mode. (The ACT/STBY LED changes to amber.)

Step 6 Physically replace the remaining TCC2/TCC2P card with the second TCC2/TCC2P card. Complete the "Physically Replace a Traffic Card" procedure on page 2-242. (The procedure is similar.)

Step 7 If the MFGMEM alarm continues to report after replacing the TCC2/TCC2P cards, the problem lies with the EEPROM.

Step 8 If the MFGMEM is reported from the fan-tray assembly, replace the fan-tray assembly. Obtain a fan-tray assembly and complete the "Replace the Fan-Tray Assembly" procedure on page 2-247.

Step 9 If the MFGMEM is reported from backplane, or if the alarm persists after the fan-tray assembly is replaced, log into the Cisco 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.

2.7.240 MS-AIS

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

SDH Logical Objects: STM1E, STMN

The Multiplex Section (MS) AIS condition indicates that there is a defect in the multiplexing section layer of the SDH overhead. The multiplex section refers to the segment between two SDH devices in the circuit and is also known as a maintenance span. The multiplex section layer of the SDH overhead deals with payload transport, and its functions include multiplexing and synchronization.

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 MS-AIS Condition

Step 1 Complete the "Clear the AIS Condition" procedure on page 2-31.

Step 2 If the condition does not clear, log into the Cisco 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.

2.7.241 MS-EOC

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

SDH Logical Object: STMN

The MS-DCC Termination Failure alarm occurs when the ONS 15454 SDH loses its data communications channel. The DCC is three bytes, D1 through D3, in the SDH overhead. The bytes convey information about Operation, Administration, Maintenance, and Provisioning (OAM&P). The ONS 15454 SDH uses the DCC on the SDH section overhead to communicate network management information.

Clear the MS-EOC Alarm

Step 1 Complete the "Clear the EOC Alarm" procedure on page 2-77.

Step 2 If the condition does not clear, log into the Cisco 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.

2.7.242 MS-RFI

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

SDH Logical Object: STM1E

The MS Remote Fault Indication (RFI) condition indicates that there is an RFI occurring at the SDH overhead multiplexing section level.

An RFI occurs when the ONS 15454 SDH detects an RFI in the SDH 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

Step 1 Log into the far-end node of the reporting ONS 15454 SDH.

Step 2 Determine whether there are other alarms, especially the "LOS (STM1E, STMN)" alarm on page 2-147.

Step 3 Clear the main alarm. See the appropriate alarm section in this chapter for the procedure.

Step 4 If the condition does not clear, log into the Cisco 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.

2.7.243 MSSP-OOSYNC

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

SDH Logical Object: STMN

The Procedural Error MS-SPRing Out of Synchronization alarm occurs when you attempt to add or delete a circuit and a node on a working ring loses its DCC connection because all transmit and receive fiber has been removed. The CTC cannot generate a table of the nodes and causes the MSSP-OOSYNC alarm.

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 MSSP-OOSYNC Alarm

Step 1 Reestablish cabling continuity to the node reporting the alarm. Refer to the "Install Cards and Fiber-Optic Cables" chapter in the *Cisco ONS 15454 SDH Procedure Guide* for cabling procedures to reestablish the DCC. To verify cable continuity, follow site practices.

When the DCC is established between the node and the rest of the MS-SPRing, the DCC becomes visible to the MS-SPRing and should be able to function on the circuits.

Step 2 If alarms occur when you have provisioned the DCC, see the "EOC" alarm on page 2-76.

Step 3 If the alarm does not clear, log into the Cisco 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 problem.

2.7.244 MSSP-SW-VER-MISM

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

SDH Logical Object: STMN

The MS-SPRing Software Version Mismatch alarm is by the TCC2/TCC2P card when it checks all software versions for all nodes in a ring and discovers a mismatch in versions.

Clear the MSSP-SW-VER-MISM Alarm

Step 1 Clear the alarm by loading the correct software version on the TCC2/TCC2P card with the incorrect load. To download software, refer to the release-specific software download document.

Step 2 If the condition does not clear, log into the Cisco 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 to report a Service-Affecting (SA) problem.

2.7.245 NO-CONFIG

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

SDH Logical Object: EQPT

The No Startup Configuration alarm applies to ML-Series Ethernet (traffic) cards and occurs when you preprovision Slot 5 to 6 and Slot 12 to 13 for the card without inserting the card first, or when you insert a card without preprovisioning. (This is an exception to the usual rule in card provisioning.) Because this is normal operation, you should expect this condition during provisioning. When the startup configuration file is copied to the active TCC2/TCC2P card, the alarm clears.

Note For more information about the ML-Series Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.*

Clear the NO-CONFIG Alarm

Step 1 Create a startup configuration for the card in Cisco IOS.

Follow the card provisioning instructions in the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.*

Step 2 Upload the configuration file to the TCC2/TCC2P card by completing the following steps:

a. In node view, right-click the ML-Series card graphic.

b. Choose **IOS Startup Config** from the shortcut menu.

c. Click **Local > TCC** and navigate to the file location.

Step 3 Complete the "Reset a Traffic Card in CTC" procedure on page 2-238.

Step 4 If the condition does not clear, log into the Cisco 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.

2.7.246 NOT-AUTHENTICATED

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

SDH Logical Object: SYSTEM

The NOT-AUTHENTICATED alarm is raised by CTC (not by the NE) when it fails to log into a node. This alarm only displays in CTC where the login failure occurred. This alarm differs from the "INTRUSION-PSWD" alarm on page 2-128 in that INTRUSION-PSWD occurs when a user exceeds the login failures threshold.

Note NOT-AUTHENTICATED is an informational alarm and is resolved when CTC successfully logs into the node.

2.7.247 OCHNC-INC

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.248 ODUK-1-AIS-PM

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.249 ODUK-2-AIS-PM

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.250 ODUK-3-AIS-PM

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.251 ODUK-4-AIS-PM

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.252 ODUK-AIS-PM

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.253 ODUK-BDI-PM

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.254 ODUK-LCK-PM

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.255 ODUK-OCI-PM

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.256 ODUK-SD-PM

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.257 ODUK-SF-PM

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.258 ODUK-TIM-PM

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.259 OOU-TPT

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

SDH Logical Objects: VCTRM-HP, VCTRM-LP

The Out of Use Transport Failure alarm is a VCAT member alarm. (VCAT member circuits are independent circuits that are concatenated from different time slots into a higher-rate signal.) This condition is raised when a member circuit in a VCAT is unused, such as when it is removed by SW-LCAS. It occurs in conjunction with the "VCG-DEG" alarm on page 2-224.

Clear the OOT-TPT Condition

Step 1 Complete the "Clear the VCG-DEG Condition" procedure on page 2-225. Clearing that condition clears this condition as well.

Step 2 If the condition does not clear, log into the Cisco 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.

2.7.260 OPTNTWMIS

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.261 OPWR-HDEG

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.262 OPWR-HFAIL

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.263 OPWR-LDEG

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.264 OPWR-LFAIL

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.265 OSRION

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.266 OTUK-AIS

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.267 OTUK-BDI

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.268 OTUK-IAE

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.269 OTUK-LOF

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.270 OTUK-SD

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.271 OTUK-SF

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.272 OTUK-TIM

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.273 OUT-OF-SYNC

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.274 PARAM-MISM

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.275 PEER-NORESPONSE

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

SDH Logical Object: EQPT

The switch agent raises a Peer Card Not Responding alarm if either traffic card in a protection group does not receive a response to the peer status request message. PEER-NORESPONSE is a software failure and occurs at the task level, as opposed to a communication failure, which is a hardware failure between peer cards.

Clear the PEER-NORESPONSE Alarm

Step 1 Complete the "Reset a Traffic Card in CTC" procedure on page 2-238 for the reporting card. For the LED behavior, see the "2.9.2 Typical Traffic Card LED Activity During Reset" section on page 2-228.

Step 2 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. Verify the LED appearance: A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

Step 3 If the alarm does not clear, log into the Cisco 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.

2.7.276 PORT-ADD-PWR-DEG-HI

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.277 PORT-ADD-PWR-DEG-LOW

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.278 PORT-ADD-PWR-FAIL-HI

The Add Port Power High Fail alarm is not used in this platform in this release. It is reserved for future development.

2.7.279 PORT-ADD-PWR-FAIL-LOW

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.280 PORT-FAIL

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.281 PORT-MISMATCH

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

SDH Logical Objects: CE-MR-10, ML-MR-10, FC_MR-4

The Pluggable PORT-MISMATCH alarm applies to FC_MR-4, ML-MR-10, and CE-MR-10 Ethernet cards.

For the ML-MR-10 and CE-MR-10 cards the alarm indicates either of the following:

- The provisioned payload, speed, or duplex configured on the port does not match that of the SFP plugged into the port.
- A non-supported SFP is plugged into the port.

For the FC_MR-4 card the alarm indicates that a non-supported GBIC is plugged into the port.

Clear the PORT-MISMATCH Alarm

To clear the alarm on the CE-MR-10 card, either plug-in a supported SFP into the CE-MR-10 port or follow these steps to provision the correct payload, speed, or duplex:

1. In node view (single-shelf mode) or shelf view (multishelf mode), double-click the CE-MR-10 card to open the card view.
2. Click the **Provisioning > Ether Ports** tabs.
3. Specify correct values in the Expected Speed and Expected Duplex fields to match the SFP configuration.
4. Click **Apply**.

To clear the alarm on the FC_MR-4 card, plug-in a supported GBIC into the FC_MR-4 port and follow these steps to provision the media type:

1. In node view (single-shelf mode) or shelf view (multishelf mode), double-click the FC_MR-4 card graphic to open the card.
2. Click the **Provisioning > Port > General** tabs.
3. Specify the proper payload value in the Media Type field.
4. Click **Apply**.

For the CE-MR-10 and FC_MR-10 card, the alarm can also be cleared using TL1 commands. For detailed instructions, refer to the *Cisco ONS 15454 SDH and Cisco ONS 15600 SDH TL1 Command Guide*.

For the ML-MR-10 card, the alarm can be cleared through Cisco IOS commands. For detailed instructions, refer to the *Cisco ONS 15454 and Cisco ONS 15454 SDH Ethernet Card Software Feature and Configuration Guide*.

If the alarm does not clear, log into the Cisco Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) to report a Service-Affecting (SA) problem.

2.7.282 PRC-DUPID

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

SDH Logical Object: STMN

The Procedural Error Duplicate Node ID alarm indicates that two identical node IDs exist in the same ring. The ONS 15454 SDH requires each node in the ring to have a unique node ID.

Clear the PRC-DUPID Alarm

Step 1 Log into a node on the ring.

Step 2 Complete the "Identify an MS-SPRing Ring Name or Node ID Number" procedure on page 2-229.

Step 3 Repeat Step 2 for all the nodes on the ring.

Step 4 If two nodes have an identical node ID number, complete the "Change an MS-SPRing Node ID Number" procedure on page 2-230 so that each node ID is unique.

Step 5 If the alarm does not clear, log into the Cisco 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.

2.7.283 PROTNA

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

SDH Logical Object: EQPT

The Protection Unit Not Available alarm is caused by a locked protection card when a TCC2/TCC2P card or cross-connect card that is provisioned as part of a protection group is not available. Unavailable protection can occur when a card is reset, but the alarm clears as soon as the card is back in service. The alarm clears if the device or facility is brought back in service.

Clear the PROTNA Alarm

Step 1 If the PROTNA alarm occurs and does not clear, and if the alarm is raised against a common control card (TCC2/TCC2P card), ensure that there is a redundant control card installed and provisioned in the chassis.

Step 2 If the alarm is raised against a line card, determine whether the ports have been taken out of service by completing the following steps:

a. In CTC, double-click the reporting card to display the card view (if the card is not a cross-connect card).

b. Click the **Provisioning > Line** tabs.

c. Click the **Admin State** column of any Unlocked ports. The port is out of service if the **Admin State** is locked,maintenance or locked,disabled.

Step 3 If any port is out of service, choose **Unlocked** to put the port in service.

Step 4 Complete the "Reset a Traffic Card in CTC" procedure on page 2-238 for the reporting card. For the LED behavior, see the "2.9.2 Typical Traffic Card LED Activity During Reset" section on page 2-228.

Step 5 Verify that the reset is complete and error-free. For LED appearance, see the "2.9 Traffic Card LED Activity" section on page 2-228.

Step 6 If the alarm does not clear, complete the "Remove and Reinsert (Reseat) Any Card" procedure on page 2-241 for the reporting card.

Step 7 If the alarm does not clear, log into the Cisco 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.

2.7.284 PROV-MISMATCH

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.285 PTIM

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.286 PWR-FAIL-A

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

SDH Logical Object: EQPT

The Equipment Power Failure at Connector A alarm occurs when there is no power supply from the main power connector to the equipment. This alarm occurs on the electrical interface assemblies (EIA), 15454_MRC-12 Multirate card, MRC-2.5G-12 Multirate card, OC192SR1/STM64IO Short Reach and OC192/STM64 Any Reach cards (also known as STM64-XFP in CTC), OC12 IR/STM4 SH 1310-4 card, OC3 IR/STM1 SH 1310-8 card or TCC2/TCC2P.

Warning **The power supply circuitry for the equipment can constitute an energy hazard. Before you install or replace the equipment, remove all jewelry (including rings, necklaces, and watches). Metal objects can come into contact with exposed power supply wiring or circuitry inside the DSLAM equipment. This could cause the metal objects to heat up and cause serious burns or weld the metal object to the equipment.** Statement 207

Clear the PWR-FAIL-A Alarm

Step 1 If a single card has reported the alarm, take the following actions depending on the reporting card:

- If the reporting card is an active traffic line port in a 1+1 protection group or is part of a path protection, ensure that an APS traffic switch has occurred to move traffic to the protect port.

  Note Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-230 for commonly used traffic-switching procedures.

- If the alarm is reported against a TCC2/TCC2P card, complete the "Reset an ActiveTCC2/TCC2P Card and Activate the Standby Card" procedure on page 2-239.
- If the alarm is reported against an STM-N card, complete the "Reset a Traffic Card in CTC" procedure on page 2-238.

Step 2 If the alarm does not clear, complete the "Remove and Reinsert (Reseat) Any Card" procedure on page 2-241.

Step 3 If the alarm does not clear, complete the "Physically Replace a Traffic Card" procedure on page 2-242 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 FMECS" chapter in the *Cisco ONS 15454 SDH Procedure 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.

Step 7 If the condition does not clear, log into the Cisco 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.

2.7.287 PWR-FAIL-B

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

SDH Logical Object: EQPT

The Equipment Power Failure at Connector B alarm occurs when there is no power supply from the main power connector to the equipment. This alarm occurs on the electrical interface assemblies (EIA), 15454_MRC-12 Multirate card, MRC-2.5G-12 Multirate card, OC192SR1/STM64IO Short Reach and OC192/STM64 Any Reach cards (also known as STM64-XFP in CTC), OC12 IR/STM4 SH 1310-4 card, OC3 IR/STM1 SH 1310-8 card or TCC2/TCC2P.

Warning **The power supply circuitry for the equipment can constitute an energy hazard. Before you install or replace the equipment, remove all jewelry (including rings, necklaces, and watches). Metal objects can come into contact with exposed power supply wiring or circuitry inside the DSLAM equipment. This could cause the metal objects to heat up and cause serious burns or weld the metal object to the equipment.** Statement 207

Clear the PWR-FAIL-B Alarm

Step 1 Complete the "Clear the PWR-FAIL-A Alarm" procedure on page 2-185.

Step 2 If the condition does not clear, log into the Cisco 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.

2.7.288 PWR-FAIL-RET-A

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

SDH Logical Object: EQPT

The Equipment Power Failure at Connector A alarm occurs when there is no power supplied to the backup power connector on the shelf. This alarm occurs on the electrical interface assemblies (EIA), 15454_MRC-12 Multirate card, MRC-2.5G-12 Multirate card, OC192SR1/STM64IO Short Reach and OC192/STM64 Any Reach cards (also known as STM64-XFP in CTC), OC12 IR/STM4 SH 1310-4 card, OC3 IR/STM1 SH 1310-8 card or TCC2/TCC2P.

Clear the PWR-FAIL-RET-A Alarm

Step 1 Complete the "Clear the PWR-FAIL-A Alarm" procedure on page 2-185.

Step 2 If the condition does not clear, log into the Cisco 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.

2.7.289 PWR-FAIL-RET-B

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

SDH 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), 15454_MRC-12 Multirate card, MRC-2.5G-12 Multirate card, OC192SR1/STM64IO Short Reach and OC192/STM64 Any Reach cards (also known as STM64-XFP in CTC), OC12 IR/STM4 SH 1310-4 card, OC3 IR/STM1 SH 1310-8 card or TCC2/TCC2P.

Clear the PWR-FAIL-RET-A Alarm

Step 1 Complete the "Clear the PWR-FAIL-A Alarm" procedure on page 2-185.

Step 2 If the condition does not clear, log into the Cisco 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.

2.7.290 RAI

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

SDH Logical Objects: DS1, E1

The Remote Alarm Indication (RAI) condition signifies an end-to-end electrical failure. The error condition is sent from one end of the SDH path to the other. RAI on the DS3i-N-12 card indicates that the far-end node is receiving a DS-3 AIS.

Clear the RAI Condition

Step 1 Complete the "Clear the AIS Condition" procedure on page 2-31.

Step 2 If the condition does not clear, log into the Cisco 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.

2.7.291 RCVR-MISS

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

SDH Logical Objects: DS1, E1

A Facility Termination Equipment Receiver Missing alarm occurs when the facility termination equipment detects an incorrect amount of impedance on its backplane connector. Incorrect impedance usually occurs when a receive cable is missing from the E-1 port or a possible mismatch of backplane equipment occurs, for example, an SMB connector or a BNC connector is connected to an E-1 card.

Note E-1s are four-wire circuits and need a positive (tip) and negative (ring) connection for both transmit and receive.

Clear the RCVR-MISS Alarm

Step 1 Ensure that the device attached to the E-1 port is operational.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454 SDH. Plug the wristband cable into the ESD jack located on the middle-right outside edge of the shelf assembly.

Step 2 If the attachment is good, verify that the cabling is securely connected.

Step 3 If the cabling is good, verify that the pinouts are correct.

Step 4 If the pinouts are correct, replace the receive cable.

Step 5 If the alarm does not clear, log into the Cisco 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.

2.7.292 RFI

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.293 RFI-V

The RFI-V condition is not used in this platform in this release. It is reserved for future development.

2.7.294 RING-ID-MIS

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

SDH Logical Object: STMN

DWDM Logical Object: OSC-RING

The Ring Name Mismatch condition refers to the ring OSC in APC. It occurs when a ring name does not match other detectable node ring names, and can cause problems with applications that require data exchange with APC. This alarm is somewhat similar to RING-MISMATCH, which applies to MS-SPRings, but instead of applying to ring protection, it applies to DWDM node discovery within the same network.

Note For more information about APC, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Clear the RING-ID-MIS Alarm

Step 1 Complete the "Clear the RING-MISMATCH Alarm" procedure on page 2-189.

Step 2 If the alarm does not clear, log into the Cisco 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.

2.7.295 RING-MISMATCH

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

SDH Logical Object: STMN

A Procedural Error Mismatched Ring alarm occurs when the ring name of the ONS 15454 SDH that is reporting the alarm does not match the ring name of another ONS node in the MS-SPRing. ONS nodes connected in an MS-SPRing must have identical ring names to function.

Note This alarm can also be expected when upgrading to Release 6.0 when the ring identifier is updated.

Clear the RING-MISMATCH Alarm

Step 1 Log into the first node in the ring.

Step 2 Verify the ring name. Complete the "Identify an MS-SPRing Ring Name or Node ID Number" procedure on page 2-229.

Step 3 Note the name in the Ring Name field.

Step 4 Log into the next ONS node in the MS-SPRing.

Step 5 Verify the ring name. Complete the "Identify an MS-SPRing Ring Name or Node ID Number" procedure on page 2-229.

Step 6 If the ring name matches the ring name in the reporting ONS node, repeat Step 5 for the next ONS node in the MS-SPRing.

Step 7 Complete the "Change an MS-SPRing Ring Name" procedure on page 2-229.

Step 8 Verify that the ring map is correct.

Step 9 If the alarm does not clear, log into the Cisco 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 to report a Service-Affecting (SA) problem.

2.7.296 RING-SW-EAST

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

SDH Logical Object: STMN

The Ring Switch Is Active East Side condition occurs when a ring switch occurs at the east side of a MS-SPRing using a Force Ring command. The condition clears when the switch is cleared. RING-SW-EAST is visible on the network view Alarms, Conditions, and History tabs. The port where the Force Ring was applied shows an "F" on the network view detailed circuit map.

Note RING-SW-EAST is an informational condition. The condition does not require troubleshooting.

2.7.297 RING-SW-WEST

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

SDH Logical Object: STMN

The Ring Switch Is Active West Side condition occurs when a ring switch occurs at the west side of a MS-SPRing using a Force Ring command. The condition clears when the switch is cleared. RING-SW-WEST is visible on the network view Alarms, Conditions, and History tabs. The port where the Force Ring was applied shows an "F" on the network view detailed circuit map.

Note RING-SW-WEST is an informational condition. The condition does not require troubleshooting.

2.7.298 ROLL

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

SDH Logical Objects: VCMON-HP, VCMON-LP, STSTRM, VCTERM-HP

The ROLL condition indicates that circuits are being rolled. This is typically carried out to move traffic for a maintenance operation or to perform bandwidth grooming. The condition indicates that a good signal has been received on the roll destination leg, but the roll origination leg has not yet been dropped. The condition clears when the roll origination leg is dropped.

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

2.7.299 ROLL-PEND

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

SDH Logical Objects: VCMON-HP, VCMON-LP, STSTRM, VCTERM-HP

ROLL-PEND indicates that a roll process has been started, but a good signal has not been received yet by the roll destination leg. This condition can be raised individually by each path in a bulk circuit roll.

The condition clears when a good signal has been received on the roll destination leg.

Note ROLL-PEND is an informational condition and does not require troubleshooting.

2.7.300 RPRW

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

SDH Logical Objects: ML100T, ML1000, MLFX

The Resilient Packet Ring (RPR) Wrapped condition applies to CE100T-8 and ML-Series cards and occurs when the RPR protocol initiates a ring wrap due to a fiber cut, node failure, node restoration, new node insertion, or other traffic problem. It can also be raised if the POS port is Admin down condition. (In this case, you will not see any SDH-level or TPTFAIL alarms.)

When the wrap occurs, traffic is redirected to the original destination by sending it in the opposite direction around the ring after a link state change or after receiving any SDH path-level alarms.

Clear the RPRW Condition

Step 1 Look for and clear any service-affecting SDH path-level alarms on the affected circuit, such as the "AU-LOP" alarm on page 2-43, "LOS (TRUNK)" alarm on page 2-149, or the "HP-TIM" alarm on page 2-122. Clearing this alarm can also clear RPRW.

Step 2 If the condition does not clear, look for and clear any service alarms for the ML-Series card itself, such as the "CARLOSS (CE100T)" alarm on page 2-53, "CARLOSS (ML100T, ML1000, MLFX)" alarm on page 2-60, "TPTFAIL (CE100T)" alarm on page 2-217, or the "TPTFAIL (ML100T, ML1000, MLFX)" alarm on page 2-219.

Step 3 If the condition does not clear, log into the Cisco 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.

2.7.301 RS-TIM

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

SDH 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.

A TIM is usually accompanied by other alarms, such as the "LOS (STM1E, STMN)" alarm on page 2-147. If so, reattach or replace the original cables/fibers to clear the alarms.

Clear the RS-TIM Alarm

Step 1 Complete the "Clear the TIM Alarm" procedure on page 2-216 for the J0 byte.

Step 2 If the alarm does not clear, log into the Cisco 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 problem.

2.7.302 RUNCFG-SAVENEED

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

SDH Logical Object: EQPT

The Run Configuration Save Needed condition occurs when you change the running configuration file for ML-Series cards. RUNCFG-SAVENEED is a reminder that you must save the change to the startup configuration file permanently.

The condition clears after you save the running configuration to the startup configuration, such as by entering:

```
copy run start
```

at the privileged EXEC mode of the Cisco IOS CLI. If you do not save the change, the change is lost after the card reboots. If the command "copy run start" is executed in configuration mode and not privileged EXEC mode, the running configuration will be saved, but the alarm will not clear

Note For more information about the ML-Series Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.*

2.7.303 SD (DS1, DS3, E1, E3, E4, STM1E, STMN)

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

SDH Logical Objects: DS1, DS3, E1, E3, E4, STM1E, STMN

A Signal Degrade (SD) condition occurs on optical STM-N lines and the low-order path termination when the quality of the signal is so poor that the BER on the incoming optical line passed the signal degrade threshold. Signal degrade is defined by the ITU as a "soft failure" condition. SD and SF both monitor the incoming BER and are similar, but SD is triggered at a lower bit error rate than SF.

An SD condition occurs for STM-N cards and the low-order path termination when the BER on the incoming optical line has passed the signal failure threshold in the range of 1E–9 dBm to 1E–5 dBm. For unprotected circuits, the BER threshold value is not user-provisionable and the error rate is set to a Telcordia GR-253-CORE specification of 1E–6 dBm.

The SD condition travels on the B2 byte of the multiplexing section SDH overhead. The condition clears when the BER level falls to one-tenth of the threshold level that triggered the condition. 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. SD can also be caused by repeated cross-connect card switches that in turn can cause switching on the lines or paths.

Warning **On the OC192 LR/STM64 LH 1550 card, the laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. The laser is off when the safety key is off (labeled 0).** Statement 293

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

Warning **Use of controls, adjustments, or performing procedures other than those specified could result in hazardous radiation exposure.** Statement 1057

Note Some levels of BER errors (such as 1E–9 dBm) take a long period to raise or clear, about 9,000 seconds, or 150 minutes. If the SD threshold is provisioned at 1E–9 dBm rate, the SD alarm requires at least one and one-half hours to raise and then another period at least as long to clear.

Note The recommended test set for use on all SDH ONS electrical cards (except E1 cards) is the Omniber 718. The FireBerd test set is recommended for testing E1 cards.

Clear the SD (DS3, E1, E3, E4, STM1E, STM-N) Condition

Step 1 Verify that the user-provisionable BER threshold is set at the expected level. Complete the "Clear an STM-N Card Facility or Terminal Loopback Circuit" procedure on page 2-244 or "Clear a Non-STM Card Facility or Terminal Loopback Circuit" procedure on page 2-245, as required.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454 SDH. Plug the wristband cable into the ESD jack located on the middle-right outside edge of the shelf assembly.

Step 2 With an optical test set, measure the power level of the line to ensure that the power is within guidelines. For specific procedures to use the test set equipment, consult the manufacturer.

Step 3 Verify that optical receive levels are within the acceptable range. These are listed in the "1.12.3 Optical Card Transmit and Receive Levels" section on page 1-135.

Step 4 If the receive levels are out of range, clean the fiber according to site practice. If no site practice exists, complete the procedure for cleaning optical connectors in the "Maintain the Node" chapter of the *Cisco ONS 15454 SDH Procedure Guide*.

Step 5 Verify that single-mode fiber is used.

Step 6 Verify that a single-mode laser is used at the far-end node.

Step 7 If the problem persists, the transmitter at the other end of the optical line could be failing and require replacement.

Step 8 If the condition does not clear, log into the Cisco 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.

2.7.304 SD (TRUNK)

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.305 SDBER-EXCEED-HO

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

SDH Logical Objects: 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

Step 1 Determine the BER threshold. Complete the "Clear an STM-N Card Facility or Terminal Loopback Circuit" procedure on page 2-244.

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 *Cisco ONS 15454 SDH Procedure Guide*.

If the condition does not clear, log into the Cisco 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. If the condition applies to VCMON-HP, it is Service-Affecting (SA).

2.7.306 SDBER-EXCEED-LO

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

SDH Logical Objects: VCMON-LP, VCTRM-LP

The Signal Degrade Threshold Exceeded for Low Order condition indicates that the signal degrade BER threshold has been exceeded for a low-order (VC-4) path on optical (traffic) cards. SDBER-EXCEED-LO 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-LO Condition

Step 1 Determine the BER threshold. Complete the "Clear an STM-N Card Facility or Terminal Loopback Circuit" procedure on page 2-244.

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 *Cisco ONS 15454 SDH Procedure Guide*.

If the condition does not clear, log into the Cisco 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. If the condition applies to VCMON-HP, it is Service-Affecting (SA).

2.7.307 SD-L

The Signal Degrade Line alarm is not used in this platform for this release. It is reserved for future development.

2.7.308 SF (DS1, DS3, E1, E3, E4, STMN)

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

SDH Logical Objects: DS1, DS3, E1, E3, E4, STMN

A Signal Failure (SF) condition occurs on optical STM-N cards and the low-order path termination when the BER on the incoming optical line has passed the signal failure threshold in the range of 1E–5 dBm to 1E–3 dBm. The condition travels on the B2 byte of the multiplexing section SDH overhead; this condition causes a protection switch at the line (facility) level.

The SF 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.

Signal failure is defined by the ITU as a "hard failure" condition. SD and SF both monitor the incoming BER error rate and are similar, but SF is triggered at a higher BER than SD.

Warning **On the OC192 LR/STM64 LH 1550 card, the laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. The laser is off when the safety key is off (labeled 0).** Statement 293

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

Warning **Use of controls, adjustments, or performing procedures other than those specified could result in hazardous radiation exposure.** Statement 1057

Clear the SF (DS3, E1, E3, E4, STMN) Condition

Step 1 Verify that the user-provisionable BER threshold is set at the expected level. Complete the "Clear an STM-N Card Facility or Terminal Loopback Circuit" procedure on page 2-244.

Step 2 Using an optical test set, measure the 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.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454 SDH. Plug the wristband cable into the ESD jack located on the middle-right outside edge of the shelf assembly.

Step 3 Verify that the optical receive levels are within the acceptable range.

Step 4 Clean the fibers at both ends according to site practice for a line signal failure. If no site practice exists, complete the procedure for cleaning optical connectors in the "Maintain the Node" chapter of the *Cisco ONS 15454 SDH Procedure Guide*.

Step 5 Verify that single-mode fiber is being used.

Step 6 If the problem persists, the transmitter at the other end of the optical line could be failing and need replacement.

Step 7 If the condition does not clear, log into the Cisco 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.

2.7.309 SF (TRUNK)

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.310 SFBER-EXCEED-HO

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

SDH Logical Objects: VCMON-HP, VCTRM-HP

The Signal Failure Threshold Exceeded for High Order condition occurs when the signal fail BER threshold has been exceeded for a high-order (VC-4 or VC-3) path on optical (traffic) cards. SFBER-EXCEED-HO occurs when the signal BER falls past the fail threshold (typically 1E-4 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 SFBER-EXCEED-HO Condition

Step 1 Determine the BER threshold by clicking the card reporting the condition, and clicking the **Provisioning** tab.

Step 2 If adjustment is acceptable in site practices, adjust the threshold.

Step 3 Verify the input power levels to the reporting card.

Step 4 Verify input fiber cable connections to the reporting card.

Step 5 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 *Cisco ONS 15454 SDH Procedure Guide*.

If the condition does not clear, log into the Cisco 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. If the condition applies to the VCTRM-HP object, it is Service-Affecting (SA).

2.7.311 SFBER-EXCEED-LO

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

SDH Logical Objects: VCMON-LP, VCTRM-LP

The Signal Failure Threshold Exceeded for High Order condition occurs when the signal fail BER threshold has been exceeded for a high-order (VC-4 or VC-3) path on optical (traffic) cards. SFBER-EXCEED-HO occurs when the signal BER falls past the fail threshold (typically 1E-4 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 SFBER-EXCEED-HO Condition

Step 1 Determine the BER threshold by clicking the card reporting the condition, and clicking the **Provisioning** tab.

Step 2 If adjustment is acceptable in site practices, adjust the threshold.

Step 3 Verify the input power levels to the reporting card.

Step 4 Verify input fiber cable connections to the reporting card.

Step 5 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 *Cisco ONS 15454 SDH Procedure Guide*.

If the condition does not clear, log into the Cisco 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. If the condition applies to the VCTRM-HP object, it is Service-Affecting (SA).

2.7.312 SF-L

The Signal Fail Line alarm is not used in this platform for this release. It is reserved for future development.

2.7.313 SFTWDOWN

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

SDH Logical Object: EQPT

A Software Download in Progress alarm occurs when the TCC2/TCC2P card is downloading or transferring software.

No action is necessary. Wait for the transfer or the software download to complete. If the condition does not clear, log into the Cisco 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.

Caution Updating software on a standby TCC2/TCC2P card can take up to 30 minutes. Wait the full time period before removing the card. Premature removal can cause flash corruption.

Note SFTWDOWN is an informational alarm and does not require troubleshooting.

2.7.314 SH-INS-LOSS-VAR-DEG-HIGH

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.315 SH-INS-LOSS-VAR-DEG-LOW

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.316 SHUTTER-OPEN

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.317 SIGLOSS

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

SDH Logical Object: FCMR

DWDM Logical Objects: FC, GE, ISC, TRUNK

The Signal Loss on Data Interface alarm is raised on FC_MR-4 card receive client ports and MXP card FC and ISC client data ports when there is a loss of signal. (Loss of Gigabit Ethernet client signal results in a CARLOSS [GE], not SIGLOSS.) SIGLOSS can also be raised on the MXP trunk port.

If the SYNCLOSS alarm was previously raised on the port, the SIGLOSS alarm will demote it.

Clear the SIGLOSS Alarm

Step 1 Ensure that the port connection at the near end of the SDH link is operational.

Step 2 Verify fiber continuity to the port. To verify fiber continuity, follow site practices.

Step 3 Check the physical port LED on the card. The port LED looks clear (that is, not lit green) if the link is not connected.

Step 4 If the alarm does not clear, log into the Cisco 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 problem.

2.7.318 SNTP-HOST

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

SDH Logical Object: NE

The Simple Network Time Protocol (SNTP) host failure alarm indicates that an ONS node serving as an IP proxy for the other ONS nodes in the ring is not forwarding SNTP information to the other ONS nodes in the network. The host failure can result from two causes: the IP network attached to the ONS proxy node is experiencing problems, or the ONS proxy node itself is not functioning properly.

Clear the SNTP-HOST Alarm

Step 1 Ping the SNTP host from a workstation in the same subnet to ensure that communication is possible within the subnet by completing the procedure in the "1.9.8 Verify PC Connection to the ONS 15454 SDH (ping)" section on page 1-109.

Step 2 If the ping fails, contact the network administrator that manages the IP network that supplies the SNTP information to the proxy and determine whether the network is experiencing problems which could affect the SNTP server/router connecting to the proxy ONS 15454 SDH.

Step 3 Ensure that the ONS 15454 SDH is provisioned correctly by completing the following steps:

a. In node view of the ONS node serving as the proxy, click the **Provisioning > General** tabs.

b. Ensure that the Use NTP/SNTP Server check box is checked.

c. If the **Use NTP/SNTP Server** check box is not checked, check it.

d. Ensure that the correct server name is entered in the NTP/SNTP Server field.

Step 4 If the alarm does not clear, log into the Cisco 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.

2.7.319 SPAN-SW-EAST

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

SDH Logical Object: STMN

The Span Switch Is Active East Side condition occurs when a span switch occurs at the east side of a four-fiber MS-SPRing span using a Force Span command. The condition clears when the switch is cleared. SPAN-SW-EAST is visible on the network view Alarms, Conditions, and History tabs. The port where the Force Span was applied shows an "F" on the network view detailed circuit map.

Note SPAN-SW-EAST is an informational condition. The condition does not require troubleshooting.

2.7.320 SPAN-SW-WEST

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

SDH Logical Object: STMN

The Span Switch Is Active West Side condition occurs when a span switch occurs at the west side of a four-fiber MS-SPRing span using a Force Span command. The condition clears when the switch is cleared. SPAN-SW-WEST is visible on the network view Alarms, Conditions, and History tabs. The port where the Force Span was applied shows an "F" on the network view detailed circuit map.

Note SPAN-SW-WEST is an informational condition. The condition does not require troubleshooting.

2.7.321 SQUELCH

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

SDH Logical Object: STMN

The Ring Squelching Traffic condition occurs in an MS-SPRing when a node that originates or terminates VC circuits fails or is isolated by multiple fiber cuts or maintenance FORCE RING commands. The isolation or failure of the node disables the circuits that originate or terminate on the failed node. Squelch conditions appear on one or both of the nodes on either side of the isolated/failed node. The AU-AIS condition also appears on all nodes in the ring, except the isolated node.

Warning **On the OC192 LR/STM64 LH 1550 card, the laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. The laser is off when the safety key is off (labeled 0).** Statement 293.

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

Warning **Use of controls, adjustments, or performing procedures other than those specified could result in hazardous radiation exposure.** Statement 1057

Clear the SQUELCH Condition

Step 1 Determine the isolated node by completing the following steps:

a. In node view, click **View > Go to Network View**.

b. The grayed out node with red spans is the isolated node.

Step 2 Verify fiber continuity to the ports on the isolated node. To verify fiber continuity, follow site practices.

Step 3 If fiber continuity is good, verify that the proper ports are 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 STM-N port is in service, double-click the card in CTC to display the card view.

c. Click the **Provisioning > Line** tabs.

d. Verify that the **Admin State** column lists the port as **Unlocked**.

e. If the **Admin State** column lists the port as locked,maintenance or locked,disabled, click the column and choose **Unlocked**. Click **Apply**.

Step 4 If the correct ports are in service, use an optical test set to verify that a valid signal exists on the line.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454 SDH. Plug the wristband cable into the ESD jack located on the middle-right outside edge of the shelf assembly.

For specific procedures to use the test set equipment, consult the manufacturer. Test the line as close to the receiving card as possible.

Step 5 If the signal is valid, verify that the power level of the optical signal is within the optical card receiver specifications. Refer to the *Cisco ONS 15454 SDH Reference Manual* for card specifications.

Step 6 If the receiver levels are acceptable, ensure that the optical transmit and receive fibers are connected properly.

Step 7 If the connectors are acceptable, complete the "Physically Replace a Traffic Card" procedure on page 2-242 for the STM-N card.

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. See the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-230 for commonly used traffic-switching procedures.

Note When you replace a card with the identical type of card, you do not need to make any changes to the database.

Step 8 If the condition does not clear, log into the Cisco 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.

2.7.322 SQUELCHED

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

SDH Logical Object: STMN

DWDM Logical Objects: 2R, ESCON, FC, GE, ISC, TRUNK

The Client Signal Squelched condition is raised by a TXP_MR_10G, TXP_MR_10E, TXP_MR_2.5G, TXPP_MR_2.5G, MXP_2.5G_10G, MXP_2.5G_10E, MXP_MR_2.5G, or MXPP_MR_2.6G card.

The condition can be raised in the following situations:

- An MXP or TXP client facility detects that an upstream receive facility has experienced a loss of signal (such as an Ethernet CARLOSS, DWDM SIGLOSS, or optical LOS). In response, the facility's transmit is turned off (SQUELCHED). The upstream receive facilities are the trunk receive on the same card as the client, as well as the client receive on the card at the other end of the trunk span.
- The client will squelch if the upstream trunk receive (on the same card) experiences a SIGLOSS, Ethernet CARLOSS, LOS, or LOS (TRUNK) alarm. In some transparent modes, the client is squelched if the trunk detects an AIS condition or a TIM alarm.

- The client will squelch if the upstream client receive (on the card at the other end of the DWDM span) experiences CARLOSS, SIGLOSS, or LOS.

In an example situation, an upstream MXP_2.5G_10G client port receive experiences a "loss of light," and this port raises CARLOSS, SIGLOSS, or LOS (determined by the payload type) locally. The port also sends client signal fail (GFP-CSF) to its downstream card. The downstream card raises a GFP-CSF alarm, turns off the client transmit laser, and raises the SQUELCHED condition.

The local client raises SQUELCHED if it also raises one of the following alarms, all of which are signalled by the upstream node:

- "GFP-CSF" alarm on page 2-110 for the client
- "GFP-LFD" alarm on page 2-112 for the client
- "GFP-NO-BUFFERS" alarm on page 2-112 for the client
- "GFP-DE-MISMATCH" alarm on page 2-110 for the client
- "GFP-EX-MISMATCH" alarm on page 2-111 for the client
- "ODUK-1-AIS-PM" alarm on page 2-177 for the client
- "ODUK-2-AIS-PM" alarm on page 2-177 for the client
- "ODUK-3-AIS-PM" alarm on page 2-177 for the client
- "ODUK-4-AIS-PM" alarm on page 2-177 for the client

On the MXP_MR_10G, the local client raises SQUELCHED if the upstream client detects one of the following alarms. Note that no corresponding local alarm is raised to indicate which of these conditions is present upstream.

- LOS for the clients including the "LOS (2R)" alarm on page 2-142, "LOS (ESCON)" alarm on page 2-146, and "LOS (ISC)" alarm on page 2-147
- CARLOSS for the clients including the "CARLOSS (FC)" alarm on page 2-57, "CARLOSS (GE)" alarm on page 2-60, and "CARLOSS (ISC)" alarm on page 2-60

The local client raises SQUELCHED if the local trunk raises one of the following alarms:

- "OTUK-LOF" alarm on page 2-180 for the trunk
- "OTUK-AIS" alarm on page 2-180 for the trunk
- "LOS (TRUNK)" alarm on page 2-149
- "OTUK-TIM" alarm on page 2-180 squelching enabled, for the trunk
- "ODUK-AIS-PM" alarm on page 2-178 for the trunk
- "ODUK-LCK-PM" alarm on page 2-178 for the trunk
- "ODUK-TIM-PM" alarm on page 2-178 with squelching enabled, for the trunk
- "TIM" alarm on page 2-216 with squelching enabled, for STM-N
- "LOF (DS1, DS3, E1, E4, STM1E, STMN)" alarm on page 2-138
- "LOS (STM1E, STMN)" alarm on page 2-147
- "CARLOSS (TRUNK)" alarm on page 2-61
- "WVL-MISMATCH" alarm on page 2-227 for the client or trunk

When troubleshooting the SQUELCHED condition locally, look for failures progressing upstream in the following order. (If you are troubleshooting this alarm remotely, reverse the order of progress.)

- Local client alarms, as above

- Local trunk alarms, as above
- Remote (upstream) client receive alarms, as above

Note Note: If you see a SQUELCHED condition on the trunk, this can only be caused by a transponder (TXP) card.

Clear the SQUELCHED Condition

Step 1 If the object is reported against any object besides ESCON, determine whether the remote node and local node reports and LOF or the LOS alarm (for the client trunk, as listed above). 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 above has occurred. If so, turn to the relevant section of this chapter and complete the troubleshooting procedure.

Step 3 If none of these alarms is reported, determine whether the local port reporting the SQUELCHED condition is in loopback. (You will see LPBKFACILITY OR LPBKTERMINAL in the condition window for this port.) If it is in loopback, complete the following steps:

a. Double-click the client card to display the card view.

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

c. If the port Admin State column says locked, maintenance or locked, disabled, click the cell to highlight it and choose **Unlocked** from the drop-down list. Changing the state to Unlocked also clears any loopback provisioned on the port.

Step 4 If the condition does not clear, log into the Cisco 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.

2.7.323 SQM

Default Severity: Critical (CR), Service-Affecting (SA) for VCTRM-HP; Major (MJ), Service-Affecting (SA) for VCTRM-LP

SDH Logical Objects: VCTRM-HP, VCTRM-LP

The Sequence Mismatch alarm is a VCAT member alarm. (VCAT member circuits are independent circuits that are concatenated from different time slots into a higher-rate signal.) The alarm occurs when the expected sequence numbers of VCAT members do not match the received sequence numbers.

Clear the SQM Alarm

Step 1 For the errored circuit, complete the "Delete a Circuit" procedure on page 2-243.

Step 2 Recreate the circuit using the procedure in the "Create Circuits and VT Tunnels" chapter of the *Cisco ONS 15454 SDH Procedure Guide*.

Step 3 If the alarm does not clear, log into the Cisco 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.

2.7.324 SSM-DUS

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

SDH Logical Objects: BITS, E1, STMN

DWDM Logical Object: TRUNK

The Synchronization Status Messaging (SSM) Quality level Changed to Do Not Use (DUS) occurs 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. SSM-DUS can also be sent for line maintenance testing.

Note SSM-DUS is an informational condition alarm. The condition does not require troubleshooting.

2.7.325 SSM-FAIL

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

SDH Logical Objects: BITS, E1

DWDM Logical Object: TRUNK

The SSM Failed BITS or STM-N alarm occurs when the SSM byte (S1 byte) of the SDH overhead multiplexing section received by the ONS 15454 SDH has failed. The problem is external to the ONS 15454 SDH.This alarm indicates that although the ONS 15454 SDH is set up to receive SSM, the timing source is not delivering valid SSM messages.

Clear the SSM-FAIL Alarm

Step 1 Verify that SSM is enabled on the external timing source.

Step 2 Use an optical test set to determine that the external timing source is delivering the SSM (S1) byte. For specific procedures to use the test set equipment, consult the manufacturer.

Step 3 If the alarm does not clear, log into the Cisco 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.

2.7.326 SSM-LNC

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

SDH Logical Objects: BITS, NE-SREF, STMN

DWDM Logical Object: TRUNK

The SSM Local Node Clock (LNC) Traceable condition occurs when the SSM (S1) byte of the SDH overhead multiplexing section has been changed to signify that the line or BITS timing source SSM quality level is G812L.

Note SSM-LNC is an informational condition. The condition does not require troubleshooting.

2.7.327 SSM-OFF

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

SDH Logical Objects: BITS, E1

DWDM Logical Object: TRUNK

The SSM Off BITS or STM-N condition applies to references used for timing the node. SSM-OFF occurs when the SSM (S1) byte of the SDH overhead multiplexing section for this reference has been turned off. The ONS 15454 SDH is set up to receive SSM, but the timing source is not delivering SSM messages.

SSM is an SDH protocol that communicates information about the quality of the timing source. SSM messages are carried on the S1 byte of the SDH multiplex section overhead. They enable SDH devices to automatically select the highest quality timing reference and to avoid timing loops.

To clear the condition, complete the "Clear the SSM-FAIL Alarm" procedure on page 2-206. If the condition does not clear, log into the Cisco 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.

2.7.328 SSM-PRC

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

SDH Logical Objects: BITS, NE-SREF, STMN

DWDM Logical Object: TRUNK

The SSM Primary Reference Clock (PRC) Traceable condition occurs when the SDH overhead multiplexing section S1 byte indicates that the line or BITS timing source SSM quality level is G811.

Note SSM-PRC is an informational condition. The condition does not require troubleshooting.

2.7.329 SSM-PRS

The SSM Primary Reference Source (PRS) Traceable condition is not used in this platform in this release. It is reserved for future development.

2.7.330 SSM-RES

The SSM Reserved (RES) For Network Synchronization Use condition is not used in this platform in this release. It is reserved for future development.

2.7.331 SSM-SDH-TN

The SSM-SDH-TN condition is not used in this platform in this release. It is reserved for future development.

2.7.332 SSM-SETS

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

SDH Logical Objects: BITS, NE-SREF, STMN

DWDM Logical Object: TRUNK

The SSM Synchronous Equipment Timing Source (SETS) Traceable condition occurs when the SSM (S1) byte indicates that the line or BITS timing source has changed to SETS.

Note SSM-SETS is an informational condition. The condition does not require troubleshooting.

2.7.333 SSM-SMC

The SSM SDH Minimum Clock (SMC) Traceable condition is not used in this platform in this release. It is reserved for future development.

2.7.334 SSM-ST2

The SSM Stratum 2 (ST2) Traceable condition is not used in this platform in this release. It is reserved for future development.

2.7.335 SSM-ST3

The SSM Stratum 3 (ST3) Traceable condition is not used in this platform in this release. It is reserved for future development.

2.7.336 SSM-ST3E

The SSM Stratum 3E (ST3E) Traceable condition is not used in this platform in this release. It is reserved for future development.

2.7.337 SSM-ST4

The SSM Stratum 4 (ST4) Traceable condition is not used in this platform in this release. It is reserved for future development.

2.7.338 SSM-STU

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

SDH Logical Objects: BITS, E1, NE-SREF, STMN

DWDM Logical Object: TRUNK

The SSM Synchronization Traceability Unknown (STU) BITS or STM-N condition occurs when the reporting node is timed to a reference that does not report the SSM S1 byte, but the ONS 15454 SDH has SSM support enabled. STU also occurs if the timing source is sending out SSM messages but SSM is not enabled on the ONS 15454 SDH.

Clear the SSM-STU Condition

Step 1 Click the **Provisioning > Timing > BITS Facilities** tabs.

Step 2 Complete one of the following depending upon the status of the Sync Messaging Enabled check box:

- If the **Sync. Messaging Enabled** check box for the BITS source is checked, uncheck the box.
- If the **Sync. Messaging Enabled** check box for the BITS source is not checked, check the box.

Step 3 Click **Apply**.

Step 4 If the condition does not clear, log into the Cisco 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.

2.7.339 SSM-TNC

For information about this alarm or condition, refer to the “Alarm Troubleshooting” chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.340 SW-MISMATCH

The SW-MISMATCH condition is not used in this platform in this release. It is reserved for future development.

2.7.341 SWMTXMOD-PROT

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

SDH Logical Object: EQPT

The Switching Matrix Module Failure on Protect Slot alarm is raised by the Slot 10 cross connect card if this card is active (ACT). Any kind of cross-connect card can raise this alarm. (Two exceptions are given in the following paragraph.) SWMTXMOD-PROT occurs when a logic component internal to the Slot 10 cross connect is out of frame (OOF) with a traffic card in the system. In this case, the alarm is raised against the traffic card slot.

The XC-VXC cross-connect card can raise this alarm (in Slot 10) whether it is ACT or standby (SBY). The XCVXL card can raise SWMTXMOD-PROT against itself if the cross-connect card is OOF with a second logic component on the same cross connect card.

Clear the SWMTXMOD-PROT Alarm

Step 1 Complete the "Reset a Traffic Card in CTC" procedure on page 2-238 for the Slot 10 card. For the LED behavior, see the "2.9.2 Typical Traffic Card LED Activity During Reset" section on page 2-228.

Step 2 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

Step 3 If the alarm does not clear, complete the "Remove and Reinsert (Reseat) Any Card" procedure on page 2-241 for the Slot 10 cross-connect card.

Step 4 Complete the "Side Switch the Active and Standby Cross-Connect Cards" procedure on page 2-240.

Note After the active cross-connect card goes into standby mode, the original standby slot becomes active. The former standby card ACT/SBY LED becomes green.

Step 5 If the alarm does not clear, log into the Cisco 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.

2.7.342 SWMTXMOD-WORK

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

SDH Logical Object: EQPT

The Switching Matrix Module Failure on Working Slot alarm is raised by the Slot 8 cross connect card if this card is active (ACT). Any kind of cross-connect card can raise this alarm. (Two exceptions are given in the following paragraph.) SWMTXMOD-WORK occurs when a logic component internal to the Slot 8 cross connect is OOF with a traffic card in the system. In this case, the alarm is raised against the traffic card slot.

The XCVXC cross-connect card can raise this alarm (in Slot 8) whether it is ACT or standby (SBY). The XCVT card can raise SWMTXMOD-WORK against itself if the cross-connect card is OOF with a second logic component on the same cross connect card.

Clear the SWMTXMOD-WORK Alarm

Step 1 Complete the "Reset a Traffic Card in CTC" procedure on page 2-238 for the Slot 8 card. For the LED behavior, see the "2.9.2 Typical Traffic Card LED Activity During Reset" section on page 2-228.

Step 2 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

Step 3 If the alarm does not clear, complete the "Remove and Reinsert (Reseat) Any Card" procedure on page 2-241 for the Slot 8 cross-connect card.

Step 4 Complete the "Side Switch the Active and Standby Cross-Connect Cards" procedure on page 2-240.

Note After the active cross-connect card goes into standby mode, the original standby slot becomes active. The former standby card ACT/SBY LED becomes green.

Step 5 If the alarm does not clear, log into the Cisco 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.

2.7.343 SWTOPRI

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

SDH Logical Objects: EXT-SREF, NE-SREF

The Synchronization Switch to Primary Reference condition occurs when the ONS 15454 SDH switches to the primary timing source (reference 1). The ONS 15454 SDH 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. The condition does not require troubleshooting.

2.7.344 SWTOSEC

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

SDH Logical Objects: EXT-SREF, NE-SREF

The Synchronization Switch to Secondary Reference condition occurs when the ONS 15454 SDH has switched to a secondary timing source (reference 2).

To clear the condition, clear alarms related to failures of the primary source, such as the "SYNCPRI" alarm on page 2-213. If the condition 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.

2.7.345 SWTOTHIRD

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

SDH Logical Objects: EXT-SREF, NE-SREF

The Synchronization Switch to Third Reference condition occurs when the ONS 15454 SDH has switched to a third timing source (reference 3).

To clear the condition, clear alarms related to failures of the primary source, such as the "SYNCPRI" alarm on page 2-213 and the "SYSBOOT" alarm on page 2-215. If the condition does not clear, log into the Cisco 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.

2.7.346 SYNC-FREQ

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

SDH Logical Objects: E1, STMN

SDH 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 NE fails this reference and chooses another reference or internal to run on.

Clear the SYNC-FREQ Condition

Step 1 Use an optical test set to verify the timing frequency of the line or BITS timing source and ensure that that timing 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 out of bounds, replace the TCC2/TCC2P card. Complete the "Physically Replace a Traffic Card" procedure on page 2-242.

Step 3 If the SYNC-FREQ condition continues to report after replacing the TCC2/TCC2P card, log into the Cisco 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.

2.7.347 SYNCLOSS

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

SDH Logical Object: FCMR

DWDM Logical Objects: FC, GE, ISC, TRUNK

The Loss of Synchronization on Data Interface alarm is raised on FC_MR-4 client ports and MXP cards client or trunk ports when there is a loss of signal synchronization on the port. This alarm is demoted by the SIGLOSS alarm.

Clear the SYNCLOSS Alarm

Step 1 Ensure that the data port connection at the near end of the SDH 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 illuminated green), the link is not connected and the alarm has not cleared.
- If the LED is red, this indicates that the fiber is pulled.

Step 4 If the SYNCLOSS 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.

2.7.348 SYNCPRI

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

SDH Logical Objects: EXT-SREF, NE-SREF

A Loss of Timing on Primary Reference alarm occurs when the ONS 15454 SDH loses the primary timing source (reference 1). The ONS 15454 SDH uses three ranked timing references. The timing references are typically two BITS-level or line-level sources and an internal reference. If SYNCPRI occurs, the ONS 15454 SDH should switch to its secondary timing source (reference 2). The timing switch also triggers the "SWTOSEC" condition on page 2-211.

Clear the SYNCPRI Alarm

Step 1 In node view, click the **Provisioning > Timing > General** tabs.

Step 2 Verify the current configuration for REF-1 of the NE reference.

Step 3 If the primary reference is a BITS input, verify the wiring connection from the ONS 15454 SDH backplane BITS clock pin fields to the timing source.

Step 4 Verify that the BITS clock is operating properly.

Step 5 If the primary reference clock is an incoming port on the ONS 15454 SDH, complete the "2.7.172 LOF (TRUNK)" procedure on page 2-139.

Step 6 If the alarm does not clear, log into the Cisco 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.

2.7.349 SYNCSEC

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

SDH Logical Objects: EXT-SREF, NE-SREF

A Loss of Timing on Secondary Reference alarm occurs when the ONS 15454 SDH loses the secondary timing source (reference 2). If SYNCSEC occurs, the ONS 15454 SDH should switch to a third timing source (reference 3) to obtain valid timing for the ONS 15454 SDH. The timing switch also triggers the "SWTOTHIRD" condition on page 2-212.

Clear the SYNCSEC Alarm

Step 1 In node view, click the **Provisioning > Timing > General** tabs.

Step 2 Verify the current configuration of REF-2 for the NE Reference.

Step 3 If the secondary reference is a BITS input, verify the wiring connection from the ONS 15454 SDH backplane BITS clock pin fields to the timing source.

Step 4 Verify that the BITS clock is operating properly.

Step 5 If the secondary timing source is an incoming port on the ONS 15454 SDH, complete the "Clear the LOS (BITS) Alarm" procedure on page 2-143.

Step 6 If the alarm does not clear, log into the Cisco 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.

2.7.350 SYNCTHIRD

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

SDH Logical Objects: EXT-SREF, NE-SREF

A Loss of Timing on Third Reference alarm occurs when the ONS 15454 SDH loses the third timing source (reference 3). If SYNCTHIRD occurs and the ONS 15454 SDH uses an internal reference for source three, then the TCC2/TCC2P card could have failed. The ONS 15454 SDH often reports either the "FRNGSYNC" condition on page 2-107 or the "HLDOVRSYNC" condition on page 2-119 after a SYNCTHIRD alarm.

Clear the SYNCTHIRD Alarm

Step 1 In node view, click the **Provisioning > Timing > General** tabs.

Step 2 Verify that the current configuration of REF-3 for the NE Reference. For more information about timing references, refer to the "Timing" chapter in the *Cisco ONS 15454 SDH Reference Manual*.

Step 3 If the third timing source is a BITS input, complete the "Clear the LOS (BITS) Alarm" procedure on page 2-143.

Step 4 If the third timing source is an incoming port on the ONS 15454 SDH, complete the "Clear the LOS (STM1E, STMN) Alarm" procedure on page 2-148.

Step 5 If the third timing source uses the internal ONS system timing, complete the "Reset an ActiveTCC2/TCC2P Card and Activate the Standby Card" procedure on page 2-239.

Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card.

Step 6 If the alarm does not clear, log into the Cisco 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.

2.7.351 SYSBOOT

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

SDH Logical Object: NE

The System Reboot alarm indicates that new software is booting on the TCC2/TCC2P card. SYSBOOT is an informational alarm.

No action is required. The alarm clears when all cards finish rebooting the new software. The reboot takes up to 30 minutes. If the alarm does not clear, log into the Cisco 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.

Note SYSBOOT is an informational alarm. It only requires troubleshooting if it does not clear.

2.7.352 TEMP-MISM

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

SDH Logical Object: NE

Temperature Reading Mismatch Between Control Cards is raised when the temperature reading on the two TCC2/TCC2P 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 TCC2/TCC2P cards, allowing the values to be compared. The temperature of each TCC2/TCC2P 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

Step 1 Complete the "Inspect, Clean, and Replace the Reusable Air Filter" procedure on page 2-245.

Step 2 If the condition does not clear, complete the "Remove and Reinsert a Fan-Tray Assembly" procedure on page 2-246.

Step 3 If this alarm does not clear, log into the Cisco 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.

2.7.353 TIM

Default Severity: Major (MJ), Service-Affecting (SA) for STM1E; Critical (CR), Service-Affecting (SA) for STMN, TRUNK

SDH Logical Objects: STM1E, STMN

SDH Logical Object: TRUNK

The Section TIM alarm occurs when the expected J0 section trace string does not match the received section trace string. This occurs because the data being received is not correct, and the receiving port could not be connected to the correct transmitter port.

If the alarm occurs on a port that has been operating with no alarms, the circuit path has changed due to a fibering misconnection, a TL1 routing change, or to someone entering an incorrect value in the Current Transmit String field.

TIM occurs on a port that has previously been operating without alarms if someone switches optical fibers that connect the ports. TIM is usually accompanied by other alarms, such as the "LOS (STM1E, STMN)" alarm on page 2-147 or the "HP-UNEQ" alarm on page 2-122. If these alarms accompany a TIM alarm, reattach or replace the original cables/fibers to clear the alarms. If a Transmit or Expected String was changed, restore the original string.

Clear the TIM Alarm

Step 1 Ensure that the physical fibers are correctly configured and attached. To do this, consult site documents. For more information about cabling the ONS 15454 SDH, refer to the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15454 SDH Procedure Guide*.

Step 2 If the alarm does not clear, you can compare the J0 expected and transmitted strings and, if necessary, change them by completing the following steps:

a. Log into the circuit source node and click the **Circuits** tab.

b. Select the circuit reporting the condition, then click **Edit**.

c. Check the "**Show Detailed Circuit Map**" check box and click **Apply**.

d. On the detailed circuit map, right-click the source circuit port and choose **Edit J0 Path Trace (port)** from the shortcut menu.

e. Compare the Current Transmit String and the Current Expected String entries in the Edit J0 Path Trace dialog box.

f. If the strings differ, correct the Transmit or Expected strings and click **Apply**.

g. Click **Close**.

Step 3 If the alarm does not clear, ensure that the signal has not been incorrectly routed. (Although the ONS 15454 SDH routes circuits automatically, the circuit route could have been changed using TL1.) If necessary, manually correct the routing using TL1. For procedures, consult the *Cisco ONS 15454 SDH TL1 Reference Guide* and the *Cisco ONS 15454 SDH TL1 Command Guide*.

Step 4 If the alarm does not clear, log into the Cisco 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.

2.7.354 TIM-MON

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

SDH Logical Objects: STMN

DWDM Logical Object: TRUNK

The TIM Section Monitor TIM alarm is similar to an HP-TIM alarm, but it applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, MXP_2.5G_10G, and TXP_MR_10E cards when they are configured in transparent mode. (In Transparent termination mode, all SDH overhead bytes are passed through from client ports to the trunk ports or from trunk ports to client ports.)

Note For more information about MXP and TXP cards, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Clear the TIM-MON Alarm

Step 1 Complete the "Clear the HP-TIM Alarm" procedure on page 2-122.

Step 2 If the alarm does not clear, log into the Cisco 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.

2.7.355 TPTFAIL (CE100T)

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

SDH Logical Object: CE100T

The Transport (TPT) Layer Failure alarm for the CE-100T-8 card indicates a break in the end-to-end Ethernet link integrity feature of the ONS 15454 SDH CE-100T-8 card. TPTFAIL indicates a far-end condition and not a problem with the port reporting TPTFAIL. TPTFAIL may also occurs on local ports with LCAS-enabled CE-100T-8 cards.

Note For more information about Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.*

Clear the TPTFAIL (CE100T) Alarm

Step 1 Complete the "Clear the TPTFAIL (G1000) Alarm" procedure on page 2-219.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) to report a Service-Affecting (SA) problem.

2.7.356 TPTFAIL (FCMR)

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

SDH Logical Object: FCMR

The Transport Fail alarm is raised against a local Fibre Channel port when the port receives another SDH error such as MS-AIS, TU-LOP, HP-UNEQ, LP-PLM, HP-TIM, LOM (for VCAT only), or SQM (for VCAT only).

The TPTFAIL can be raised against Fibre Channel cards if the remote FC_MR-4 card port is down from INC-SIG-LOSS or INC-SYNC-LOSS. In that case, the remote FC_MR-4 card port sends an error code in the SDH C2 byte and signals the local FC_MR-4 port transmitter to turn off (thus causing the local FC_MR-4 port to raise the TPTFAIL alarm). A pulled receive cable at the far end can also cause the TPTFAIL. This alarm can be demoted when a facility loopback is placed on the FC_MR-4 port.

Clear the TPTFAIL (FCMR) Alarm

Step 1 Find and clear any path alarms applying to the port. See the correct section of this chapter for trouble clearing instructions. Clearing the path alarm also clears the TPTFAIL.

Step 2 If the alarm does not clear, log into the Cisco 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.

2.7.357 TPTFAIL (G1000)

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

SDH Logical Object: G1000

The Transport (TPT) Layer Failure alarm indicates a break in the end-to-end Ethernet link integrity feature of the G-Series cards. TPTFAIL indicates a far-end condition and not a problem with the port reporting TPTFAIL.

The TPTFAIL alarm indicates a problem on either the SDH path or the remote Ethernet port that prevents the complete end-to-end Ethernet path from working. If any SDH path conditions or alarms such as the "AU-AIS" condition on page 2-41, the "AU-LOF" alarm on page 2-43, or the "HP-UNEQ" alarm on page 2-122 exist on the SDH path used by the Ethernet port, the affected port causes a TPTFAIL alarm. Also, if the far-end G-Series Ethernet port is administratively disabled or the port is reporting the "CARLOSS (G1000)" alarm on page 2-57, the C2 byte in the SDH path overhead causes a TPTFAIL to be reported against the near-end port.

When a TPTFAIL alarm occurs, the near-end port is automatically disabled (transmit laser turned off). In turn, the laser shutoff can also cause the external Ethernet device attached at the near end to detect a link down and turn off its transmitter. This also causes a CARLOSS condition to occur on the reporting port. In all cases, the source problem is either in the SDH path being used by the G-Series port or the far-end G-Series port to which it is mapped.

An occurrence of TPTFAIL on a G-Series port indicates either a problem with the SDH path that the port is using or with the far end G-Series port that is mapped to the port.

Note For more information about Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.*

Clear the TPTFAIL (G1000) Alarm

Step 1 Clear any alarms being reported by the STM-N card on the G-Series card circuit.

Step 2 If no alarms are reported by the STM-N card, the problem could be on the far-end G-Series port. Clear any alarms, such as CARLOSS, reported against the far-end port or card.

Step 3 If the alarm does not clear, log into the Cisco 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.

2.7.358 TPTFAIL (ML100T, ML1000, MLFX)

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

SDH Logical Objects: ML100T, ML1000, MLFX

The TPT Layer Failure alarm indicates a break in the end-to-end packet-over-SDH (POS) link integrity feature of the ML-Series POS cards. TPTFAIL indicates a far-end condition or misconfiguration of the POS port.

The TPTFAIL alarm indicates a problem on either the SDH path, the remote POS port, or a misconfiguration of the POS port that prevents the complete end-to-end POS path from working. If any SDH conditions or alarms such as the "AU-AIS" condition on page 2-41, the "AU-LOP" alarm on page 2-43, or the "HP-UNEQ" alarm on page 2-122 exist on the circuit used by the POS port, the affected port could report a TPTFAIL alarm. If the far-end ML-Series POS port is administratively disabled, the port inserts the "AU-AIS" condition on page 2-41 that is detected by the near-end port. The near-end port could report TPTFAIL in this event. If the POS port is misconfigured at the Cisco IOS CLI level, the misconfiguration causes the port to go down and report TPTFAIL.

Note For more information about the ML-Series Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.*

Clear the TPTFAIL (ML100T, ML1000, MLFX) Alarm

Step 1 If there are no SDH alarms reported against the POS port circuit, verify that both POS ports are properly configured. Refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327* for configuration information.

Step 2 If the "LP-PLM" alarm on page 2-161 is the only alarm reported against the POS port circuit, verify that both POS ports are properly configured. Refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327* for configuration information.

Step 3 If present, clear the "AU-AIS" condition on page 2-41, the "AU-LOP" alarm on page 2-43, or the "HP-UNEQ" alarm on page 2-122.

Step 4 If the alarm does not clear, log into the Cisco 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.

2.7.359 TRMT

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

SDH Logical Objects: DS1, E1

A Facility Termination Equipment Failure alarm occurs when there is a transmit failure on the E1-N-14 card because of an internal hardware failure. The card must be replaced.

Clear the TRMT Alarm

Step 1 Replace the E1-N-14 card reporting the failure. Complete the "Physically Replace a Traffic Card" procedure on page 2-242.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454 SDH. Plug the wristband cable into the ESD jack located on the middle-right outside edge of the shelf assembly.

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 "Maintain the Node" chapter in the *Cisco ONS 15454 SDH Procedure Guide* for more information about protection switches.

Note When you replace a card with the identical type of card, you do not need to make any changes to the database.

Step 2 If the alarm does not clear, log into the Cisco 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.

2.7.360 TRMT-MISS

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

SDH Logical Objects: DS1, E1

A Facility Termination Equipment Transmitter Missing alarm occurs when the facility termination equipment detects an incorrect amount of impedance on its backplane connector. Incorrect impedance is detected when a transmit cable is missing on the E-1 port or the backplane does not match the inserted card, for example, an SMB connector or a BNC connector is connected to an E-1 card.

Note E-1s are four-wire circuits and need a positive and negative connection for both transmit and receive.

Clear the TRMT-MISS Alarm

Step 1 Verify that the device attached to the E-1 port is operational.

Step 2 If the device is operational, verify that the cabling is securely connected.

Step 3 If the cabling is secure, verify that the pinouts are correct.

Step 4 If the pinouts are correct, replace the transmit cable.

Step 5 If the alarm does not clear, log into the Cisco 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.

2.7.361 TU-AIS

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

SDH Logical Objects: VCMON-LP, VCTRM-LP

A Tributary Unit (TU) AIS occurs when there is an AIS, indicating a secondary condition, in the low-order tributary overhead of the virtual circuit (VC).

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 TU-AIS Condition

Step 1 Complete the "Clear the AIS Condition" procedure on page 2-31.

Step 2 If the condition does not clear, log into the Cisco 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.

2.7.362 TU-LOP

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

SDH Logical Objects: VCMON-LP, VCTRM-LP

A TU LOP alarm indicates that the SDH low order path overhead section of the administration unit has detected a loss of path. TU-LOP occurs when a mismatch between the expected and provisioned circuit size.

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 TU-LOP Alarm

Step 1 Complete the "Clear the AU-LOP Alarm" procedure on page 2-44.

Step 2 If the alarm does not clear, log into the Cisco 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.

2.7.363 TX-AIS

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

SDH Logical Objects: DS1, DS3, E1, E3

The Transmit Direction AIS condition is raised by the ONS backplane when it receives a far-end LOS from a DS1i-N-14, DS3i-N-14, or E-N card.

Clear the TX-AIS Condition

Step 1 Determine whether there are alarms on the downstream nodes and equipment, especially the "LOS (STM1E, STMN)" alarm on page 2-147, or locked ports.

Step 2 Clear the downstream alarms using the applicable procedures in this chapter.

Step 3 If the condition does not clear, log into the Cisco 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.

2.7.364 TX-LOF

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

SDH Logical Objects: DS1, E1

The Transmit Direction LOF condition is transmitted by the backplane when it receives a DS-1 TX-LOF.

This alarm is raised only at the transmit (egress) side.

Clear the TX-LOF Condition

Step 1 Complete the "Clear the LOF (DS1, DS3, E1, E4, STM1E, STMN) Alarm" procedure on page 2-138.

Step 2 If the condition does not clear, log into the Cisco 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.

2.7.365 TX-RAI

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SDH Logical Objects: DS1, E1, E3

The Transmit Direction RAI condition is transmitted by the backplane when it receives a DS1i-N-14, DS3i-N-12, or E-N card TX-AIS. This alarm is raised only at the transmit side, but RAI is raised at both ends.

Clear the TX-RAI Condition

Step 1 Complete the "Clear the TX-AIS Condition" procedure on page 2-223.

Step 2 If the condition does not clear, log into the Cisco 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.

2.7.366 UNC-WORD

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.367 UNREACHABLE-TARGET-POWER

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.368 UT-COMM-FAIL

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.369 UT-FAIL

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.370 VCG-DEG

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SDH Logical Object: VCG

The VCAT Group Degraded alarm is a VCAT group alarm. (VCATs are groups of independent circuits that are concatenated from different time slots into higher-rate signals.) The alarm occurs when one member circuit carried by the ML-Series Ethernet card is down. This alarm is accompanied by the "OOU-TPT" alarm on page 2-178. It only occurs when a Critical (CR) alarm, such as LOS, causes a signal loss.

Note For more information about the ML-Series Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.*

Clear the VCG-DEG Condition

Step 1 Look for and clear any Critical (CR) alarms that apply to the errored card, such as the "LOS (OTS)" alarm on page 2-147.

Step 2 If the condition does not clear, log into the Cisco 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.

2.7.371 VCG-DOWN

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SDH Logical Object: VCG

The VCAT Group Down alarm is a VCAT group alarm. (VCATs are groups of independent circuits that are concatenated from different time slots into higher-rate signals.) The alarm occurs when both member circuits carried by the ML-Series Ethernet card are down. This alarm occurs in conjunction with another Critical (CR) alarm, such as the "LOS (2R)" alarm on page 2-142.

Note For more information about the ML-Series Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.*

Clear the VCG-DOWN Condition

Step 1 Complete the "Clear the VCG-DEG Condition" procedure on page 2-225.

Step 2 If the condition does not clear, log into the Cisco 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.

2.7.372 VOA-HDEG

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.373 VOA-HFAIL

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.374 VOA-LDEG

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.375 VOA-LFAIL

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.7.376 VOLT-MISM

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SDH Logical Object: PWR

The Power Monitoring Mismatch Between Control Cards alarm is raised against the shelf when the power voltages of both TCC2/TCC2P cards are out of range of each other by more than 5Vdc.

Clear the VOLT-MISM Condition

Step 1 Check the incoming voltage level to the shelf using a voltmeter. Follow site practices or consult the "Install the Shelf and FMECs" chapter in the *Cisco ONS 15454 SDH Procedure Guide* for power installation procedures.

Step 2 Correct any incoming voltage issues.

Step 3 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.7.377 WKSWPR

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SDH Logical Objects: EQPT, STMN, VCMON-HP, VCMON-LP

DWDM Logical Objects: 2R, ESCON, FC, GE, ISC, TRUNK

The Working Switched To Protection condition occurs when a line raises the "LOS (STM1E, STMN)" alarm on page 2-147, the "SF (DS1, DS3, E1, E3, E4, STMN)" condition on page 2-196, or the "SD (DS1, DS3, E1, E3, E4, STM1E, STMN)" condition on page 2-192.

Clear the WKSWPR Condition

Step 1 Complete the "Clear the LOS (STM1E, STMN) Alarm" procedure on page 2-148.

Step 2 If the condition does not clear, log into the Cisco 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.

2.7.378 WTR

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SDH Logical Objects: EQPT, STMN, VCMON-HP, VCMON-LP

DWDM Logical Objects: 2R, ESCON, FC, GE, ISC, TRUNK

The Wait To Restore condition occurs when the "WKSWPR" condition on page 2-226 is raised and the wait-to-restore time has not expired, meaning 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.

Caution E-1 traffic loss can occur on an E-1 with 1:N protection if an E-1 card is reset with the protect card in the WTR state.

Note WTR is an informational condition. It does not require troubleshooting.

2.7.379 WVL-MISMATCH

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8 DWDM Card LED Activity

ONS 15454 SDH DWDM card LED activity differs from typical traffic card activity. The following sections list the DWDM card LED sequences during card insertion and reset.

2.8.1 DWDM Card LED Activity After Insertion

When a DWDM card is inserted in the shelf, the following LED activities occur:

1. The FAIL LED illuminates for approximately 35 seconds.
2. The FAIL LED blinks for approximately 40 seconds.
3. All LEDs illuminate and then turn off within 5 seconds.
4. If new software is being downloaded to the card, the ACT and SF LEDs blink for 20 seconds to 3.5 minutes, depending on the card type.
5. The ACT LED illuminates.

6. The SF LED stays illuminated until all card ports connect to their far-end counterparts and a signal is present.

2.8.2 DWDM Card LED Activity During Reset

When a DWDM card resets (by software or hardware), the following LED activities occur:

1. The FAIL LED switches on for few seconds.
2. The FAIL LED on the physical card blinks and turns off.
3. The white LED with the letters “LDG” appears on the reset card in CTC.
4. The green ACT LED appears in CTC.

2.9 Traffic Card LED Activity

ONS 15454 SDH traffic card LED behavior patterns are listed in the following sections. These sections give behavior for card insertion, reset, and side-switch.

2.9.1 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.

2.9.2 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.

2.9.3 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 ONS 15454 SDH, the ACT/SBY LED is illuminated.
- If you are looking at node view of the ONS 15454 SDH, 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 of the ONS 15454 SDH, 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.

2.9.4 Typical Cross-Connect LED Activity During Side Switch

While a cross-connect card is switched in CTC from active (ACT) to standby (SBY) or from SBY to ACT, the following LED activity occurs:

1. The FAIL LED on the physical card blinks and turns off.
2. The yellow SBY LED becomes a green ACT LED, indicating that it is now active.
3. The green ACT LED becomes a yellow SBY LED, indicating that it is now standby.

2.10 Frequently Used Alarm Troubleshooting Procedures

This section gives common procedures that are frequently used when troubleshooting alarms. Most of these procedures are summarized versions of fuller procedures existing elsewhere in the ONS 15454 SDH documentation. They are included in this chapter for the user’s convenience. For further information, please refer to the *Cisco ONS 15454 SDH Procedure Guide*.

2.10.1 Node and Ring Identification, Change, Visibility, and Termination

The following procedures relate how to identify or change MS-SPRing names and node IDs, and how to verify visibility from other nodes.

Identify an MS-SPRing Ring Name or Node ID Number

Step 1 Log into a node on the network. If you are already logged in, go to Step 2.

Step 2 In node view, click **View > Go to Network View**.

Step 3 Click the **Provisioning > MS-SPRing** tabs.

From the Ring Name column, record the ring name, or in the Nodes column, record the Node IDs in the MS-SPRing. The Node IDs are the numbers in parentheses next to the node name.

Note For more information about ring or node traffic switching operations, refer to the “Maintain the Node” chapter in the *Cisco ONS 15454 SDH Procedure Guide*.

Change an MS-SPRing Ring Name

Step 1 Log into a node on the network. If you are already logged in, go to Step 2.

Step 2 In node view, click **View > Go to Network View**.

Step 3 Click the **Provisioning > MS-SPRing** tabs.

Step 4 Highlight the ring and click **Edit**.

Step 5 In the MS-SPRing 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 an MS-SPRing Node ID Number

Step 1 Log into a node on the network. If you are already logged in, go to Step 2.

Step 2 In node view, click **View > Go to Network View**.

Step 3 Click the **Provisioning > MS-SPRing** tabs.

Step 4 Highlight the ring and click **Edit**.

Step 5 In the MS-SPRing 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

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 > MS-SPRing** tabs.

Step 3 Highlight a MS-SPRing.

Step 4 Click **Ring Map**.

Step 5 In the MS-SPRing 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**.

2.10.2 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

This procedure switches 1+1 protection group traffic from one port in the group to the other using a Force switch.

Caution The Force command overrides normal protective switching mechanisms. Applying this command incorrectly can cause traffic outages.

Caution Traffic is not protected during a Force protection switch.

Note A Force command switches traffic on a working path even if the path has signal degrade (SD) or signal fail (SF) conditions. A force-switch does not switch traffic on a protect path. A Force switch preempts a Manual switch.

Step 1 In node view, click the **Maintenance > Protection** tabs.

Step 2 In the Protection Groups area, select the protection group with the port you want to switch.

Step 3 In the Selected Groups area, select the port belonging to the card you are replacing. You can carry out this command for the working or protect port. For example, if you need to replace the card with the protect/standby port, click this port.

Step 4 In the Switch Commands area, click **Force**.

Step 5 Click **Yes** in the Confirm Force Operation dialog box.

Step 6 If the switch is successful, the group now says "Force to working" in the Selected Groups area.

Initiate a 1+1 Protection Port Manual Switch Command

This procedure switches 1+1 protection group traffic from one port in the group to the other using a Manual switch.

Note A Manual command switches traffic if the path has an error rate less than the signal degrade. A Manual switch is preempted by a Force switch.

Step 1 In node view, click the **Maintenance > Protection** tabs.

Step 2 In the Protection Groups area, select the protection group with the port you want to switch.

Step 3 In the Selected Groups area, select the port belonging to the card you are replacing. You can carry out this command for the working or protect port. For example, if you need to replace the card with the protect/standby port, click this port.

Step 4 In the Switch Commands area, click **Manual**.

Step 5 Click **Yes** in the Confirm Force Operation dialog box.

Step 6 If the switch is successful, the group now says "Manual to working" in the Selected Groups area.

Clear a 1+1 Protection Port 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 protect. If ports are not configured as revertive, clearing a Force switch to protect does not move traffic back.

Note If the Force Switch was user-initiated, the reversion occurs immediately when the clear command is issued. The five-minute WTR period is not needed in this case. If the Force was system-initiated, allow the five-minute waiting period (during WTR) before the reversion occurs.

Step 1 In node view, click the **Maintenance > Protection** tabs.

Step 2 In the Protection Groups area, choose the protection group containing the port you want to clear.

Step 3 In the Selected Group area, choose the port you want to clear.

Step 4 In the Switching Commands area, click **Clear**.

Step 5 Click **Yes** in the Confirmation Dialog box.

The Force switch is cleared. Traffic immediately reverts to the working port if the group was configured for revertive switching.

Initiate a Card or Port Lock On Command

Note For 1:1 and 1:N electrical protection groups, working or protect cards can be placed in the Lock On state. For a 1+1 optical protection group, only the working port can be placed in the Lock On state.

Step 1 In node view, click the **Maintenance > Protection** tabs.

Step 2 In the Protection Groups list, click the protection group where you want to apply a lock-on.

Step 3 If you determine that the protect card is in standby mode and you want to apply the lock-on to the protect card, make the protect card active if necessary by completing the following steps:

- **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 Lock Out Command

Note For 1:1 or 1:N electrical protection groups, working or protect cards can be placed in the Lock Out state. For a 1+1 optical protection group, only the protect port can be placed in the Lock Out state.

Step 1 In node view, click the **Maintenance > Protection** tabs.

Step 2 In the Protection Groups list, click the protection group that contains the card you want to lock out.

Step 3 In the Selected Group list, click the card you want to lock traffic out of.

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 Card or Port Lock On or Lock Out Command

Step 1 In node view, click the **Maintenance > Protection** tabs.

Step 2 In the Protection Groups list, click the protection group that contains the card you want to clear.

Step 3 In the Selected Group list, click the card you want to clear.

Step 4 In the Inhibit Switching area, click **Unlock**.

Step 5 Click **Yes** in the confirmation dialog box.

The lock-on or lockout is cleared.

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.

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.

Initiate a Force Switch for All Circuits on an SNCP Span

This procedure forces all circuits in an SNCP from the working span to the protect. It is used to remove traffic from a card that originates or terminates SNCP circuits.

Caution The Force command overrides normal protective switching mechanisms. Applying this command incorrectly can cause traffic outages.

Caution Traffic is not protected during a Force protection switch.

Step 1 Log into a node on the network. If you are already logged in, continue with Step 3.

Step 2 Click **View > Go to Network View**.

Step 3 Right-click a network span and choose **Circuits**.

The Circuits on Span dialog box shows the SNCP circuits, including circuit names, locations, and a color code showing which circuits are active on the span.

Step 4 Click the **Perform SNCP span switching** field.

Step 5 Choose **FORCE SWITCH AWAY** from the drop-down list.

Step 6 Click **Apply**.

Step 7 In the Confirm SNCP Switch dialog box, click **Yes**.

Step 8 In the Protection Switch Result dialog box, click **OK**.

In the Circuits on Span dialog box, the switch state for all circuits is FORCE. Unprotected circuits do not switch.

Initiate a Manual Switch for All Circuits on an SNCP Span

This procedure manually switches all circuits in an SNCP from the working span to the protect. It is used to remove traffic from a card that originates or terminates SNCP circuits.

Caution The Manual command does not override normal protective switching mechanisms.

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 Click **View > Go to Network View**. If you are already in network view, continue with Step 3.

Step 3 Right-click a network span and choose **Circuits**.

The Circuits on Span dialog box shows the SNCP circuits, including circuit names, locations, and a color code showing which circuits are active on the span.

Step 4 Click the **Perform SNCP span switching** field.

Step 5 Choose **MANUAL** from the drop-down list.

Step 6 Click **Apply**.

Step 7 In the Confirm SNCP Switch dialog box, click **Yes**.

Step 8 In the Protection Switch Result dialog box, click **OK**.

In the Circuits on Span dialog box, the switch state for all circuits is MANUAL. Unprotected circuits do not switch.

Initiate a Lock-Out-of-Protect Switch for All Circuits on an SNCP Span

This procedure prevents all circuits in an SNCP working span from switching to the protect span. It is used to keep traffic off cards that originate or terminate SNCP circuits.

Caution The Lock Out of Protect command does not override normal protective switching mechanisms.

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 Click **View > Go to Network View**. If you are already in network view, continue with Step 3.

Step 3 Right-click a network span and choose **Circuits**.

The Circuits on Span dialog box shows the SNCP circuits, including circuit names, locations, and a color code showing which circuits are active on the span.

Step 4 Click the **Perform SNCP span switching** field.

Step 5 Choose **LOCK OUT OF PROTECT** from the drop-down list.

Step 6 Click **Apply**.

Step 7 In the Confirm SNCP Switch dialog box, click **Yes**.

Step 8 In the Protection Switch Result dialog box, click **OK**.

In the Circuits on Span dialog box, the switch state for all circuits is FORCE. Unprotected circuits do not switch.

Clear an SNCP Span External Switching Command

Note If the ports terminating a span are configured as revertive, clearing a Force switch to protect (or working) moves traffic back to the working port. If ports are not configured as revertive, clearing a Force switch to protect does not move traffic back.

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 Click **View > Go to Network View**. If you are already in network view, continue with Step 3.

Step 3 Right-click a network span and choose **Circuits**.

The Circuits on Span dialog box shows the SNCP circuits, including circuit names, locations, and a color code showing which circuits are active on the span.

Step 4 Initiate a Force switch for all circuits on the span by completing the following steps:

a. Click the **Perform SNCP span switching** field.

b. Choose **CLEAR** from the drop-down list.

c. Click **Apply**.

d. In the Confirm SNCP Switch dialog box, click **Yes**.

e. In the Protection Switch Result dialog box, click **OK**.

In the Circuits on Span dialog box, the switch state for all circuits is CLEAR. Unprotected circuits do not switch.

Initiate a Force Ring Switch on an MS-SPRing

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 From the View menu, choose **Go to Network View**.

Step 3 In network view, click the **Provisioning > MS-SPRing** tabs.

Step 4 Click the row of the MS-SPRing you are switching, then click **Edit**.

Step 5 Right-click a MS-SPRing node west port and choose **Set West Protection Operation**.

Step 6 In the Set West Protection Operation dialog box, choose **FORCE RING** from the drop-down list.

Step 7 Click **OK**.

Step 8 Click **Yes** in the two Confirm MS-SPRing Operation dialog boxes that appear.

Initiate a Force Span Switch on a Four-Fiber MS-SPRing

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 From the View menu, choose **Go to Network View**.

Step 3 In network view, click the **Provisioning > MS-SPRing** tabs.

Step 4 Click the row of the MS-SPRing you are switching, then click **Edit**.

Step 5 Right-click a MS-SPRing node west port and choose **Set West Protection Operation**.

Step 6 In the Set West Protection Operation dialog box, choose **FORCE SPAN** from the drop-down list.

Step 7 Click **OK**.

Step 8 Click **Yes** in the two Confirm MS-SPRing Operation dialog boxes that appear.

Initiate a Manual Ring Switch on an MS-SPRing

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Click the **Provisioning > MS-SPRing** tabs.

Step 3 Choose the MS-SPRing and click **Edit**.

Step 4 Right-click the MS-SPRing 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 **MANUAL RING** from the drop-down list.

Step 6 Click **OK**.

Step 7 Click **Yes** in the two Confirm MS-SPRing Operation dialog boxes.

Initiate a Lockout on an MS-SPRing Protect Span

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Click the **Provisioning > MS-SPRing** tabs.

Step 3 Choose the MS-SPRing and click **Edit**.

Step 4 Right-click the MS-SPRing 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 MS-SPRing Operation dialog boxes.

Initiate an Exercise Ring Switch on an MS-SPRing

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 Click **View > Go to Network View**.

Step 3 Click the **Provisioning > MS-SPRing** tabs.

Step 4 Click the row of the MS-SPRing you are exercising, then click **Edit**.

Step 5 Right-click the west port of a node and choose **Set West Protection Operation**.

Step 6 In the Set West Protection Operation dialog box, choose **EXERCISE RING** from the drop-down list.

Step 7 Click **OK**.

Step 8 Click **Yes** in the Confirm MS-SPRing Operation dialog box.

Initiate an Exercise Ring Switch on a Four Fiber MS-SPRing

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 Click **View > Go to Network View**.

Step 3 Click the **Provisioning > MS-SPRing** tabs.

Step 4 Click the row of the MS-SPRing you are exercising, then click **Edit**.

Step 5 Right-click the west port of a node and choose **Set West Protection Operation**.

Step 6 In the Set West Protection Operation dialog box, choose **EXERCISE SPAN** from the drop-down list.

Step 7 Click **OK**.

Step 8 Click **Yes** in the Confirm MS-SPRing Operation dialog box.

Clear an MS-SPRing External Switching Command

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 Click **View > Go to Network View**.

Step 3 Click the **Provisioning > MS-SPRing** tabs.

Step 4 Click the MS-SPRing you want to clear.

Step 5 Right-click the west port of the MS-SPRing 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 MS-SPRing Operation dialog box.

2.10.3 CTC Card Resetting and Switching

This section gives instructions for resetting traffic cards, TCC2/TCC2P card, and cross-connect 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 *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Caution Resetting the active card in a Y-cable group will cause a traffic outage if the standby card is down for any reason.

Note When an AIC-I card is rest in CTC, any subsequent user client operations (such as CTC or TL1 activity) is paused for approximately 5-10 seconds. The reset does not cause any conditions to be raised.

Note For more information about MXP and TXP cards, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Reset a Traffic Card in CTC

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 In node view, position the cursor over the optical or electrical traffic card slot reporting the alarm.

Step 3 Right-click the card. Choose **Reset Card** from the shortcut menu.

Step 4 Click **Yes** in the Resetting Card dialog box.

Reset an ActiveTCC2/TCC2P Card and Activate the Standby Card

Caution Resetting an active TCC2/TCC2P card reset can be traffic-affecting.

Caution In a node equipped with two TCCPs (not TCC2s), resetting an active TCC2P causes the ALM-PWR and CRFT-TMG ports to transition into the Locked-disabled, NotInstalled&Unassigned state. The ports return to the Unlocked state approximately two minutes after the reset is completed.

Note Before you reset the TCC2/TCC2P card, you should wait at least 60 seconds after the last provisioning change you made to avoid losing any changes to the database.

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 Identify the active TCC2/TCC2P card:

If you are looking at the physical ONS 15454 SDH shelf, the ACT/SBY LED of the active card is green. The ACT/STBLY LED of the standby card is amber.

Step 3 Right-click the active TCC2/TCC2P 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 "2.9 Traffic Card LED Activity" section on page 2-228.

Double-click the node and ensure that the reset TCC2/TCC2P card is in standby mode and that the other TCC2/TCC2P card is active.

- If you are looking at the physical ONS 15454 SDH 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.

Reset the Standby TCC2/TCC2P Card

Step 1 Right-click the standby TCC2/TCC2P card in CTC.

Step 2 Choose Reset Card from the shortcut menu.

Step 3 Click Yes in the Are You Sure dialog box. The card resets, the FAIL LED blinks on the physical card.

Step 4 Wait ten minutes to verify that the card you reset completely reboots. The ACT/STBY LED of this card is amber and the card is in STBY state.

Side Switch the Active and Standby Cross-Connect Cards

Caution The cross-connect card side switch is usually traffic-affecting.

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 Display node view.

Step 3 Determine the active or standby cross-connect card.

The ACT/SBY LED of the active card is green. The ACT/SBY LED of the standby card is amber.

Note You can also position the cursor over the card graphic to display a popup identifying the card as active or standby.

Step 4 In node view, click the **Maintenance > Cross-Connect > Cards** tabs.

Step 5 Click **Switch**.

Step 6 Click **Yes** in the Confirm Switch dialog box. See the "2.9.4 Typical Cross-Connect LED Activity During Side Switch" section on page 2-229 for LED information.

Note During a maintenance side switch or soft reset of an active XC10G card, the 1+1 protection group might display a protection switch. To disallow the protection switch from being displayed, the protection group should be locked at the node where XC switch or soft reset of an active XC switch is in progress.

Caution Active cross connect (XC10G/XCVT) cards should not be physically removed.

The following rules must be followed for removing an Active Cross Connect Card (XC10G/XCVT):

If the active cross connect has to be removed, perform an XCVT/XC10G side switch to change the status of the card from active to standby and then remove the cross connect card once it goes back to standby.

OR

Perform a lockout on all circuits that originate from the node whose active cross connect card has to be removed (performing a lockout on all spans will also accomplish the same goal).

2.10.4 Physical Card Reseating, Resetting, and Replacement

Caution Do not physically replace a card without first making provisions to switch or move traffic to a different card or circuit. General procedures for this are located in the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-230. In-depth traffic switching procedures and information can be found in the *Cisco ONS 15454 SDH Procedure Guide*.

Remove and Reinsert (Reseat) the Standby TCC2/TCC2P Card

Caution Do not perform this action without the supervision and direction of Cisco. 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 TAC numbers for your country.

Caution The TCC2/TCC2P card reseat could be traffic-affecting.

Note Before you reset the TCC2/TCC2P card, you should wait at least 60 seconds after the last provisioning change you made to avoid losing any changes to the database.

Note When a standby TCC2/TCC2P card is removed and reinserted (reseated), all three fan lights could momentarily illuminate, indicating that the fans have also reset.

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Ensure that theTCC2/TCC2P 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 TCC2/TCC2P card is in standby mode, unlatch both the top and bottom ejectors on the TCC2/TCC2P 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 TCC2/TCC2P card requires several minutes to reboot and displays the amber standby LED after rebooting. Refer to the *Cisco ONS 15454 SDH Reference Manual* for more information about LED behavior during card rebooting.

Remove and Reinsert (Reseat) Any Card

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 Traffic Card

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. See the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-230 for commonly used traffic-switching procedures.

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.

Physically Replace an In-Service Cross-Connect Card

Caution The cross-connect reseat could be traffic-affecting. See the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-230 for traffic-switching procedures prior to completing this procedure.

Note This procedure is placed in the chapter as a quick guide for the user's convenience. An in-depth procedure is located in the *Cisco ONS 15454 SDH Procedure Guide*.

Step 1 Determine the active cross-connect card (XC-VXL or XC-VXC-10G). The ACT/STBY LED of the active card is green. The ACT/STBY LED of the standby card is amber.

Note You can also place the cursor over the card graphic to display a popup identifying the card as active or standby.

Step 2 Switch the active cross-connect card (XC-VXL) to standby by completing the following steps:

a. In the node view, click the **Maintenance > Cross-Connect** tabs.

b. Under Cross Connect Cards, choose **Switch**.

c. Click **Yes** in the Confirm Switch dialog box.

Note After the active XC-VXL goes into standby, the original standby slot becomes active. This causes the ACT/STBY LED to become green on the former standby card.

Step 3 Physically remove the new standby cross-connect card (XC-VXL) from the ONS 15454 SDH.

Note An improper removal (IMPROPRMVL) alarm is raised when a card reseat is performed, unless the card is first deleted in Cisco Transport Controller (CTC). The alarm clears after the card replacement is complete.

Step 4 Insert the replacement cross-connect card (XC-VXL) into the empty slot.

The replacement card boots up and becomes ready for service after approximately one minute.

2.10.5 Generic Signal and Circuit Procedures

Verify the Signal BER Threshold Level

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 In node view, double-click the card reporting the alarm to display the card view.

Step 3 Click the **Provisioning > Line** tabs.

Step 4 Under the **SD BER** (or **SF BER**) column on the Provisioning tab, 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 display the range of choices and click the original entry.

Step 7 Click **Apply**.

Delete a Circuit

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 In node view, click the **Circuits** tab.

Step 3 Click the circuit row to highlight it and click **Delete**.

Step 4 Click **Yes** in the Delete Circuits dialog box.

Verify or Create Node RS-DCC Terminations

Note Portions of this procedure are different for ONS 15454 SDH DWDM nodes.

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 Facility or Terminal Loopback Circuit

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 Double-click the reporting card in CTC to display the card view.

Step 3 Click the **Maintenance > Loopback > Port** 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 a state other than Unlocked.

Step 7 If a row shows a state other than Unlocked, click the column cell to display the drop-down list and select **Unlocked**.

Step 8 Click **Apply**.

Clear an STM-N Card XC Loopback Circuit

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

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**.

Clear a Non-STM Card Facility or Terminal Loopback Circuit

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 Double-click the reporting card in CTC to display 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 a state other than Unlocked.

Step 7 If a row shows a state other than Unlocked click in the column cell to display the drop-down list and select **Unlocked**.

Step 8 Click **Apply**.

2.10.6 Air Filter and Fan Procedures

Inspect, Clean, and Replace the Reusable Air Filter

You need a vacuum cleaner or detergent and water faucet, a spare 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.

Step 1 Verify that you are replacing a reusable air filter. The reusable filter is made of a gray, open-cell, polyurethane foam that is specially coated to provide fire and fungi resistance. NEBS 3E and later versions of the ONS 15454 SDH use a reusable air filter.

Step 2 If the air filter is installed in the external filter brackets, slide the filter out of the brackets while being careful not to dislodge any dust that could have collected on the filter by completing the following steps. If the filter is installed beneath the fan tray and not in the external filter brackets:

a. Open the front door of the shelf assembly by completing the following substeps. (If it is already open or if the shelf assembly does not have a front door, continue with Step 3.)

- Open the front door lock.
- Press the door button to release the latch.
- Swing the door open.

b. Remove the front door by completing the following substeps (optional):

- Detach the ground strap from either the door or the chassis by removing one of the Kepnuts.
- Place the Kepnut back on the stud after the ground strap is removed to avoid misplacement.
- Secure the dangling end of the ground strap to the door or chassis with tape.

Step 3 Push the outer side of the handles on the fan-tray assembly to expose the handles.

Step 4 Pull the handles and slide the fan-tray assembly one inch (25.4 mm) out of the shelf assembly and wait until the fans stop.

Step 5 When the fans have stopped, pull the fan-tray assembly completely out of the shelf assembly.

Step 6 Gently remove the air filter from the shelf assembly. Be careful not to dislodge any dust that could have collected on the filter.

Step 7 Visually inspect the air filter material for dirt and dust.

Step 8 If the reusable air filter has a concentration of dirt and dust, either vacuum or wash the air filter. Prior to washing the air filter, replace the dirty air filter with a clean air filter and also reinsert the fan-tray assembly. Wash the dirty air filter under a faucet with a light detergent.

Spare ONS 15454 SDH filters should be kept in stock for this purpose.

Note Cleaning should take place outside the operating environment to avoid releasing dirt and dust near the equipment.

Step 9 If you washed the filter, allow it to completely air dry for at least eight hours.

Caution Do not put a damp filter back in the ONS 15454 SDH.

Step 10 If the air filter should be installed in the external filter brackets, slide the air filter all the way to the back of the brackets to complete the procedure.

Step 11 If the filter should be installed beneath the fan-tray assembly, remove the fan-tray assembly and slide the air filter into the recessed compartment at the bottom of the shelf assembly. Put the front edge of the air filter flush against the front edge of the recessed compartment. Push the fan tray back into the shelf assembly.

Caution If the fan tray does not slide all the way to the back of the shelf assembly, pull the fan tray out and re-adjust the position of the reusable filter until the fan tray fits correctly.

Note On a powered-up ONS 15454 SDH, the fans start immediately after the fan-tray assembly is correctly inserted.

Step 12 To verify that the tray is plugged into the backplane, ensure that the LCD on the front of the fan-tray assembly is activated and displays node information.

Step 13 Rotate the retractable handles back into their compartments.

Step 14 Replace the door and reattach the ground strap.

Remove and Reinsert a Fan-Tray Assembly

Step 1 Use the retractable handles embedded in the front of the fan-tray assembly to pull it forward several inches.

Step 2 Push the fan-tray assembly firmly back into the ONS 15454 SDH.

Step 3 Close the retractable handles.

Replace the Fan-Tray Assembly

Caution The 15454-FTA3 fan-tray assembly can only be installed in ONS 15454 SDH R3.1 and later shelf assemblies (15454-SA-ANSI, P/N: 800-19857; 15454-SA-HD, P/N: 800-24848). It includes a pin that does not allow it to be installed in ONS 15454 shelf assemblies released before ONS 15454 SDH R3.1 (15454-SA-NEBS3E, 15454-SA-NEBS3, and 15454-SA-R1, P/N: 800-07149). Equipment damage can result from attempting to install the 15454-FTA3 in a incompatible shelf assembly.

Caution Do not force a fan-tray assembly into place. Doing so can damage the connectors on the fan tray and/or the connectors on the backplane.

Note The 15454-SA-ANSI or 15454-SA-HD shelf assembly and 15454-FTA3 fan-tray assembly are required with the ONS 15454 STM-64, and STM-16 any slot (AS) cards.

To replace the fan-tray assembly (FTA), it is not necessary to move any of the cable management facilities.

Step 1 Open the front door of the shelf assembly by completing the following steps. If the shelf assembly does not have a front door, continue with Step 3.

- **a.** Open the front door lock.
- **b.** Press the door button to release the latch.
- **c.** Swing the door open.

Step 2 Remove the front door (optional) by completing the following steps:

- **a.** Detach the ground strap from either the door or the chassis by removing one of the Kepnuts.
- **b.** Place the Kepnut back on the stud after the ground strap is removed to avoid misplacement.
- **c.** Secure the dangling end of the ground strap to the door or chassis with tape.

Step 3 Push the outer side of the handles on the fan-tray assembly to expose the handles.

Step 4 Fold out the retractable handles at the outside edges of the fan tray.

Step 5 Pull the handles and slide the fan-tray assembly one inch (25.4 mm) out of the shelf assembly and wait until the fans stop.

Step 6 When the fans have stopped, pull the fan-tray assembly completely out of the shelf assembly.

Step 7 If you are replacing the fan-tray air filter and it is installed beneath the fan-tray assembly, slide the existing air filter out of the shelf assembly and replace it before replacing the fan-tray assembly.

If you are replacing the fan-tray air filter and it is installed in the external bottom bracket, you can slide the existing air filter out of the bracket and replace it at anytime. For more information on the fan-tray air filter, see the "Inspect, Clean, and Replace the Reusable Air Filter" section on page 2-245.

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.

Transients Conditions

This chapter gives a description, entity, SNMP number, and trap for each commonly encountered Cisco ONS 15454 SDH transient condition.

3.1 Transients Indexed By Alphabetical Entry

Table 3-1 alphabetically lists all ONS 15454 SDH transient conditions and their entity, SNMP number, and SNMP trap.

Note The CTC default alarm profile might contain conditions that are not currently implemented but are reserved for future use.

Table 3-1 ONS 15454 SDH Transient Condition Alphabetical Index

Transient Condition	Entity	SNMP Number	SNMP Trap
3.3.1 ADMIN-DISABLE, page 3-4	NE	5270	disableInactiveUser
3.3.2 ADMIN-DISABLE-CLR, page 3-4	NE	5280	disableInactiveClear
3.3.3 ADMIN-LOCKOUT, page 3-4	NE	5040	adminLockoutOfUser
3.3.4 ADMIN-LOCKOUT-CLR, page 3-4	NE	5050	adminLockoutClear
3.3.5 ADMIN-LOGOUT, page 3-4	NE	5020	adminLogoutOfUser
3.3.6 ADMIN-SUSPEND, page 3-4	NE	5340	suspendUser
3.3.7 ADMIN-SUSPEND-CLR, page 3-5	NE	5350	suspendUserClear
3.3.8 AUTOWDMANS, page 3-5	NE	5690	automaticWdmAnsFinished
3.3.9 DBBACKUP-FAIL, page 3-5	EQPT	3724	databaseBackupFailed
3.3.10 DBRESTORE-FAIL, page 3-5	EQPT	3726	databaseRestoreFailed
3.3.11 EXERCISING-RING, page 3-5	OCN	3400	exercisingRingSuccessfully
3.3.12 FIREWALL-DIS, page 3-5	NE	5230	firewallHasBeenDisabled
3.3.13 FRCDWKSWBK-NO-TRFSW, page 3-6	OCN	5560	forcedSwitchBackToWorkingResultedInNoTrafficSwitch

Table 3-1 ONS 15454 SDH Transient Condition Alphabetical Index (continued)

3.3.14 FRCDWKSWPR-NO-TRFSW, page 3-6	OCn	5550	forcedSwitchToProtectResultedInNoTrafficSwitch
3.3.15 INTRUSION, page 3-6	NE	5250	securityIntrusionDetUser
3.3.16 INTRUSION-PSWD, page 3-6	NE	5240	securityIntrusionDetPwd
3.3.17 IOSCFG-COPY-FAIL, page 3-6	—	3660	iosConfigCopyFailed
3.3.18 LOGIN-FAILURE-LOCKOUT, page 3-6	NE	5080	securityInvalidLoginLockedOutSeeAuditLog
3.3.19 LOGIN-FAILURE-ONALRDY, page 3-7	NE	5090	securityInvalidLoginAlreadyLoggedOnSeeAuditLog
3.3.20 LOGIN-FAILURE-PSWD, page 3-7	NE	5070	securityInvalidLoginPasswordSeeAuditLog
3.3.21 LOGIN-FAILURE-USERID, page 3-7	NE	3722	securityInvalidLoginUsernameSeeAuditLog
3.3.22 LOGOUT-IDLE-USER, page 3-7	—	5110	automaticLogoutOfIdleUser
3.3.23 MANWKSWBK-NO-TRFSW, page 3-7	OCN	5540	manualSwitchBackToWorkingResultedInNoTrafficSwitch
3.3.24 MANWKSWPR-NO-TRFSW, page 3-7	OCN	5530	manualSwitchToProtectResultedInNoTrafficSwitch
3.3.25 MSSP-RESYNC, page 3-8	STMN	4340	msspMultiNodeTableUpdateCompleted
3.3.26 PARAM-MISM, page 3-8	OTS, OMS, OCH, AOTS	5840	pluginModuleRangeSettingsMismatch
3.3.27 PM-TCA, page 3-8	—	2120	performanceMonitorThresholdCrossingAlert
3.3.28 PS, page 3-8	EQPT	2130	protectionSwitch
3.3.29 PSWD-CHG-REQUIRED, page 3-8	NE	6280	userPasswordChangeRequired
3.3.30 RMON-ALARM, page 3-8	—	2720	rmonThresholdCrossingAlarm
3.3.31 RMON-RESET, page 3-8	—	2710	rmonHistoriesAndAlarmsResetReboot
3.3.32 SESSION-TIME-LIMIT, page 3-9	NE	6270	sessionTimeLimitExpired
3.3.33 SFTWDOWN-FAIL, page 3-9	EQPT	3480	softwareDownloadFailed
3.3.34 SPANLENGTH-OUT-OF-RANGE, page 3-9	OTS	6150	spanLengthOutOfRange
3.3.35 SWFTDOWNFAIL, page 3-9	EQPT	3480	softwareDownloadFailed
3.3.36 USER-LOCKOUT, page 3-9	NE	5030	userLockedOut

Table 3-1 ONS 15454 SDH Transient Condition Alphabetical Index (continued)

3.3.37 USER-LOGIN, page 3-9	NE	5100	loginOfUser
3.3.38 USER-LOGOUT, page 3-10	NE	5120	logoutOfUser
3.3.39 WKSWBK, page 3-10	EQPT, OCN	2640	switchedBackToWorking
3.3.40 WKSWPR, page 3-10	2R, TRUNK, EQPT, ESCON, FC, GE, ISC, OCN, STSMON, VT-MON	2650	switchedToProtection
3.3.41 WRMRESTART, page 3-10	NE	2660	warmRestart
3.3.42 WTR-SPAN, page 3-10	—	3420	spanIsInWaitToRestoreState

3.2 Trouble Notifications

The ONS 15454 SDH reports trouble by using standard condition characteristics that follow the rules in Telcordia GR-253 and graphical user interface (GUI) state indicators.

The ONS 15454 SDH uses standard Telcordia categories to characterize levels of trouble. The system reports trouble notifications as alarms and reports status or descriptive notifications (if configured to do so) as conditions in the CTC Alarms window. Alarms typically signify a problem that you need to remedy, such as a loss of signal. Conditions do not necessarily require troubleshooting.

3.2.1 Condition Characteristics

Conditions include any problem detected on an ONS 15454 SDH shelf. They can include standing or transient notifications. You can retrieve a snapshot of all currently raised conditions on the network, node, or card in the CTC Conditions window or by using the RTRV-COND commands in TL1.

Note Some cleared conditions are found on the History tab.

For a comprehensive list of conditions, refer to the *Cisco ONS 15454 TL1 Command Guide*.

3.2.2 Condition States

The History tab state (ST) column indicates the disposition of the condition, as follows:

- A raised (R) event is active.
- A cleared (C) event is no longer active.
- A transient (T) event is automatically raised and cleared in CTC during system changes such as user login, log out, and loss of connection to node view. Transient events do not require user action.

3.3 Transient Conditions

This section lists in alphabetical order all the transient conditions encountered in Software Release 6.0. The description, entity, SNMP number, and SNMP trap accompany each condition.

3.3.1 ADMIN-DISABLE

The ADMIN-DISABLE (Disable Inactive User) condition occurs when the administrator disables the user or the account is inactive for a specified period.

This transient condition does not result in a standing condition.

3.3.2 ADMIN-DISABLE-CLR

The ADMIN-DISABLE-CLR (Disable Inactive Clear) condition occurs when the administrator clears the disable flag on the user account.

This transient condition does not result in a standing condition.

3.3.3 ADMIN-LOCKOUT

The ADMIN-LOCKOUT (Admin Lockout of User) condition occurs when the administrator locks a user account.

This transient condition does not result in a standing condition.

3.3.4 ADMIN-LOCKOUT-CLR

The ADMIN-LOCKOUT-CLR (Admin Lockout Clear) condition occurs when the administrator unlocks a user account or the lockout time expires.

This transient condition does not result in a standing condition.

3.3.5 ADMIN-LOGOUT

The ADMIN-LOGOUT (Admin Logout of User) condition occurs when the administrator logs off a user session.

This transient condition does not result in a standing condition.

3.3.6 ADMIN-SUSPEND

The ADMIN-SUSPEND (Suspend User) condition occurs when the password for a user account expires.

This transient condition does not result in a standing condition.

3.3.7 ADMIN-SUSPEND-CLR

The ADMIN-SUSPEND-CLR (Suspend User Clear) condition occurs when the user or administrator changes the password.

This transient condition does not result in a standing condition.

3.3.8 AUTOWDMANS

The AUTOWDMANS (Automatic WDM ANS Finish) condition indicates that an automatic node setup command has been initiated. It normally occurs when you replace DWDM cards; the condition is an indication that the system has regulated the card.

This transient condition does not result in a standing condition.

3.3.9 DBBACKUP-FAIL

The DBBACKUP-FAIL (Database Backup Failed) condition occurs when the system fails to back up the database when the backup command is initiated.

This condition can occur when the server is not able to handle the backup operation due to network or server issues. Repeat the same operation again and check to see if it is successful. If the backup fails, it could be due to a network issue or software program failure. Contact TAC for assistance.

3.3.10 DBRESTORE-FAIL

The DBRESTORE-FAIL (Database Restore Failed) condition occurs when the system fails to restore the backed up database when the restore command is initiated.

This condition can be due to server issues, network issues, or human error (pointing to a file that does not exist, wrong file name, etc.). Retrying the database restore with the correct file will usually succeed. If the network issue persists, you must contact network lab support. If the condition is caused by a network element (NE) failure, contact TAC for assistance.

3.3.11 EXERCISING-RING

The EXERCISING-RING (Exercising Ring Successfully) condition occurs whenever you issue an Exercise-Ring command from CTC or TL1. This condition indicates that a command is being executed. You must issue another command to clear the exercise and the condition.

3.3.12 FIREWALL-DIS

The FIREWALL-DIS (Firewall Has Been Disabled) condition occurs when you provision the firewall to Disabled.

This transient condition does not result in a standing condition.

3.3.13 FRCDWKSWBK-NO-TRFSW

The FRCDWKSWBK-NO-TRFSW (Forced Switch Back to Working Resulted in No Traffic Switch) condition occurs when you perform a Force Switch to the working port/card and the working port/card is already active.

This transient condition might result in a Force Switch (Ring or Span) standing condition for an MS-SPRing.

3.3.14 FRCDWKSWPR-NO-TRFSW

The FRCDWKSWPR-NO-TRFSW (Forced Switch to Protection Resulted in No Traffic Switch) condition occurs when you perform a Force Switch to the protect port/card, and the protect port/card is already active.

This transient condition does not result in a standing condition.

3.3.15 INTRUSION

The INTRUSION (Invalid Login Username) condition occurs when you attempt to log in with an invalid user ID.

This transient condition does not result in a standing condition.

3.3.16 INTRUSION-PSWD

The INTRUSION -PSWD (Security Intrusion Attempt Detected) condition occurs when you attempt to login with an invalid password.

This transient condition does not result in a standing condition.

3.3.17 IOSCFG-COPY-FAIL

The IOSCFG-COPY-FAIL (IOS Config Copy Failed) condition occurs on ML-Series Ethernet cards when the software fails to upload or download the Cisco IOS startup configuration file to or from an ML-Series card. This condition is similar to the "SFTWDOWN-FAIL" condition on page 3-9, but the IOSCFG-COPY-FAIL condition applies to ML-Series Ethernet cards rather than the TCC2/TCC2P card.

3.3.18 LOGIN-FAILURE-LOCKOUT

The LOGIN-FAILURE-LOCKOUT (Invalid Login–Locked Out) condition occurs when you attempt to log into a locked account.

This transient condition does not result in a standing condition.

3.3.19 LOGIN-FAILURE-ONALRDY

The LOGIN-FAILURE-ONALRDY (Security: Invalid Login–Already Logged On) condition occurs when you attempt to log in with an existing session and SUPN policy.

This transient condition does not result in a standing condition.

3.3.20 LOGIN-FAILURE-PSWD

The LOGIN-FAILURE-PSWD (Invalid Login–Password) condition occurs when you attempt to log in with an invalid password.

This transient condition does not result in a standing condition.

3.3.21 LOGIN-FAILURE-USERID

The LOGIN-FAILURE-USERID (Invalid Login–Username) condition occurs when a user login (CTC, CTM, or TL1) fails because the login username is not present on the node database. You must log in again with an existing user ID.

This transient condition is equivalent to a security warning. You must check the security log (audit log) for other security-related actions that have occurred.

3.3.22 LOGOUT-IDLE-USER

The LOGOUT-IDLE-USER (Automatic Logout of Idle User) condition occurs when a user session is idle for too long (the idle timeout expires) and the session terminates as a result. You must log in again to restart your session.

3.3.23 MANWKSWBK-NO-TRFSW

The MANWKSWBK-NO-TRFSW (Manual Switch Back To Working Resulted in No Traffic Switch) condition occurs when you perform a Manual switch to the working port/card and the working port/ card is already active.

This transient condition does not result in a standing condition.

3.3.24 MANWKSWPR-NO-TRFSW

The MANWKSWPR-NO-TRFSW (Manual Switch to Protect Resulted in No Traffic Switch) condition occurs when you perform a Manual switch to the protect port/card and the protect port/card is already active.

This transient condition results in an MS-SPRing Manual Switch (Span or Ring) standing condition.

3.3.25 MSSP-RESYNC

The MSSP-RESYNC (MS-SPRing Multi-Node Table Update Completed) condition occurs when a node receives all relevant information such as Payload, pathState, Rip, XcTbls, and XcVtTbls 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 Switched Ring commands.

3.3.26 PARAM-MISM

The PARAM-MISM (Plug-in Module Range Settings Mismatch) condition occurs when the parameter range values stored on a small-form factor pluggable (SFP) device are different from the parameters stored in the TCC2/TCC2P database.

The transient condition is not user-serviceable.

3.3.27 PM-TCA

The PM-TCA (Performance Monitor Threshold Crossing Alert) condition occurs when network collisions cross the rising threshold for the first time.

3.3.28 PS

The PS (Protection Switch) condition occurs when the traffic switches from a working/active card to a protect/standby card.

3.3.29 PSWD-CHG-REQUIRED

The PSWD-CHG-REQUIRED (User Password Change Required) condition occurs when you are denied login for a shell function such as telnet or FTP because you did not change the login password. You can change the password through CTC or TL1.

3.3.30 RMON-ALARM

The RMON-ALARM (RMON Threshold Crossing Alarm) condition occurs when the remote monitoring variable crosses the threshold.

3.3.31 RMON-RESET

The RMON-RESET (RMON Histories and Alarms Reset Reboot) condition occurs when the time-of-day settings on the TCC2/TCC2P card are increased or decreased by more than five seconds. This invalidates all the history data and remote monitoring (RMON) must restart. It can also occur when you reset a card.

3.3.32 SESSION-TIME-LIMIT

The SESSION-TIME-LIMIT (Session Time Limit Expired) condition occurs when a login session exceeds the time limit and you are logged out of the session. You must login again.

3.3.33 SFTWDOWN-FAIL

The SFTDOWN-FAIL (Software Download Failed) condition occurs when the system fails to download the required software.

An incorrect input that points to the wrong place or file, network issues, or a bad (corrupt) package can cause this failure. Retrying the operation with the correct name/location will usually succeed. If network issues persist, you must contact the network lab support. If the package is corrupt, contact Cisco TAC.

3.3.34 SPANLENGTH-OUT-OF-RANGE

The SPANLENGTH-OUT-OF-RANGE (Span Length Out of Range) condition occurs when the measured span loss does not fall within the limits of minimum and maximum expected span loss. It can also occur when the difference between MaxExpSpanLoss and MinExpSpanLoss is greater than 1dB.

When you perform a Calculate Span Loss operation on a DWDM node, the software measures the real span loss in the field by comparing the far-end POSC power and the near-end OSC power.

3.3.35 SWFTDOWNFAIL

The SFTDOWN-FAIL (Software Download Failed) condition occurs when the system fails to download the required software.

An incorrect input that points to the wrong place or file, network issues, or a bad (corrupt) package can cause this failure. Retrying the operation with the correct name/location will usually succeed. If network issues persist, you must contact the network lab support. If the package is corrupt, contact Cisco TAC.

3.3.36 USER-LOCKOUT

The USER-LOCKOUT (User Locked Out) condition occurs when the system locks an account because of a failed login attempt. To proceed, the administrator must unlock the account or the lockout time must expire.

3.3.37 USER-LOGIN

The USER-LOGIN (Login of User) occurs when you begin a new session by verifying your User ID and password.

This transient condition does not result in a standing condition.

3.3.38 USER-LOGOUT

The USER-LOGOUT (Logout of User) condition occurs when you stop a login session by logging out of your account.

This transient condition does not result in a standing condition.

3.3.39 WKSWBK

The WKSWBK (Switched Back to Working) condition occurs when traffic switches back to the working port/card in a non-revertive protection group.

This transient condition does not result in a standing condition.

3.3.40 WKSWPR

The Switched to Protection (WKSWPR) condition occurs when traffic switches to the protect port/card in a non-revertive protection group. This transient condition does not result in a standing condition. The (WKSWPR) is raised as a standing condition in a revertive protection group.

The Switched to Protection (WKSWPR) condition also occurs after the protection switch in a 1+1 non-revertive protection group as a transient condition. When the protection group is changed to revertive, the (WKSWPR) is not raised as a standing condition or as a new transient condition. However, after a protection switch in a 1:1 protection group, the user will not be allowed to configure the protection group from non-revertive to revertive.

3.3.41 WRMRESTART

The WRMRESTART (Warm Restart) condition occurs when the node restarts while powered up. A restart can be caused by provisioning, such as database-restore and IP changes, or software defects. A WRMRESTART is normally accompanied by MANRESET or AUTORESET to indicate whether the reset was initiated manually (MAN) or automatically (AUTO).

This is the first condition that appears after a TCC2/TCC2P card is powered up. The condition changes to COLD-START if the TCC2/TCC2P card is restarted from a physical reseat or a power loss.

3.3.42 WTR-SPAN

The WTR-SPAN (Span is in Wait To Restore State) condition occurs when a BLSR switches to another span due to a Signal Failure-Span command or a fiber is pulled from a four-fiber BLSR configuration. The condition is raised until the WaitToRestore (WTR) period expires.

This transient condition clears when the BLSR returns to a normal condition or the IDLE state.

Error Messages

Note The terms "Unidirectional Path Switched Ring" and "UPSR" may appear in Cisco literature. These terms do not refer to using Cisco ONS 15xxx products in a unidirectional path switched ring configuration. Rather, these terms, as well as "Path Protected Mesh Network" and "PPMN," refer generally to Cisco's path protection feature, which may be used in any topological network configuration. Cisco does not recommend using its path protection feature in any particular topological network configuration.

This chapter lists the Cisco ONS 15454, 15454 SDH, 15600, 15327 and 15310-CL error messages. The error dialog box in Figure 4-1 consists of three parts: the error title, error ID, and error message. The table lists two types of messages: error messages (EID-*nnnn*) and warning messages (WID-*nnnn*). Error messages are alerts that an unexpected or undesirable operation has occurred which either indicates the risk of loss of traffic or an inability to properly manage devices in the network. Warnings are alerts that the requested operation could lead to an error. Warnings are sometimes used to convey important information.

Figure 4-1 Error Dialog Box

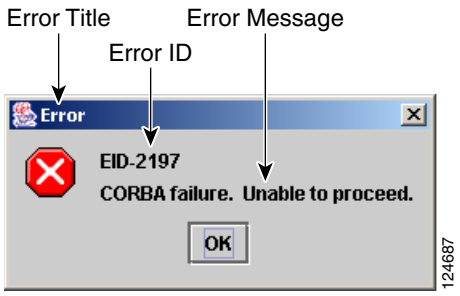


Table 4-1 gives a list of all error or warning message numbers, the messages, and a brief description of each message.

Table 4-1 Error Messages

Error or Warning ID	Error or Warning Message	Description
EID-0	Invalid error ID.	The error ID is invalid.
EID-1	Null pointer encountered in {0}.	Cisco Transport Controller (CTC) encountered a null pointer in the area described by the specified item.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
EID-1000	The host name of the network element cannot be resolved to an address.	Refer to error or warning message text.
EID-1001	Unable to launch CTC due to applet security restrictions. Please review the installation instructions to make sure that the CTC launcher is given the permissions it needs. Note that you must exit and restart your browser in order for the new permissions to take effect.	Refer to error or warning message text.
EID-1002	The host name (e.g., for the network element) was successfully resolved to its address, but no route can be found through the network to reach the address.	The node is not reachable from CTC client station.
EID-1003	An error was encountered while attempting to launch CTC. {0}	Unexpected exception or error while launching CTC from the applet.
EID-1004	Problem Deleting CTC Cache: {0} {1}	Unable to delete the CTC cached JARs, because another application may have the JAR files running; for example, another instance of CTC.
EID-1005	An error occurred while writing to the {0} file.	CTC encountered an error while writing to log files, preference files, etc.
EID-1006	The URL used to download {0} is malformed.	The URL used to download the Launcher.jar file is malformed.
EID-1007	An I/O error occurred while trying to download {0}.	An input or output exception was encountered when CTC tried to download the GUI launcher.
EID-1018	Password must contain at least 1 alphabetic, 1 numeric, and 1 special character (+, # or %). 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}.	Failed to display the indicated view—node or network.
EID-1022	A session cannot be opened right now with this slot. Most likely someone else (using a different CTC) already has a session opened with this slot. Please try again later.	Refer to the error message text. Ensure that the shell access in CTC (Provisioning>Security>Access) is set to non-secure mode.
EID-1023	This session has been terminated. This can happen if the card resets, the session has timed out, or if someone else (possibly using a different CTC) already has a session open with this slot.	Refer to error message text.
EID-1025	Unable to create Help Broker.	CTC was unable to create the help broker for the online help.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
EID-1026	Unable to locate HelpSet.	CTC was unable to locate the help set for the online help.
EID-1027	Unable to locate Help ID: {0}	CTC was unable to locate the help ID for the online help.
EID-1028	Error saving table. {0}	There was an error while saving the specified table.
EID-1031	CTC cannot locate the online user manual files. The files may have been moved, deleted, or not installed. To install online user manuals, run the CTC installation wizard on the software or documentation CD.	Refer to error message text.
EID-1032	CTC cannot locate Acrobat Reader. If Acrobat Reader is not installed, you can install the Reader using the CTC installation wizard provided on the software or documentation CD.	Refer to error message text.
EID-1034	Unable to locate HelpSet when searching for Help ID "{0}".	CTC is unable to locate the specified help ID of the context sensitive help files.
EID-1035	CTC experienced an I/O error while working with the log files. Usually this means that the computer has run out of disk space. This problem may or may not cause CTC to stop responding. Ending this CTC session is recommended, but not required.	Refer to error message text.
WID-1036	WARNING: Deleting the CTC cache may cause any CTC running on this system to behave in an unexpected manner.	Refer to warning message text.
EID-1037	Could not open {0}. Please enter another filename.	Invalid file name. CTC is unable to open the file.
EID-1038	The file {0} does not exist.	The specified file does not exist.
EID-1039	The version of the browser applet does not match the version required by the network element. Please close and restart your browser in order to launch the Cisco Transport Controller.	Refer to error message.
WID-1040	WARNING: Running the CTC with a JRE version other than the recommended JRE version might cause the CTC to behave in an unexpected manner.	Refer to warning message.
EID-2001	No rolls selected. {0}	No rolls were selected for the bridge and roll.
EID-2002	The Roll must be completed or cancelled before it can be deleted.	You cannot delete the roll unless it has been completed or cancelled.
EID-2003	Error deleting roll.	There was an error when CTC tried to delete the roll.
EID-2004	No IOS slot selected.	You did not select a Cisco IOS slot.
EID-2005	CTC cannot find the online help files for {0}. The files may have been moved, deleted, or not installed. To install online help, run the setup program on the software or documentation CDs.	CTC cannot find the online help files for the specified window. The files might have been moved, deleted, or not installed. To install online help, run the setup program on the software or documentation CDs.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
EID-2006	Error editing circuit(s). {0} {1}.	An error occurred when CTC tried to open the circuit for editing.
EID-2007	Unable to save preferences.	CTC cannot save the preferences.
EID-2008	Unable to store circuit preferences: {0}	CTC cannot find the file needed to save the circuit preferences.
EID-2009	Unable to download package: {0}	Refer to error message text.
EID-2010	Delete destination failed.	CTC could not delete the destination.
EID-2011	Circuit destroy failed.	CTC could not destroy the circuit.
EID-2012	Reverse circuit destroy failed.	CTC could not reverse the circuit destroy.
EID-2013	Circuit creation error. Circuit creation cannot proceed due to changes in the network which affected the circuit(s) being created. The dialog will close. Please try again.	Refer to error message text.
EID-2014	No circuit(s) selected. {0}	You must select a circuit to complete this function.
EID-2015	Unable to delete circuit {0}as it has one or more rolls.	You must delete the rolls in the circuit before deleting the circuit itself.
EID-2016	Unable to delete circuit.	CTC could not delete the tunnel as there are circuits that use the tunnel.
EID-2017	Error mapping circuit. {0}	There was an error mapping the circuit.
EID-2018	Circuit roll failure. The circuit has to be in the DISCOVERED state in order to perform a roll.	There was a failure in circuit roll. Change the circuit state to DISCOVERED and proceed.
EID-2019	Circuit roll failure. Bridge and roll is not supported on a DWDM circuit.	Refer to error message text.
EID-2020	Circuit roll failure. The two circuits must have the same direction.	Refer to error message text.
EID-2021	Circuit roll failure. The two circuits must have the same size.	Refer to error message text.
EID-2022	Circuit roll failure. A maximum of two circuits can be selected for a bridge and roll operation.	Refer to error message text.
EID-2023	Unable to create new user account.	Refer to error message text.
EID-2024	Node selection error.	There was an error during node selection.
EID-2025	This feature cannot be used. Verify that each of the endpoints of this circuit are running software that supports this feature.	Refer to error or warning message text. This error is generated from the AnsOpticsParamsPane to indicate that the selected ring type is not supported by the endpoints of the circuit. In the VLAN tab it indicates that the back-end spanning tree protocol (STP) disabling is not supported.
EID-2026	Unable to apply {0} request. {1}	Error occurred while attempting to switch a path protection circuit away from a span.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
EID-2027	Error deleting circuit drop.	CTC could not delete the circuit drop.
EID-2028	Error removing circuit node.	CTC could not remove the circuit node.
EID-2029	The requested operation is not supported.	The task you are trying to complete is not supported by CTC.
EID-2030	Provisioning error.	There was an error during provisioning.
EID-2031	Error adding node.	There was an error while adding a node.
EID-2032	Unable to rename circuit. {0}	CTC could not rename the circuit.
EID-2033	An error occurred during validation. {0}	There was an internal error while validating the user changes after the Apply button was pressed. This error can occur in the Edit Circuit dialog box or in the BLSR table in the shelf view (rare condition).
EID-2034	Unable to add network circuits: {0}	Refer to error message text.
EID-2035	The source and destination nodes are not connected.	Refer to error message text.
EID-2036	Cannot delete this {0}. LAN Access has been disabled on this node and this {0} is needed to access the node.	You cannot delete the DCC/GCC link as it is needed to access the node.
EID-2037	Application error. Cannot find attribute for {0}.	CTC cannot find an attribute for the specified item.
EID-2038	Invalid protection operation.	The protection operation you tried to execute is invalid.
EID-2040	Please select a node first.	You must select a node before performing the task.
EID-2041	No paths are available on this link. Please make another selection.	You must select a link that has paths available.
EID-2042	This span is not selectable. Only the green spans with an arrow may be selected.	Refer to error message text.
EID-2043	This node is not selectable. Only the source node and nodes attached to included spans (blue) are selectable. Selecting a selectable node will enable its available outgoing spans.	Refer to error message text.
EID-2044	This link may not be included in the required list. Constraints only apply to the primary path. Each node may have a maximum of one incoming signal and one outgoing link.	You must select only one link going in and out of a node. Selecting more than one link is contradictory to the path selection algorithm.
EID-2045	This link may not be included in the required list. Only one outgoing link may be included for each node.	Refer to error message text.
EID-2047	Error validating slot number. Please enter a valid value for the slot number.	There was an error due to an invalid slot number.
EID-2048	Error validating port number. Please enter a valid value for the port number.	There was an error due to an invalid port number.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
EID-2050	New circuit destroy failed.	CTC could not destroy the new circuit.
EID-2051	Circuit cannot be downgraded. {0}	The specified circuit cannot be downgraded.
EID-2052	Error during circuit processing.	There was an error during the circuit processing.
EID-2054	Endpoint selection error.	There was an error during the endpoint selection.
EID-2055	No endpoints are available for this selection. Please make another selection.	This error occurs in the circuit creation dialog only during a race condition that has incorrectly allowed entities without endpoints to be displayed in the combo boxes.
EID-2056	Communication error. {0}	An internal error occurred in Network Alarm tab while synchronizing alarms with the nodes.
EID-2059	Node deletion Error. {0}	There was an error during the node deletion.
EID-2060	No PCA circuits found.	CTC could not find any protection channel access (PCA) circuits for this task.
EID-2061	Error provisioning VLAN.	There was an error defining the VLAN.
EID-2062	Cannot delete VLAN. No VLAN(s) are selected. Please select a VLAN.	Cannot delete VLAN. No VLAN(s) are selected. Please select a VLAN.
EID-2063	Cannot delete default VLAN.	The selected VLAN is the default VLAN, and cannot be deleted.
EID-2064	Error deleting VLANs. {0}	There was an error deleting the specified VLAN.
EID-2065	Cannot import profile. Profile "{0}" exists in the editor and the maximum number of copies (ten) exists in the editor. Aborting the import. The profile has already been loaded eleven times.	Cannot import the profile as the profile has reached the maximum number of copies in the editor.
EID-2066	Unable to store profile. Error writing to {0}.	CTC encountered an error while trying to store the profile.
EID-2067	File write error. {0}	CTC encountered an error while writing the specified file.
EID-2068	Unable to load alarm profile from node.	CTC encountered an error trying to load the alarm profile from the node.
EID-2069	File not found or I/O exception. (No such file or directory)	Either the specified file was not found, or there was an input/output exception.
EID-2070	Failure deleting profile. {0}	There was a failure in deleting the specified profile.
EID-2071	Only one column may be highlighted.	You cannot select more than one column during clone action.
EID-2072	Only one profile may be highlighted.	You cannot select more than one profile.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
EID-2073	This column is permanent and may not be removed.	You cannot delete a permanent column.
EID-2074	Select one or more profiles.	You have not selected any profile or column. Reset operation is done by right-clicking the selected column.
EID-2075	This column is permanent and may not be reset.	A permanent column is nonresettable.
EID-2077	This column is permanent and may not be renamed.	You cannot rename a permanent column.
EID-2078	At least two columns must be highlighted.	You cannot compare two profiles unless you select two columns.
EID-2079	Cannot load alarmables into table. There are no reachable nodes from which the list of alarmables may be loaded. Please wait until such a node is reachable and try again.	Refer to error message text.
EID-2080	Node {0} has no profiles.	The specified node does not have any profiles.
EID-2081	Error removing profile {0} from node {1}.	There was an error while removing the specified profile from the specified node.
EID-2082	Cannot find profile {0} on node {1}.	CTC cannot find the specified profile from the specified node.
EID-2083	Error adding profile {0} to node {1}.	There was an error adding the specified profile to the specified node.
EID-2085	Invalid profile selection. No profiles were selected.	You tried to select an invalid profile. Select another profile.
EID-2086	Invalid node selection. No nodes were selected.	You tried to select an invalid node. Select another node.
EID-2087	No profiles were selected. Please select at least one profile.	Refer to error message text.
EID-2088	Invalid profile name.	The profile name cannot be empty.
EID-2089	Too many copies of {0} exist. Please choose another name.	Select a unique name.
EID-2090	No nodes selected. Please select the node(s) on which to store the profile(s).	You must select one or more nodes on which you can store the profile.
EID-2091	Unable to switch to node {0}.	CTC is unable to switch to the specified node.
EID-2092	General exception error.	CTC encountered a general exception error while trying to complete the task.
EID-2093	Not enough characters in name. {0}	The name must have a minimum of six characters.
EID-2094	Password and confirmed password fields do not match.	You must make sure the two fields have the same password.
EID-2095	Illegal password. {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.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
EID-2097	No user name specified.	You did not specify a user name.
EID-2099	Ring switching error.	There was an error during the ring switch.
EID-2100	Please select at least one profile to delete.	You have not selected the profile to delete.
EID-2101	Protection switching error.	There was an error during the protection switching.
EID-2102	The forced switch could not be removed for some circuits. You must switch these circuits manually.	The forced switch could not be removed for some circuits. You must switch these circuits manually.
EID-2103	Error upgrading span.	There was an error during the span upgrade.
EID-2104	Unable to switch circuits back as one or both nodes are not reachable.	This error occurs during the path protection span upgrade procedure.
EID-2106	The node name cannot be empty.	You must supply a name for the node.
EID-2107	Error adding {0}, unknown host.	There was an error adding the specified item.
EID-2108	{0} is already in the network.	The specified item exists in the network.
EID-2109	The node is already in the current login group.	The node you are trying to add is already present in the current login group.
EID-2110	Please enter a number between 0 and {0}.	You must enter a number in the range between 0 and the specified value.
EID-2111	This node ID is already in use. Please choose another.	Select a node ID that is not in use.
EID-2113	Cannot set extension byte for ring. {0}	CTC cannot set the extension byte.
EID-2114	Card communication failure. Error applying operation.	This error can occur during an attempt to apply a BLSR protection operation to a line.
EID-2115	Error applying operation. {0}	There was an error in applying the specified operation.
EID-2116	Invalid extension byte setting for ring. {0}	The extension byte set for the specified ring is invalid.
EID-2118	Cannot delete ring. There is a protection operation set. All protection operations must be clear for ring to be deleted.	Delete all the protection operations for the ring before it can be deleted.
EID-2119	Cannot delete {0} because a protection switch is in effect. Please clear any protection operations, make sure that the reversion time is not "never" and allow any protection switches to clear before trying again.	Clear all protection operations or switches before deleting the ring.
EID-2120	The following nodes could not be unprovisioned {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	Cannot upgrade ring. {0}	CTC cannot upgrade the specified ring.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
EID-2122	Inadequate ring speed for upgrade. Only {0} (or higher) {1} can be upgraded to 4-fiber.	You have selected an incorrect ring speed for upgrade. Only rings within the specified parameters can be upgraded to 4-fiber BLSR.
EID-2123	Verify that the following nodes have at least two in-service ports with the same speed as the 2-fiber {0}. The ports cannot serve as a timing reference, and they cannot have DCC terminations or overhead circuits. {1}	Nonupgradable nodes. Verify that the specified nodes have at least two IS-NR ports with the same speed as the 2-fiber BLSR. The specified ports cannot serve as a timing reference, and they cannot have data communications channel (DCC) terminations or overhead circuits.
EID-2124	You cannot add this span because it is connected to a node that already has the east and west ports defined.	Refer to error message text.
EID-2125	You cannot add this span as it would cause a single card to host both the east span and the west span. A card cannot protect itself.	Refer to error message text.
EID-2126	OSPF area error. {0}	There is an Open Shortest Path First (OSPF) area error.
EID-2127	You cannot add this span. It would cause the following circuit(s) to occupy different STS regions on different spans. {0} Either select a different span or delete the above circuit(s).	A circuit cannot occupy different STS regions on different spans. You may add a different span or delete the specified circuit.
EID-2128	Illegal state error.	An internal error occurred while trying to remove a span from a BLSR. This alarm occurs in the network-level BLSR creation dialog box.
EID-2129	This port is already assigned. The east and west ports must be different.	Refer to error message text.
EID-2130	The ring ID value, {0}, is not valid. Please enter a valid number between 0 and 9999.	Enter a ring ID value between 0 and 9999.
EID-2131	Cannot set reversion to INCONSISTENT.	You must select another reversion type.
EID-2135	Unable to store overhead circuit preferences: {0}	Input/Output error. Unable to store overhead circuit preferences.
EID-2137	Circuit merge error. {0}	There was an error while merging the circuits.
EID-2138	Cannot delete all destinations. Please try again.	Refer to error message text.
EID-2139	Error updating destinations.	There was an error in updating the circuit destinations.
EID-2143	No online help version selected. Cannot delete the online help book.	Select the version of online help, and proceed.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
EID-2144	Error deleting online help book(s). {0}	You cannot delete the specified online help.
EID-2145	Unable to locate a node with an IOS card.	Refer to error message.
EID-2146	Security violation. You may only logout your own account.	You cannot logout of an account other than your own.
EID-2147	Security violation. You may only change your own account.	You cannot change an account other than your own.
EID-2148	Security violation. You may not delete the account under which you are currently logged in.	You cannot delete the account you are currently lodge in.
WID-2149	There is nothing exportable on this view.	Refer to error message text.
WID-2150	Node {0} is not initialized. Please wait and try again.	Wait till the specified node is initialized and try again.
WID-2152	Spanning tree protection is being disabled for this circuit.	Refer to warning message text.
WID-2153	Adding this drop makes the circuit a PCA circuit.	Refer to warning message text.
WID-2154	Disallow creating monitor circuits on a port grouping circuit.	Refer to warning message text.
WID-2155	Only partial switch count support on some nodes. {0}	The specified nodes do not support switch counts completely.
WID-2156	Manual roll mode is recommended for dual rolls. For auto dual rolls, please verify that roll to facilities are in service and error free.	Refer to warning message text.
WID-2157	Cannot complete roll(s). {0}	CTC could not complete the roll because roll is destroyed, roll is in incomplete state, roll is in TL1_roll state, roll is cancelled, or roll is not ready to complete.
EID-2158	Invalid roll mode. {0}	There are two roll modes such as auto and manual. For one way circuit source roll, the roll mode must be auto and for one way circuit destination roll, the roll mode must be manual.
EID-2159	Roll not ready for completion. {0}	The roll is not ready for completion.
EID-2160	Roll not connected. {0}	Refer to error message text.
EID-2161	Sibling roll 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 manual roll, you must complete the roll from CTC if Bridge and Roll is operated from CTC, or from TL1 if Bridge and Roll is operated from TL1.
EID-2162	Error during roll acknowledgement. {0}	Refer to error message text.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
EID-2163	Cannot cancel roll. {0}	CTC cannot cancel the roll.
EID-2164	Roll error. {0}	CTC encountered a roll error.
WID-2165	The MAC address of node {0} has been changed. All circuits originating from or dropping at this node will need to be repaired.	Repair the circuits that originate from or drop at the specified node, with the new MAC address.
WID-2166	Unable to insert node into the domain as the node is not initialized.	Initialize the node and proceed.
WID-2167	Insufficient security privilege to perform this action.	You do not have the privilege to perform this action.
WID-2168	Warnings loading{0}. {1}	CTC encountered warnings while loading the alarm profile import file.
WID-2169	One or more of the profiles selected do not exist on one or more of the nodes selected.	The profile selected does not exist on the node. Select another profile.
WID-2170	The profile list on node {0} is full. Please delete one or more profiles if you wish to add profile. {1}	The number of profile that can exist on a node has reached the limit. To add a profile, delete any of the existing profiles.
WID-2171	You have been logged out. Click OK to exit CTC.	Refer to warning message text.
WID-2172	The CTC CORBA (IIOP) listener port setting of {0} will be applied on the next CTC restart.	The Internet Inter-ORB Protocol (IIOP) listener port setting for the CTC Common Object Request Broker Architecture (CORBA) will be applied on the next CTC restart.
EID-2173	Port unavailable. The desired CTC CORBA (IIOP) listener port, {0}, is already in use or you do not have permission to listen on it. Please select an alternate port.	Select an alternate port, as the current port is either in use or you do not have enough permission on it.
EID-2174	Invalid number entered. Please check it and try again.	You entered an invalid firewall port number. Try again.
WID-2175	Extension byte mismatch. {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 warning message text.
WID-2178	Only one edit pane can be opened at a time. The existing pane will be displayed.	Refer to warning message text.
WID-2179	There is no update as the circuit has been deleted.	Refer to warning message text.
EID-2180	CTC initialization failed in step {0}.	CTC initialization has failed in the specified step.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
EID-2181	This link may not be included as it originates from the destination.	You must not include this link as it originates from destination of a circuit. It is against the path selection algorithm.
EID-2182	The value of {0} is invalid.	The value of the specified item is invalid.
EID-2183	Circuit roll failure. Current version of CTC does not support bridge and roll on a VCAT circuit.	Refer to error message text.
EID-2184	Cannot enable the STP on some ports because they have been assigned an incompatible list of VLANs. You can view the VLAN/Spanning Tree table or reassign ethernet ports VLANs.	Refer to error message text.
EID-2185	Cannot assign the VLANs on some ports because they are incompatible with the Spanning Tree Protocol. You can view the VLAN/Spanning Tree table or reassign VLANs.	Refer to error message text.
EID-2186	Software download failed on node {0}.	The software could not be downloaded onto the specified node.
EID-2187	The maximum length for the ring name that can be used is {0}. Please try again.	You must shorten the length of the ring name.
EID-2188	The nodes in this ring do not support alphanumeric IDs. Please use a ring ID between {0} and {1}.	The ring ID should not contain alphanumeric characters, and must be in the specified range.
EID-2189	TL1 keyword "all" can not be used as the ring name. Please provide another name.	Refer to error message text.
EID-2190	Adding this span will cause the ring to contain more nodes than allowed.	You have reached the maximum number of nodes allowed.
EID-2191	Ring name must not be empty.	You must supply a ring name.
EID-2192	Cannot find a valid route for the circuit creation request.	CTC could not complete the circuit creation request either because there are no physical links, or the bandwidth of the available links are already reserved.
EID-2193	Cannot find a valid route for the circuit drop creation request.	Refer to error message text.
EID-2194	Cannot find a valid route for the roll creation request.	Refer to error message text.
EID-2195	The circuit VLAN list cannot be mapped to one spanning tree. You can view the VLAN/Spanning Tree table or reassign VLANs.	Refer to error message text.
EID-2196	Unable to relaunch the CTC. {0}	There is an error relaunching CTC.
EID-2197	CORBA failure. Unable to proceed.	There was a CORBA failure, and the task cannot proceed. Verify the Java version.
EID-2198	Unable to switch to the {0} view.	CTC is unable to switch to the specified view.
EID-2199	Login failed on {0} {1}	The login failed on the specified tasks.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
EID-2200	CTC has detected a jar file deletion. The jar file was used to manage one or more nodes. This CTC session will not be able to manage those nodes and they will appear gray on the network map. It is recommended that you exit this CTC session and start a new one.	Refer to error message text.
EID-2202	Intra-node circuit must have two sources to be Dual Ring Interconnect.	Intranode circuit must have two sources to be a dual ring interconnect (DRI).
EID-2203	No member selected.	You must select a member.
EID-2204	Number of circuits must be a positive integer	The number of circuits cannot be zero or negative.
EID-2205	Circuit Type must be selected.	You must select a circuit type.
EID-2206	Unable to autoselect profile! Please select profile(s) to store and try again.	Refer to error message text.
EID-2207	You cannot add this span. Either the ring name is too big (i.e., ring name length is greater than {0}) or the endpoints do not support alphanumeric IDs.	Reduce the length of the ring name, or remove the 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 selected.	You must select a package name.
EID-2211	No node selected for upgrade.	You must select a node for the upgrade.
EID-2212	Protected Line is not provisionable.	The protected line cannot be provisioned. Choose another line.
WID-2213	The current type or state of some drops does not allow the new circuit state of {0} to be applied to them indirectly.	The circuit state, specified by {0} cannot be applied to the selected drops.
EID-2214	The node is disconnected. Please wait till the node reconnects.	Refer to error message text.
EID-2215	Error while leaving {0} page.	There was an error while leaving the specified page.
EID-2216	Error while entering {0} page.	There was an error while entering the specified page.
EID-2217	Some conditions could not be retrieved from the network view	Refer to error message text.
EID-2218	Bandwidth must be between {0} and {1} percent.	The bandwidth must be within the specified parameters.
EID-2219	Protection operation failed, XC loopback is applied on cross-connection.	As the protection operation failed, a cross-connect (XC) loopback will be applied on cross-connection.
EID-2220	The tunnel status is PARTIAL. CTC will not be able to change it. Please try again later	Refer to error message text.
EID-2221	Cannot find a valid route for the unprotected to {0} upgrade request.	Refer to error message text.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
EID-2222	One or more of the following nodes are currently part of a 4-fiber {0}. Only a single 4-fiber {0} is supported per node. {1}	The nodes, specified by {1}, are already part of a 4-fiber ring type, specified by {0}.
EID-2223	Only one circuit can be upgraded at a time.	Refer to error message text.
EID-2224	This link may not be included as it terminates on the source.	Refer to error message text.
EID-2225	No valid signal while trying to complete the roll. (0)	Roll can be completed only when a valid signal is detected. If not, the roll completion may result in an error.
EID-2226	Circuit roll failure. {0}	Refer to error message text.
EID-2320	This VCAT circuit does not support deletion of its member circuits.	You can not delete a circuit that is a member of VCAT circuit.
EID-2321	Error deleting member circuits. {0}	Refer to error message text.
WID-2322	Not all cross-connects from selected circuits could be merged into the current circuit. They may appear as partial circuits.	Refer to warning message text.
EID-2323	Circuit roll failure. Bridge and roll is not supported on a monitor circuit.	A monitor circuit does not support Bridge and Roll.
EID-2324	Circuit upgrade error. {0}	Refer to error message text.
EID-2325	You have failed {0} times to unlock this session. CTC will exit after you click OK or close this dialog box.	The maximum amount of attempts to unlock this session has been reached.
WID-2326	Currently, CTC does not support bridge and roll on circuits that are entirely created by TL1. To continue with bridge and roll in CTC, selected circuits must be upgraded. OK to upgrade selected circuits and continue bridge and roll operation?	Refer to warning message text.
WID-2327	Currently, CTC does not support bridge and roll on circuits that are partially created by TL1. To continue with bridge and roll in CTC, selected circuits must be upgraded. OK to upgrade selected circuits and continue bridge and roll operation?	Refer to warning message text.
EID-2328	Circuit reconfigure error. {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	Circuit verification: selected {0} invalid! {1}	The selected item, specified by {0}, is invalid as per the details, specified in {1}.
EID-2331	Deleting {0} may be service affecting.	Deleting the item can affect the service of CTC.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
EID-2332	Hold-off timer validation error in row [0]. {1} hold-off timer for {2} must be between {3}-10,000 ms, in steps of 100 ms.	Refer to error message text.
EID-3001	An Ethernet RMON threshold with the same parameters already exists. Please change one or more of the parameters and try again.	Change a few parameters in an Ethernet remote monitoring (RMON) threshold and try again.
EID-3002	Error retrieving defaults from the node: {0}	There was an error while retrieving the defaults from the specified node.
EID-3003	Cannot load file {0}.	CTC cannot load the specified file.
EID-3004	Cannot load properties from the node	Refer to error message text.
EID-3005	Cannot save NE Update values to file {0}	CTC cannot save the network element (NE) update values to the specified file.
EID-3006	Cannot load NE Update properties from the node	Refer to error message text.
EID-3007	Provisioning Error for {0}	There was a provisioning error for the specified item.
EID-3008	Not a valid Card	You cannot perform DWDM automatic node setup (ANS) from the Card view. Please navigate to the Node view and try again.
EID-3009	No {0} selected	Select the specified item, for example, VLAN, port, slot, etc.
EID-3010	Unable to create bidirectional optical link	Refer to error message text.
EID-3011	The file {0} doesn't exist or cannot be read.	The specified file does not exist or cannot be read.
EID-3012	The size of {0} is zero.	The size of the specified item is zero.
EID-3013	{0} encountered while restoring database.	The specified item was encountered while restoring the database.
EID-3014	The operation was terminated due to the following error: {0}	Refer to error message text.
EID-3015	{0} encountered while performing DB backup.	The specified item or condition was encountered while performing the DB backup.
EID-3016	Invalid subnet address.	Refer to error message text.
EID-3017	Subnet address already exists.	Refer to error message text.
EID-3018	Standby TSC not ready.	The standby Timing and Shelf Control card (TSC) not ready.
EID-3019	Incomplete internal subnet address.	Enter the complete internal subnet address.
EID-3020	TSC One and TSC Two subnet addresses cannot be the same.	A node's internal subnet must be different from one another as each TSC is on separate ethernet buses, isolated by broadcast domains.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
EID-3021	An error was encountered while retrieving the diagnostics: {0}	Refer to error message text.
EID-3022	Requested action not allowed.	The requested action is not allowed.
EID-3023	Unable to retrieve low order cross connect mode.	Refer to error message text.
EID-3024	Unable to switch {0} cross connect mode. Please verify that the type and/or number of circuits provisioned does not exceed the criterion for switching modes.	CTC cannot switch the cross-connect mode for the specified item, as the type or the number of circuits does not match with the criterion for switching modes.
EID-3025	Error while retrieving thresholds.	There was an error retrieving the thresholds.
EID-3026	Cannot modify send DoNotUse.	You cannot modify the Send DoNotUse field.
EID-3027	Cannot modify SyncMsg.	You cannot modify the SyncMsg field.
EID-3028	Cannot change port type.	You cannot change the port type.
EID-3029	Unable to switch to the byte because an overhead change is present on this byte of the port.	Refer to error message text.
EID-3031	Error hard-resetting card.	There was an error while resetting card hardware.
EID-3032	Error resetting card.	There was an error while resetting the card.
EID-3033	The lamp test is not supported on this shelf.	Refer to error message text.
EID-3035	The cross connect diagnostics cannot be performed	Refer to error message text.
EID-3036	The cross connect diagnostics test is not supported on this shelf.	The cross-connect diagnostics test is not supported on this shelf.
EID-3037	A software downgrade cannot be performed to the selected version while a SSXC card is inserted in this shelf. Please follow the steps to replace the SSXC with a CXC card before continuing the software downgrade.	Refer to error message text.
EID-3038	A software downgrade cannot be performed at the present time.	Refer to error message text.
EID-3039	Card change error.	There was an error while changing the card.
EID-3040	Invalid card type.	The selected card type is invalid.
EID-3041	Error applying changes.	CTC is unable to create a protection group. Check if the protect port supports circuits, a timing reference, SDH SRS-DCC, 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 error message text.
EID-3043	Error while retrieving line info settings.	Refer to error message text.
EID-3044	Error while retrieving line admin info settings.	Refer to error message text.
EID-3045	Error while retrieving transponder line admin info settings.	Refer to error message text.
EID-3046	The flow control water mark value must be between {0} and {1}, inclusive.	The flow control watermark value must be between the two specified values.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
EID-3047	The file named {0} could not be read. Please check the name and try again.	Refer to error message text.
EID-3048	There is no IOS startup config file available to download.	CTC could not find the configuration file for IOS startup.
EID-3049	There is an update in progress so the download cannot be done at this time.	Refer to error message text.
EID-3050	An exception was caught trying to save the file to your local file system.	Check whether the file already exists and cannot be over written, or there is a space constraint in the file system.
EID-3051	The maximum size for a config file in bytes is: {0}	The size of the configuration file should not exceed the specified number of bytes.
EID-3052	There was an error saving the config file to the TCC.	Refer to error message text.
EID-3053	The value of {0} must be between {1} and {2}	The value of the item must be between the specified values.
EID-3054	Cannot remove provisioned input/output ports or another user is updating the card, please try later.	Another user may be updating the card. You can try again later.
EID-3055	Cannot create soak maintenance pane.	Refer to error message text.
EID-3056	Cannot save defaults to file {0}	CTC cannot save the defaults to the specified file.
EID-3057	Cannot load default properties from the node.	Refer to error message text.
EID-3058	File {0} does not exist.	Refer to error message text.
EID-3059	Error encountered while refreshing.	There was an error while refreshing.
EID-3060	The ALS Recovery Pulse Interval must be between {0} seconds and {1} seconds.	The automatic laser shutdown (ALS) Recovery Interval must be between the specified range of seconds.
EID-3061	The ALS Recovery Pulse Duration must be between {0} seconds and {1} seconds.	The automatic laser shutdown (ALS) Recovery Duration must be between the specified range of seconds.
EID-3062	Error encountered while setting values.	Refer to error message text.
EID-3063	Unable to retriever bridge port settings.	Refer to error message text.
EID-3064	Not a G1000 Card.	This card is not a G1000-4 card.
EID-3065	An error was encountered while attempting to create RMON threshold: {0}	You must wait some time before you try again.
EID-3066	Minimum sample period must be greater than or equal to 10.	Refer to error message text.
EID-3067	Rising Threshold: Invalid Entry, valid range is from 1 to {0}	This is an invalid rising threshold entry. The valid range is from 1 to the specified value.
EID-3068	Falling Threshold: Invalid Entry, valid range is from 1 to {0}	This is an invalid falling threshold entry. The valid range is from 1 to the specified value.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
EID-3069	Rising threshold must be greater than or equal to falling threshold.	Refer to error message text.
EID-3070	Error in data for ports {0} Exactly one VLAN must be marked untagged for each port. These changes will not be applied.	CTC encountered data error for the specified ports. Only one VLAN should be marked untagged for each port.
EID-3071	Get Learned Address	Unable to retrieve the learned MAC address from the NE.
EID-3072	Clear Learned Address	Failure attempting to clear the learned MAC address from a specific card or Ether group.
EID-3073	Clear Selected Rows	Failure attempting to clear the learned MAC address from a specific card or Ether group.
EID-3074	Clear By {0}	Error encountered trying to clear the learned MAC address from either a VLAN or a port.
EID-3075	At least one row in param column needs to be selected.	Refer to error message text.
EID-3076	CTC lost its connection with this node. The NE Setup Wizard will exit.	Refer to error message text.
EID-3077	No optical link selected.	Refer to error message text.
EID-3078	Unable to create optical link.	Refer to error message text.
EID-3079	Cannot apply defaults to node: {0}	CTC cannot apply the defaults to the specified node.
EID-3080	Cannot go to the target tab {0}	CTC cannot go to the specified target tab.
EID-3081	Port type cannot be changed.	Refer to error message text.
EID-3082	Cannot modify the {0} extension byte.	You cannot modify the specified extension byte.
EID-3083	Error while retrieving stats.	Error in getting statistics.
EID-3084	Error encountered while trying to retrieve laser parameters for {0}	There is no card, or there was an internal communications error when attempting to get the laser parameters for the card.
EID-3085	No OSC Terminations selected	Select an OSC termination and proceed.
EID-3086	One or more Osc terminations could not be created.	Refer to error message text.
EID-3087	OSC termination could not be edited.	Refer to error message text.
EID-3088	No {0} card to switch.	No card of the specified type to switch.
EID-3089	Cannot use/change {0} state when {1} is failed or missing.	Cannot use or change the specified state when the card is failed or missing.
EID-3090	Cannot perform operation as {0} is {1}LOCKED_ON/LOCKED_OUT.	Cannot perform operation.
EID-3091	Cannot perform the operation as protect is active.	Refer to error message text.
EID-3092	Invalid service state. The requested action cannot be applied.	Select another service state and proceed.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
EID-3093	Cannot perform the operation as duplex pair is {0}locked.	Refer to error message text.
EID-3094	Cannot perform the operation as no XC redundancy is available.	You cannot perform the requested operation on the cross connect card without having a backup cross connect card.
EID-3095	Deletion failed since the circuit is in use	Refer to error message text.
WID-3096	Internal communication error encountered while trying to retrieve laser parameters. This can happen when equipment is not present or when equipment is resetting. Check the equipment state and try to refresh the values again.	Refer to warning message text.
EID-3097	The ring termination is in use.	The ring termination you are trying to access is in use. Try after sometime.
EID-3098	No ring terminations selected.	Select one of the ring terminations.
EID-3099	Sorry, entered key does not match existing authentication key.	Check the authentication key and reenter.
EID-3100	Error encountered during authentication.	There was an error in authentication. Verify that the key does not exceed the character limit.
EID-3101	DCC Metric is not in the range 1 - 65535.	The DCC metric should be in the range of 1 to 65535.
EID-3102	Invalid DCC Metric	There was an invalid DCC metric.
EID-3103	Invalid IP Address: {0}	The IP address is invalid.
EID-3104	Router priority is not in the range of 0 - 255	The router priority should be in the range of 0 to 255.
EID-3105	Invalid Router Priority	The router priority is invalid.
EID-3106	Hello Interval is not in the range of 1 - 65535	The hello interval should be in the range of 1 to 65535.
EID-3107	Invalid Hello Interval	The hello interval is invalid.
EID-3109	Invalid Dead Interval value. Valid range is 1 - 2147483647	The dead interval value must be between 1 and 2147483647.
EID-3110	Dead Interval must be larger than Hello Interval	Refer to error message text.
EID-3111	LAN transit delay is not in the range of 1 - 3600 seconds	The LAN transit delay should be in the range of 1 to 3600 seconds.
EID-3112	Invalid Transmit Delay	The transmit delay is invalid.
EID-3113	Retransmit Interval is not in the range 1 - 3600 seconds	The retransmit interval should be in the range of 1 to 3600 seconds.
EID-3114	Invalid Retransit Interval	The retransmit interval is invalid.
EID-3115	LAN Metric is not in the range 1 - 65535.	The LAN metric should be in the range of 1 to 65535.
EID-3116	Invalid LAN Metric	The LAN metric is invalid.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
EID-3117	If OSPF is active on LAN, no DCC Area Ids may be 0.0.0.0. Please change all DCC Area Ids to non-0.0.0.0 values before enabling OSPF on the LAN.	Refer to error message text.
EID-3118	If OSPF is active on LAN, LAN Area ID may not be the same as DCC Area Id.	LAN must be part of a different OSPF area other than the DCC network.
EID-3119	Validation Error	CTC was unable to validate the values entered by the user. This error message is common to several different provisioning tabs within CTC (examples include the SNMP provisioning tab, the General> Network provisioning tab, the Security > Configuration provisioning tab, etc.).
EID-3120	No object of type {0} selected to delete.	Choose an object of the specified type to delete.
EID-3121	Error Deleting {0}	There is an error deleting the item.
EID-3122	No object of type {0} selected to edit.	Choose an object of the specified type to edit.
EID-3123	Error Editing {0}	There was an error editing the item.
EID-3124	{0} termination is in use. Delete the associated OSPF Range Table Entry and try again	Refer to error message text.
EID-3125	No {0} Terminations selected.	No specified terminations are selected.
EID-3126	{0} termination could not be edited.	CTC could not edit the specified termination.
EID-3127	Unable to provision orderwire because E2 byte is in use by {0}.	Refer to error message text.
EID-3128	The authentication key may only be {0} characters maximum	The authentication key cannot exceed the specified number of characters.
EID-3129	The authentication keys do not match!	Refer to error message text.
EID-3130	Error creating OSPF area virtual link.	CTC encountered an error while creating the area virtual link.
EID-3131	Error creating OSPF virtual link.	CTC encountered an error creating the virtual link.
EID-3132	Error setting OSPF area range: {0}, {1}, false.	CTC encountered an error while setting the area range for the specified values.
EID-3133	Max number of OSPF area ranges exceeded.	OSPF area ranges exceeded the maximum number.
EID-3134	Invalid Area ID. Use DCC OSPF Area ID, LAN Port Area ID, or 0.0.0.0.	Refer to error message text.
EID-3135	Invalid Mask	Refer to error message text.
EID-3136	Invalid Range Address	The range address is invalid. Try again.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
EID-3137	Your request has been rejected because the timing source information was updated while your changes were still pending. Please retry.	Refer to error message text.
EID-3138	Invalid clock source for switching.	You have selected an invalid clock source. Choose another clock.
EID-3139	Cannot switch to a reference of inferior quality.	Refer to error message text.
EID-3140	Higher priority switch already active.	You cannot switch the timing source manually when a higher priority switch is already active.
EID-3141	Attempt to access a bad reference.	Refer to error message text.
EID-3142	No Switch Active.	None of the switches are active.
EID-3143	Error creating static route entry.	CTC encountered an error while a creating static route entry.
EID-3144	Max number of static routes exceeded.	The number of static routes has exceeded its limit.
EID-3145	RIP Metric is not in the range 1-15.	The Routing Information Protocol (RIP) metric should be in the range of 1 to 15.
EID-3146	Invalid RIP Metric	Refer to error message text.
EID-3147	Error creating summary address.	There was an error while creating the summary address.
EID-3148	No Layer 2 domain has been provisioned.	You must provision any one of the layer 2 domain.
EID-3149	Unable to retrieve MAC addresses.	Refer to error message text.
EID-3150	The target file {0} is not a normal file.	The specified target file is not a normal file.
EID-3151	The target file {0} is not writeable.	The target file is not writable. Specify another file.
EID-3152	Error creating Protection Group	CTC encountered an error creating Protection Group.
EID-3153	Cannot delete card, it is in use.	Cannot delete card. It is in use.
EID-3154	Cannot {0} card, provisioning error.	CTC cannot perform the task on the card.
EID-3155	Error Building Menu	CTC encountered an error building the menu.
EID-3156	Error on building menu (cards not found for {0} group)	CTC encountered an error while building the menu, as cards could not be found for the specified group).
EID-3157	Unable to set selected model: unexpected model class {0}	CTC encountered an unexpected model class while trying to complete the task.
EID-3158	Unable to switch, a similar or higher priority condition exists on peer or far-end card.	Refer to error message text.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
EID-3159[1]	Error applying operation.	CTC encountered an error while applying this operation.
EID-3160	{0} error encountered.	CTC encountered the specified error.
EID-3161	Ring Upgrade Error	An error was encountered while attempting to upgrade the BLSR. Refer to the details portion of the error dialog box for more information.
EID-3162	This protection operation cannot be set because the protection operation on the other side has been changed but not yet applied.	Refer to error message text.
EID-3163	Cannot validate data for row {0}	CTC cannot validate the data for the specified row.
EID-3164	New Node ID ({0}) for Ring ID {1} duplicates ID of node {2}	The new specified node ID for the specified ring ID is the same as another node ID.
EID-3165	The Ring ID provided is already in use. Ring IDs must be unique	Refer to error message text.
EID-3166	Error refreshing {0} table	CTC encountered an error while refreshing the specified table.
EID-3167	Slot already in use	Refer to error message text.
EID-3168	Provisioning Error	An error was encountered while attempting the specified provisioning operation. Refer to the details portion of the error dialog box for more information.
EID-3169	Error Adding Card	CTC encountered an error while adding the card.
EID-3170	Cannot delete card, {0}	Refer to error message text.
EID-3171	Error creating Trap Destination	CTC encountered an error creating the trap destination.
EID-3172	No RMON Thresholds selected	Select an RMON threshold.
EID-3173	The contact “{0}” exceeds the limit of {1} characters.	The specified contact exceeds the specified character limit.
EID-3174	The location “{0}” exceeds the limit of {1} characters.	The specified location exceeds the specified character limit.
EID-3175	The operator identifier “{0}” exceeds the limit of {1} characters.	The specified operator identifier exceeds the specified character limit.
EID-3176	The operator specific information “{0}” exceeds the limit of {1} characters.	The specified operator specific information exceeds the specified character limit.
EID-3177	The node name cannot be empty.	The specified name is empty.
EID-3178	The name “{0}” exceeds the limit of {1} characters.	The specified name exceeds the specified character limit.
EID-3179	Protect card is in use.	Refer to error message text.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
EID-3180	1+1 Protection Group does not exist.	Create a 1+1 protection group.
EID-3181	Y Cable Protection Group does not exist.	Refer to error message text.
EID-3182	The Topology Element is in use and cannot be deleted as requested	You cannot delete the topology element which is in use.
EID-3183	Error Deleting Protection Group	CTC encountered an error while deleting the protection group.
EID-3184	No {0} selected.	You must select an item before completing this task.
EID-3185	There is a protection switch operation on this ring. Therefore, it cannot be deleted at this time.	Refer to error message text.
EID-3186	Busy: {0} is {1} and cannot be deleted as requested.	The request cannot be completed.
EID-3187	Error deleting trap destination.	CTC encountered an error deleting the trap destination.
EID-3214	Could not get number of HOs for line.	The number of High Orders for line is not available.
EID-3215	Error in refreshing.	Used frequently in pane classes to indicate a general error condition when trying to refresh from the model.
EID-3216	Invalid proxy port.	Refer to error message text.
EID-3217	Could not refresh stats.	CTC could not refresh statistics values.
EID-3218	Unable to launch automatic node setup.	Refer to error message text.
EID-3219	Unable to refresh automatic node setup information.	Failure trying to retrieve automatic node setup information.
EID-3220	Error refreshing row {0}	Error refreshing the specified row.
EID-3222	Could not clear stats.	Refer to error message text.
EID-3223	Error cancelling software upgrade.	CTC encountered an error while cancelling the upgrade. Software is not upgraded.
EID-3224	Error accepting load.	Refer to error message text.
EID-3225	Error while refreshing pane.	Used frequently in pane classes to indicate a general error condition when trying to refresh from the model.
EID-3226	{0} termination(s) could not be deleted. {1}	Refer to error message text.
EID-3227	Unable to record a baseline, performance metrics will remain unchanged.	CTC failed to set the baseline values while provisioning NE. Previous values remain unchanged.
EID-3228	{0} termination(s) could not be created. {1}	Refer to error message text.
EID-3229	RIP is active on the LAN. Please disable RIP before enabling OSPF.	Turn off the Routing Information Protocol (RIP) on the LAN, before enabling OSPF.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
EID-3230	OSPF is active on the LAN. Please disable OSPF before enabling RIP.	Turn off the OSPF on the LAN before enabling RIP.
EID-3231	Error in Set OPR	An error was encountered while attempting to provision the optical power received (OPR).
WID-3232	Cannot transition port state indirectly because the port is still providing services: if the port state should be changed, edit it directly via port provisioning.	Edit the port state while provisioning the port.
EID-3233	Current loopback provisioning does not allow this state transition.	Refer to error message text.
EID-3234	Current synchronization provisioning does not allow this state transition	You cannot transition the port state to the target date while in the current synchronization state.
EID-3235	Cannot perform requested state transition on this software version.	Refer to error message text.
EID-3236	Database Restore failed. {0}	CTC failed to restore the specified database.
EID-3237	Database Backup failed. {0}	CTC failed to backup the specified database.
EID-3238	Send PDIP setting on {0} is inconsistent with that of control node {1}	The send payload defect indicator path (PDI-P) setting on the specified item should be consistent with that of the specified control node.
EID-3239	The overhead termination is invalid	Refer to error message text.
EID-3240	The maximum number of overhead terminations has been exceeded.	Overhead terminations have exceeded the limit.
EID-3241	The {0} termination port is in use.	The specified termination port is in use. Select another port.
EID-3242	{1} exists on the selected ports. Please create {0} one by one.	The specified DCC already exists on the selected port. You may create a DCC of another type.
WID-3243	The port you have chosen as an {0} endpoint already supports an {1}. The port cannot support both DCCs. After the {0} is created, verify that no EOC alarms are present and then delete the {1} to complete the downgrade.	The same port can not be used by multiple DCCs.
EID-3244	{0} exists on the selected ports. Please create {1} one by one.	The specified DCC already exists on the selected port. You may create a DCC of another type.
WID-3245	The port you have chosen as an {1} endpoint already supports an {0}. The port cannot support both DCCs. After the {1} is created, verify that no EOC alarms are present and then delete the {0} to complete the upgrade.	The port selected as a DCC endpoint already supports another DCC. Refer to warning message text.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
EID-3246	Wizard unable to validate data: {0}	CTC encountered an error.
EID-3247	Ordering error. The absolute value should be {0}	The absolute value entered was wrong.
EID-3248	Wrong parameter is changed: {0}	CTC changed the incorrect parameter.
EID-3249	Invalid voltage increment value.	Refer to error message text.
EID-3250	Invalid power monitor range.	Refer to error message text.
EID-3251	Unable to complete requested action. {0}	CTC could not complete the specified action.
EID-3252	No download has been initiated from this CTC session.	Refer to error message text.
EID-3253	Reboot operation failed. {0}	Refer to error message text.
EID-3254	Validation Error. {0}	The Cisco Transport Controller (CTC) was unable to validate the values entered by the user, specified by {0}. This error message is common to several different provisioning tabs within the CTC.
EID-3255	Cannot change timing configuration, manual/force operation is performed.	Refer to error message text.
WID-3256	Could not assign timing reference(s) because - at least one timing reference has already been used and/or - a timing reference has been attempted to be used twice. Please use the “Reset” button and verify the settings.	Refer to warning message text.
EID-3257	Duplicate DCC number detected: {0}.	CTC detected more than one occurrence of the a DCC number. Remove one of them.
EID-3258	There was a software error attempting to download the file. Please try again later.	Refer to error message text.
EID-3259	Create FC-MR Threshold	You must create a Fibre Channel Multirate (FC_MR) card threshold.
EID-3260	An error was encountered while provisioning the internal subnet: {0}	The specified internal subnet could not be provisioned.
EID-3261	The port rate provisioning cannot be changed while circuits exist on this port.	Refer to error message text.
EID-3262	The port provisioning cannot be changed when the port status is not OOS.	You must provision the ports only when the port is Out of Service.
WID-3263	You are using Java version {0}. CTC should run with Java version {1}. It can be obtained from the installation CD or http://java.sun.com/j2se/	CTC is being launched with the wrong version of the JRE {0}. This version of CTC requires a particular version of the JRE {1}. The CTC and browser must be closed and restarted to allow the correct Java version to be loaded.
EID-3264	The port provisioning cannot be changed while the port is {0}.	You must modify the port provisioning only when the port is out of service.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
EID-3265	Error modifying Protection Group	Protection Group could not be modified.
EID-3266	Conditions could not be retrieved from the shelf or card view.	Refer to error message text.
WID-3267	Cannot edit XTC protection group.	Refer to warning message text.
WID-3268	Invalid entry. {0}	The specified entry is invalid.
WID-3269	{0} was successfully initiated for {1} but its completion status was not able to be obtained from the node. {0} may or may not have succeeded. When the node is accessible, check its software version.	Refer to error message text.
WID-3270	The file {0} does not exist.	The specified file does not exist.
WID-3271	The value entered must be greater than {0}.	The value entered must be greater than the specified value.
WID-3272	Entry required	An entry is required to complete this task.
WID-3273	{0} already exists in the list.	The specified item already exists in the list.
WID-3274	A software upgrade is in progress. Network configuration changes that results a node reboot can not take place during software upgrade. Please try again after software upgrade is done.	Refer to warning message text.
WID-3275	Make sure the Remote Interface ID and the Local Interface ID on the two sides are matched. (Local Interface ID on this node should equal Remote Interface ID on the neighbor node and vice-versa.)	Refer to warning message text.
WID-3276	Both {0} and {1} exist on the same selected port. {2}	The specified port has both SDCC and LDCC.
WID-3277	The description cannot contain more than {0} characters. Your input will be truncated.	The input exceeds the character limit. The value will be truncated to the maximum character limit.
WID-3279	Card deleted, returning to shelf view.	CTC returns to node view.
WID-3280	ALS will not engage until both the protected trunk ports detect LOS.	Refer to warning message text.
WID-3281	A software upgrade is in progress. {0} can not proceed during a software upgrade. Please try again after the software upgrade has completed.	Refer to warning message text.
WID-3282	Performing a software upgrade while TSC 5 is active could result in a service disruption. It is recommended that you make TSC 10 the active TSC by performing a soft reset of TSC 5. The following 15600s are currently unsafe to upgrade...	Refer to warning message text.
WID-3283	Before activating a new version, make sure you have a database backup from the current version.	Refer to warning message text.
WID-3284	Reverting to an older version.	CTC is being reverted to an older version of application.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
WID-3285	Applying FORCE or LOCKOUT operations may result in traffic loss.	Refer to warning message text.
WID-3286	The ring status is INCOMPLETE. CTC cannot determine if there are existing protection operations or switches in other parts of the ring. Applying a protection operation at this time could cause a traffic outage. Please confirm that no other protection operations or switches exist before continuing.	Refer to warning message text.
WID-3287	There is a protection operation or protection switch present on the ring. Applying this protection operation now will probably cause a traffic outage.	Refer to warning message text.
WID-3288	This ring status is INCOMPLETE. CTC will not be able to apply this change to all of the nodes in the {0}.	Change the ring status to apply the change to all nodes in the ring type.
EID-3290	Unable to delete specified provisionable patchcord(s).	Refer to error message text.
EID-3291	Cannot change revertive behavior due to an active protection switch.	Protection switch should not be active to change the revertive behavior.
EID-3292	Error resetting shelf.	CTC encountered an error while resetting the node.
EID-3293	No such provisionable patchcord.	You are attempting to delete a provisionable patchcord that does not exist. This happens when multiple instances of CTC are running and attempting to delete the same provisionable patchcord concurrently.
EID-3294	No RMON thresholds available for selected port.	Refer to error message text.
EID-3295	This card does not support RMON thresholds.	Refer to error message text.
EID-3296	Buffer-to-buffer credit is only supported for Fibre Channel (FC) and FICON.	Refer to error message text.
EID-3298	ALS Auto Restart is not supported by this interface.	Refer to error message text.
EID-3300	Can not have duplicate OSPF area IDs.	OSPF area IDs should be unique.
EID-3301	LAN metric may not be zero.	Refer to error message text.
EID-3302	Standby {0} not ready.	Standby controller card is not ready.
EID-3303	DCC Area ID and {0} conflict. {1}	DCC Area ID and ring type, specified by {0}, conflict each other due to the details specified by {1}.
EID-3304	DCC number is out of range.	Enter a DCC number that is within the range
EID-3305	Can not have OSPF turned on on the LAN interface and the back bone area set on a DCC interface.	You cannot have the default OSPF area on a DCC while OSPF is enabled on the LAN.
EID-3306	Ethernet circuits must be bidirectional.	Refer to error message text.
EID-3307	Error while creating connection object at {0}.	CTC encountered an error at the specified connection while creating the connection.
EID-3308	DWDM Link can be used only for optical channel circuits.	Refer to error message text.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
EID-3309	OCH-NC circuit: link excluded - wrong direction.	The optical channel (circuit) does not allow the specified link to be included because it is in the wrong optical direction.
EID-3310	DWDM Link does not have wavelength available.	Refer to error message text.
EID-3311	Laser already on.	Refer to error message text.
EID-3312	Unable to change the power setpoint {0} {1}	CTC cannot change the power setpoint. The new setpoint would either make the thresholds inconsistent or set the fail threshold outside the range.
EID-3313	Unable to modify offset. Amplifier port is in service state.	Refer to error message text.
EID-3314	Requested action not allowed. Invalid state value.	Refer to error message text.
EID-3315	Unable to perform operation.	CTC is unable to perform operation.
EID-3316	Wrong node side.	This task was applied to the wrong node side.
EID-3317	Name too long.	Reduce the number of characters in the name.
EID-3318	Illegal name.	The name you entered is illegal.
EID-3319	Wrong line selection.	Select another line
EID-3320	Unable to delete optical link.	CTC cannot delete the optical link.
EID-3321	This feature is unsupported by this version of software.	Refer to error message text.
EID-3322	Equipment is not plugged-in.	Plug-in the equipment and proceed.
EID-3323	APC system is busy.	Automatic Power Control (APC) system is busy.
EID-3324	No path to regulate.	There is no circuit path to regulate.
EID-3325	Requested action not allowed.	Generic DWDM provisioning failure message.
EID-3326	Wrong input value.	The input value is incorrect.
EID-3327	Error in getting thresholds.	There was an error retrieving the thresholds. This message is displayed only for the OSCM/OSC-CSM line thresholds.
EID-3328	Error applying changes to row {0}.Value out of range.	There was an error applying the changes to the specified row. The value is out of range.
EID-3330	Unable to switch to the byte because an overhead channel is present on this byte of the port.	Refer to error message text.
EID-3331	Error applying changes to row.	Refer to error message text.
EID-3334	Cannot change timing parameters on protect port.	You cannot change timing parameters on protect port.
EID-3335	The type of this port cannot be changed: SDH validation check failed. Check if this port is part of a circuit, protection group, SONET DCC, orderwire, or UNI-C interface.	Refer to error message text.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
EID-3336	Error on reading a control mode value.	The Control Mode must be retrieved.
EID-3337	Error on setting a set point gain value.	The Gain Set Point must be set.
EID-3338	Error on reading a set-point gain value.	The Gain Set Point must be retrieved.
EID-3339	Error on setting a tilt calibration value.	The tilt calibration must be set.
EID-3340	Error on setting expected wavelength.	The expected wavelength must be set.
EID-3341	Error on reading expected wavelength.	The expected wavelength must be retrieved.
EID-3342	Error on reading actual wavelength.	The actual wavelength must be retrieved.
EID-3343	Error on reading actual band.	The actual band must be retrieved.
EID-3344	Error on reading expected band.	The expected band must be retrieved.
EID-3345	Error on setting expected band.	The expected band must be set.
EID-3346	Error retrieving defaults from the node: {0}.	There was an error retrieving defaults from the specified node.
EID-3347	Cannot load file {0}.	CTC cannot load the specified file.
EID-3348	Cannot load properties from the node.	Refer to error message text.
EID-3349	Cannot save NE Update values to file.	Check your file system for space constraint or any other problem.
EID-3350	Cannot load NE Update properties from the node:	Refer to error message text.
EID-3351	File {0} does not exist.	The specified file does not exist.
EID-3352	Error on setting value at {0}.	There was an error while setting the value at the specified location.
EID-3353	There is no such interface available.	The interface specified is not present in CTC.
EID-3354	Specified endpoint is in use.	Select another endpoint that is not in use.
EID-3355	Specified endpoint is incompatible.	Refer to error message text.
EID-3357	Unable to calculate connections.	Refer to error message text.
EID-3358	Optical link model does not exist for specified interface.	Create an optical linkmodel for the interface, and proceed.
EID-3359	Unable to set optical parameters for the node.	Refer to error message text.
EID-3361	Ring termination is in use. Error deleting ring termination	You cannot delete a ring in use.
EID-3362	Error deleting ring termination.	There was an error while deleting ring termination.
EID-3363	No ring terminations selected.	You must select a ring termination.
EID-3364	Error creating ring ID.	There was an error while creating the ring ID.
EID-3365	OSC termination is in use.	Select another optical service channel (OSC) which is not in use.
EID-3366	Unable to delete OSC termination.	There was an error deleting the OSC termination.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
EID-3370	No optical link has been selected	You must select an optical link.
EID-3371	Error while calculating automatic optical link list.	Refer to error message text.
EID-3372	Attempt to access an OCH-NC connection that has been destroyed.	CTC destroyed an external attempt to access an optical channel network connection.
EID-3375	Expected span loss must be set.	Refer to error message text.
EID-3376	Unable to retrieve measured span loss.	Refer to error message text.
EID-3377	Wrong interface used.	The interface used for the card is wrong.
EID-3378	Duplicate origination patchcord identifier.	The provisionable patchcord identifier to the patchcord you are attempting to provision is already in use by another patchcord on the origination node.
EID-3379	Duplicate termination patchcord identifier.	The provisionable patchcord identifier to the patchcord you are attempting to provision is already in use by another patchcord on the remote node.
EID-3380	Unable to locate host.	Refer to error message text.
EID-3381	Maximum Frame size must be between {0} and {1} and may be increased in increments of {2}.	The frame size must be in the specified range. This can incremented by the specified value.
EID-3382	Number of credits must be between {0} and {1}.	The number of credits must be between the specified values.
EID-3383	GFP Buffers Available must be between {0} and {1} and may be increased in increments of {2}.	The GFP buffers must be in the specified range. This can incremented by the specified value.
WID-3384	You are about to force the use of Secure Mode for this chassis. You will not be able to undo this operation. OK to continue?	Refer to warning message text.
EID-3385	{0}. Delete circuits, then try again.	Refer to error message text.
EID-3386	Unable to provision transponder mode: {0}	The specified transponder mode cannot be provisioned.
EID-3387	You must change port{0} to an out-of-service state before changing card parameters. Click Reset to revert the changes.	All the card ports should be changed to out-of-service before changing the parameters.
EID-3388	Unable to change the card mode because the card has circuits.	Refer to error message text.
EID-3389	Error encountered while changing the card mode.	Refer to error message text.
EID-3390	Port is in use.	Refer to error message text.
EID-3391	Unable to change the port rate because the port has been deleted.	You cannot change the port rate of a card that has been deleted.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
WID-3392	Could not assign timing reference(s) because - with external timing, only a single protected, or two unprotected timing references per BITS Out may be selected. Please use the "Reset" button and verify the settings.	Refer to warning message text.
WID-3393	Could not assign timing reference(s) because - with line or mixed timing, only a single unprotected timing reference per BITS Out may be selected. Please use the "Reset" button and verify the settings.	Refer to warning message text.
EID-3394	Error refreshing Power Monitoring values.	Refer to error message text.
EID-3395	Invalid Configuration: {0}	CTC encountered an error in IP address, net mask length, or default router, or a restricted IIOP port was selected.
EID-3396	Invalid Configuration: The standby controller card is not a TCC2P card.	The standby controller card should be a TCC2P card.
EID-3397	Wrong version for file {0}.	The specified file is of wrong version.
EID-3398	Cannot delete PPM.	Refer to error message text.
EID-3399	Cannot delete PPM. It has port(s) in use.	Remove the ports connected to the Pluggable Port Module before it can be deleted.
EID-3400	Unable to switch, force to Primary Facility not allowed.	Refer to error message text.
EID-3401	{0} cannot be provisioned for the port while {1} is enabled.	The relationship between parameters {0} and {1} are such that enabling either one, prevents the provisioning of the other.
EID-3402	Unable to complete the switch request. The protect card is either not present or is not responding. Try again after ensuring that the protect card is present and is not resetting.	Refer to error message text.
EID-3403	Admin state transition has not been attempted on the monitored port.	Refer to error message text.
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 error message text.
EID-4000	The {0} ring name cannot be changed now. A {0} switch is active.	You cannot change the ring name because a switch of the same ring type is active.
EID-4001	The {0} ring ID cannot be changed now. A {0} switch is active.	You cannot change the ring ID because a switch of the same ring type is active.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or 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 7.0.0 before, reverting will restore the 7.0.0 provisioning, losing any later provisioning. If the node was running some other version, reverting will LOSE ALL PROVISIONING. Also, any FPGA downgrades that occur while reverting might affect traffic. OK to continue?	Refer to warning message text.
EID-5000	Cannot find a valid route for tunnel change request.	Refer to error message text.
EID-5001	Tunnel could not be changed.	Refer to error message text.
EID-5002	Tunnel could not be restored and must be recreated manually.	Refer to error message text.
EID-5003	Circuit roll failure. {0}	Refer to error message text.
EID-5004	There is already one 4F {0} provisioned on the set of nodes involved in {1}. The maximum number of 4F {0} rings has been reached for that node.	There is already one 4F BLSR provisioned on the set of nodes involved in the ring. The maximum number of 4F BLSR rings has been reached for that node.
WID-5005	A non-zero hold-off time can violate switching time standards, and should only be used for a circuit with multiple path selectors.	Refer to warning message text.
WID-5006	Warning: Different secondary {0} node should only be used for DRI or Open-ended path protected circuits.	You should use different secondary end point only for DRI or open-ended path protected circuits.
WID-5007	If you change the scope of this view, the contents of this profile editor will be lost.	Refer to warning message text.
WID-5008	Please make sure all the protection groups are in proper state after the cancellation.	Refer to warning message text.
WID-5009	Circuit {0} not upgradable. No {1} capable {2}s are available at node {3}.	No VT capable STSs are available at the node.
EID-5010	Domain name already exists.	Refer to error message text.
EID-5011	Domain name may not exceed {0} characters.	You may have reached the maximum number of characters.
WID-5012	Software load on {0} does not support the addition of a node to a 1+1protection group.	Refer to warning message text.
EID-5013	{0} doesn't support Bridge and Roll Feature. Please select a different port.	The specified port does not support Bridge and Roll.
EID-5014	An automatic network layout is already in progress, please wait for it to complete for running it again.	You must for the automatic network layout to complete before running it again.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
WID-5015	{0} cannot be applied to {1}.	You cannot apply the admin state operation, specified by {0}, to port count, specified by {1}.
EID-5016	An error was encountered while attempting to provision the {0}. {1}	CTC encountered an error while provisioning the card.
EID-5017	Unable to rollback provisioning, the {0} may be left in an INCOMPLETE state and should be manually removed.	You may have to remove the BLSR manually as it was left incomplete.
EID-5018	{0} is {1} node and cannot be added to {2} network.	You cannot add the node {0} of type {1} to the host node of type {2}. This prevents you from hosting both SONET and SDH nodes in the same session.
EID-5019	Manual mode for this equipment does not support an expected string consisting of all null characters. Please change the expected string or the path trace mode.	The path trace mode does not support strings that consist of null characters. You must either change the expected string or the path trace mode.
WID-5020	Unable to transition port state indirectly because the port aggregates low order circuits: if the port state should be changed, edit it directly via port provisioning	Refer to warning message text.
EID-5021	No nodes are selected. Please choose a node.	Refer to error message text.
WID-5022	Warning: Ethergroup circuits are stateless (i.e., always in service). Current state selection of {0} will be ignored.	Refer to warning message text.
EID-5023	Unable to communicate with node. Operation failed.	CTC encountered a network communication error. Connectivity between CTC and the NE was disrupted, either transiently or permanently.
EID-5024	Overhead circuit will not be upgraded.	Refer to error message text.
WID-5025	The path targeted for this switch request is already active. The switch request can be applied, but traffic will not switch at this time.	Refer to warning message text.
EID-5026	A 15600 cannot serve as the primary or secondary node in a 4 Fiber {0} circuit. Please change your ring and/or node selections so that a 15600 is not chosen as the primary or secondary node in this 4 Fiber {1} circuit.	Refer to error message text.
WID-5027	The {0} Edit Window for {1} has been closed due to significant provisioning changes. These changes may only be transitory, so you may re-open the {0} Edit Window to view the updated state.	Re-open the BLSR/MS-SPRing edit window to view the updated state of the node.
WID-5028	Warning: This operation should only be used to clean up rolls that are stuck. It may also affect completeness of the circuit. Continue with deletion?	Refer to warning message text.
EID-5033	Unable to load profile. Error decoding characters.	CTC detected an error while decoding characters and could not load the profile.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
EID-5034	Unable to load profile. File format error.	CTC detected an error and could not load the profile.
EID-5035	Unable to load profile. File read error.	CTC could not read the file ad hence not able to load the profile.
EID-5036	The GNE Host Name {0} is invalid.	The specified host name is invalid. CTC could not resolve the host name to any valid IP address.
EID-5039	Provisionable patchcords created between transponder trunk ports and mux/demux 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-6000	Platform does not support power monitoring thresholds	Refer to error message text.
EID-6001	One of the XC cards has failures or is missing.	Check whether all the cross connect cards are installed and are working.
EID-6002	One of the XC cards is locked.	Unlock the cross connect card.
EID-6003	Unable to create OSC termination. Ring ID already assigned.	Enter a new ID for the ring and proceed.
EID-6004	Unable to perform a system reset while a BLSR ring is provisioned on the node.	Remove the BLSR ring from the node and proceed with the reset procedure.
EID-6005	Could not assign timing references: - 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 error message text.
EID-6006	Could not assign timing references: - NE reference can only be used if timing mode is LINE. - A BITS reference can only be used if timing mode is not LINE. - A line reference can only be used if timing mode is not EXTERNAL.	Refer to error message text.
WID-6007	Cancelling a software upgrade during standby TSC clock acquisition may result in a traffic outage.	Refer to warning message text.
EID-6008	SF BER and SD BER are not provisionable on the protect line of a protection group.	SF BER and SD BER cannot be provisioned in a protect card as these values are inherited by the protect card or group from the card for which it is offering protection.
WID-6009	If Autoadjust GFP Buffers is disabled, GFP Buffers Available must be set to an appropriate value based on the distance between the circuit end points.	Refer to warning message text.
WID-6010	If Auto Detection of credits is disabled, Credits Available must be set to a value less than or equal to the number of receive credits on the connected FC end point.	Refer to warning message text.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
WID-6011	Idle filtering should be turned off only when required to operate with non-Cisco Fibre Channel/FICON-over-SONET equipment.	Refer to warning message text.
EID-6012	Could not change the retiming configuration. There are circuits on this port.	You cannot change the timing configuration on this port unless the circuits on this port are deleted.
EID-6013	NTP/SNTP server could not be changed. {1}	Refer to error message text.
EID-6014	Operation failed. The reference state is OOS.	Change the Out-of-service state to Active.
EID-6015	Distance Extension cannot be disabled if the port media type is FICON 1Gbps ISL or FICON 2Gbps ISL.	Refer to error message text.
EID-6016	Card mode cannot be changed to Fibre Channel Line Rate if the port media type is FICON 1Gbps ISL or FICON 2Gbps ISL.	Refer to error message text.
EID-6017	The destination of a {0} route cannot be a node IP address.	A node IP address cannot be the destination for a static route.
EID-6018	The destination of a {0} route cannot be the same as the subnet used by the node.	Refer to error message text.
EID-6019	The destination of a static route cannot be 255.255.255.255	The network address such as 255.255.255.255 is not valid. Enter a valid address.
EID-6020	The destination of a static route cannot be the loopback network (127.0.0.0/8)	Refer to error message text.
EID-6021	The subnet mask length for a non-default route must be between 8 and 32.	Length of subnet mask must be within the specified range.
EID-6022	The subnet mask length for a default route must be 0.	Refer to error message text.
EID-6023	The destination of a {0} route cannot be an internal network{1}.	The destination of a static route must not be an internal network.
EID-6024	The destination of a {0} route cannot be a class D (224.0.0.0/4) or class E (240.0.0.0/4) address.	The destination of a static route must not be a class D or class E address.
EID-6025	The destination of a {0} route cannot be a class A broadcast address (x.255.255.255/8)	The destination of a static route must not be a class A broadcast address. It should be (xxx.0.0.0).
EID-6026	The destination of a {0} route cannot be a class B broadcast address (x.x.255.255/16)	The destination of a static route must not be a class B broadcast address.
EID-6027	The destination of a {0} route cannot be a class C broadcast address (x.x.x.255/24)	The destination of a static route must not be a class C broadcast address.
EID-6028	The destination of a {0} route cannot be the subnet broadcast address associated with a node IP address.	The destination of a static route must not be a subnet broadcast address of a node IP.
EID-6029	The next hop of a static route cannot be the same as the destination of the route or an internal network{0}.	Static route must have the default route as the next hop, and not destination of the route or internal network.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
EID-6030	The next hop of a static default route must be the provisioned default router.	The default route is selected for networks that do not have a specific route.
EID-6031	No more static routes can be created.	You have reached the maximum number of static routes.
EID-6032	This static route already exists.	Refer to error message text.
EID-6033	Previous operation is still in progress.	Another operation is in progress. You must try after sometime.
EID-6035	Parent entity does not exist.	Refer to error message text.
EID-6036	Parent PPM entity does not exist.	Create a parent entity for PPM.
EID-6037	Equipment type is not supported.	CTC does not support this equipment.
EID-6038	Invalid PPM port.	Refer to error message text.
EID-6039	Card is part of a regeneration group.	Select another card.
EID-6040	Out of memory.	Refer to error message text.
EID-6041	Port is already present.	Refer to error message text.
EID-6042	Port is used as timing source.	Choose another port as the selected port is being used as timing source.
EID-6043	DCC or GCC is present.	Refer to error message text.
EID-6044	Card or port is part of protection group.	Refer to error message text.
EID-6045	Port has overhead circuit(s).	Refer to error message text.
EID-6046	G.709 configuration is not compatible with data rate.	Refer to error message text.
EID-6047	Port cannot be deleted because its service state is OOS-MA,LPBK&MT.	To delete the port, you must change the port state to OOS-DSBLD.
EID-6048	{0} is {1}.	Trunk port is in the wrong state to carry out the action.
EID-6049	Mode {0} is not supported.	CTC does not support the mode of operation requested on the card.
EID-6050	Some {0} terminations were not {1}d. {2}	Refer to error message text.
WID-6051	All {0} terminations were {1}d successfully. {2}	Refer to 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 invalid as the receiver of SNMP traps
EID-6055	The IP address is already in use.	Refer to error message text.
EID-6056	Invalid SNMP trap destination. {0}	The specified SNMP trap destination is invalid. Choose another destination.
WID-6057	Changing the card mode will result in an automatic reset.	Refer to warning message text.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
EID-6058	Max number of GRE tunnels exceeded.	Refer to error message text.
EID-6059	The specified GRE tunnel already exists!	Specify another GRE tunnel.
EID-6060	Cannot {0} GRE tunnel entry: {1}.	Refer to error message text.
EID-6061	Error deleting GRE tunnel entry.	CTC encountered an error while deleting the GRE tunnel entry.
EID-6062	Selected GRE tunnel does not exist.	Create a GRE tunnel and proceed.
EID-6063	Selected router does not exist.	Create a router and proceed.
EID-6064	MAA address list is full.	Refer to error message text.
EID-6065	Selected area address is duplicated.	Enter another area address.
EID-6066	Primary area address can not be removed.	Refer to error message text.
EID-6067	Selected area address does not exist.	Choose another area address.
EID-6068	The GRE NSEL may not be modified while there are GRE Tunnel Routes provisioned.	You can not change the NSEL address if there are tunnels provisioned.
EID-6069	The node is currently in ES mode. Only router #1 may be provisioned.	An End System needs only one provisioned router.
EID-6070	No router selected.	Select a router.
EID-6071	Cannot flush TARP data cache.	You cannot flush the cache in the Tunnel identifier Address Resolution Protocol (TARP) state.
EID-6072	Cannot add TARP data cache entry: {0}	You cannot add the specified cache entry.
WID-6073	TARP request has been initiated. Try refreshing TARP data cache later.	Refer to warning message text.
EID-6074	End System mode only supports one subnet.	Refer to error message text.
EID-6075	Trying to remove MAT entry that does not exit.	CTC is removing the non-existent MAT entry.
EID-6076	Cannot {0} TARP manual adjacency entry: {1}	CTC can not add the specified adjacency entry for reasons unknown.
EID-6077	Area address shall be 1 to 13 bytes long.	Area address should not be more than 13 characters.
EID-6078	TDC entry with TID {0} does not exist in the table.	The specified Tunnel Identifier does not exist.
EID-6079	Unable to remove TDC entry with TID {0}. Please verify that TARP is enabled.	You must enable TARP in order to remove the TDC entry.
WID-6080	Router #{0} does not have an area address in common with router #1. Switching from IS L1/L2 to IS L1 in this case will partition your network.	Refer to warning message text.
EID-6081	The limit of 10 RADIUS server entries has been reached.	CTC does not allow more than 10 RADIUS servers.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
EID-6082	{0} cannot be empty.	The Shared Secrets field should not be empty.
EID-6083	The entry you selected for editing has been altered by other. Changes cannot be committed.	Refer to error message text.
EID-6084	The RADIUS server entry already exists.	Specify another RADIUS server entry.
WID-6085	Disabling shell access will prevent Cisco TAC from connecting to the vxWork shell to assist users.	Refer to warning message text.
EID-6086	Cannot change card. Card resources are in use.	The card you are trying to remove is being used. Cannot change the card.
EID-6087	Cannot change card. The new card type is invalid or incompatible.	Refer to error message text.
EID-6088	This line cannot be put into loopback while it is in use as a timing source	Refer to error message text.
EID-6089	Interface not found. {0}	CTC cannot find the specified interface.
EID-6090	Interface type not valid for operation. {0}	Choose another interface.
EID-6091	The interface's current state prohibits this operation. {0}	The port is in an invalid state to set loopback.
EID-6092	Operation prohibited for this interface. {0}	CTC does not allow this operation for the specified interface.
EID-6093	Max number of Tarp Data Cache entry exceeded.	You have exceeded the allowed number of characters.
EID-6094	Max number of Manual Adjacency Table entry exceeded.	Refer to error message text.
EID-6095	Invalid Ais/Squelch mode.	Refer to error message text.
EID-6096	Default GRE tunnel route is only allowed on a node without a default static route and a default router of 0.0.0.0	Refer to error message text.
EID-6097	The authorization key does not comply with IOS password restrictions. {0}	Specify another authorization key.
EID-6098	Default static route is not allowed when default GRE tunnel exists	Refer to error message text.
EID-6099	You cannot create a subnet on a disabled router.	Create the subnet on an active router.
WID-6100	Disabling a router that has a provisioned subnet is not recommended.	Refer to warning message text.
EID-6101	The MAT entry already exists.	Refer to error message text.
WID-6102	The new card has less bandwidth than the current card. Circuits using VT15 and higher will be deleted.	Refer to warning message text.
EID-6103	The TDC entry already exists.	Specify another entry for TARP Data Cache.
EID-6104	APC ABORTED.	Automatic Power Control is aborted.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
EID-6105	The 'Change Card' command is valid for MRC cards only when port 1 is the sole provisioned port.	Refer to error message text.
EID-6106	To delete all RADIUS server entries, RADIUS authentication must be disabled.	Disable Radius authentication and proceed.
EID-6107	The node failed to restart the TELNET service on the selected port. Try using another unreserved port that is not being used within the following ranges: 23, 1001-9999.	Refer to error message text.
EID-6108	There is an active TELNET session.	Restart a TELNET session.

1. EID-3159 can appear if you attempt to perform another switching operation within a certain time interval. This interval is an algorithm of three seconds per working card in the protection group. The maximum interval is 10 seconds.

CHAPTER 5

Performance Monitoring

Performance monitoring (PM) parameters are used by service providers to gather, store, set thresholds, and report performance data for early detection of problems. In this chapter, PM parameters and concepts are defined for electrical cards, Ethernet cards, and optical cards in the Cisco ONS 15454 SDH.

For information about enabling and viewing PM values, refer to the *Cisco ONS 15454 SDH Procedure Guide*.

Chapter topics include:

Note For additional information regarding PM parameters, refer to ITU G.826, and Telcordia documents GR-820-CORE, GR-499-CORE, and GR-253-CORE.

5.1 Threshold Performance Monitoring

Thresholds are used to set error levels for each PM parameter. You can set individual PM threshold values from the Cisco Transport Controller (CTC) card view Provisioning tab. For procedures on provisioning card thresholds, such as line, path, and SDH thresholds, refer to the *Cisco ONS 15454 SDH Procedure Guide*.

During the accumulation cycle, if the current value of a performance monitoring parameter reaches or exceeds its corresponding threshold value, a threshold crossing alert (TCA) is generated by the node and displayed by CTC. TCAs provide early detection of performance degradation. When a threshold is crossed, the node continues to count the errors during a given accumulation period. If 0 is entered as the threshold value, the performance monitoring parameter is disabled.

Note Due to limitations of memory and the number of TCAs generated by different platforms, you can manually add or modify the following two properties to their property file (CTC.INI for Windows and .ctcrc for UNIX) to fit the need:
ctc.15xxx.node.tr.lowater=yyy (where xxx is the platform and yyy is the number of the lowater mark. The default lowater mark is 25.)
ctc.15xxx.node.tr.hiwater=yyy (where xxx is the platform and yyy is the number of the hiwater mark. The default hiwater mark is 50.)
If the number of incoming TCA is greater than the hiwater mark, it will keep the latest lowater mark and discard older ones.

Change the threshold if the default value does not satisfy your error monitoring needs. For example, customers with a critical E1 installed for 911 calls must guarantee the best quality of service on the line; therefore, they lower all thresholds so that the slightest error raises a TCA.

5.2 Intermediate-Path Performance Monitoring

Intermediate-path performance monitoring (IPPM) allows transparent monitoring of a constituent channel of an incoming transmission signal by a node that does not terminate that channel. Many large ONS 15454 SDH networks only use line terminating equipment (LTE), not path terminating equipment (PTE). Table 5-1 shows ONS 15454 SDH cards that are considered LTE.

Table 5-1 Line Terminating Equipment (LTE)

Electrical LTE	
STM1E-12	—
Optical LTE	
OC3 IR 4/STM1 SH 1310	OC3 IR/STM1 SH 1310-8
OC12 IR/STM4 SH1310	OC12 LR/STM4 LH1310
OC12 LR/STM4 LH 1550	OC12 IR/STM4 SH 1310-4
OC48 IR/STM16 SH AS 1310	OC48 LR/STM16 LH AS 1550
OC48 ELR/STM16 EH 100 GHz	OC192 SR/STM64 IO 1310
OC192 IR/STM64 SH 1550	OC192 LR/STM64 LH 1550
OC192 LR/STM64 LH ITU 15xx.xx	TXP_MR_10G
MXP_2.5G_10G	MXP_MR_2.5G
MXPP_MR_2.5G	—

Software Release 3.0 (R3.0) and later allow LTE cards to monitor near-end PM data on individual high-order paths by enabling IPPM. After enabling IPPM provisioning on the line card, service providers can monitor high-order paths that are configured in pass-through mode on an ONS 15454 SDH operating in SDH AU4 mode, thus making troubleshooting and maintenance activities more efficient.

IPPM occurs only on high-order paths that have IPPM enabled, and TCAs are raised only for PM parameters on the IPPM enabled paths. The monitored IPPM parameters are HP-EB, HP-BBE, HP-ES, HP-SES, HP-UAS, HP-ESR, HP-SESR, and HP-BBER.

Note The E1 card and STM-1 card can monitor far-end IPPM. For all other cards listed in Table 5-1, far-end IPPM is not supported. However, SDH path PM parameters can be monitored by logging into the far-end node directly.

The ONS 15454 SDH performs IPPM by examining the overhead in the monitored path and by reading all of the near-end path PM values in the incoming direction of transmission. The IPPM process allows the path signal to pass bidirectionally through the node completely unaltered.

For detailed information about specific IPPM parameters, locate the card name in the following sections and review the appropriate definition.

5.3 Pointer Justification Count Performance Monitoring

Pointers are used to compensate for frequency and phase variations. Pointer justification counts indicate timing errors on SDH networks. When a network is out of synchronization, jitter and wander occur on the transported signal. Excessive wander can cause terminating equipment to slip.

Slips cause different effects in service. Voice service has intermittent audible clicks. Compressed voice technology has short transmission errors or dropped calls. Fax machines lose scanned lines or experience dropped calls. Digital video transmission has distorted pictures or frozen frames. Encryption service loses the encryption key causing data to be transmitted again.

Pointers provide a way to align the phase variations in VC4 payloads. The VC4 payload pointer is located in the H1 and H2 bytes of the AU pointers section and is a count of the number of bytes the VC4 path overhead (POH) J1 byte is away from the H3 byte, not including the section overhead bytes. Clocking differences are measured by the offset in bytes from the pointer to the first byte of the VC4 POH called the J1 byte. Clocking differences that exceed the normal range of 0 to 782 can cause data loss.

There are positive (PPJC) and negative (NPJC) pointer justification count parameters. PPJC is a count of path-detected (PPJC-Pdet) or path-generated (PPJC-Pgen) positive pointer justifications. NPJC is a count of path-detected (NPJC-Pdet) or path-generated (NPJC-Pgen) negative pointer justifications depending on the specific PM name.

A consistent pointer justification count indicates clock synchronization problems between nodes. A difference between the counts means the node transmitting the original pointer justification has timing variations with the node detecting and transmitting this count. Positive pointer adjustments occur when the frame rate of the POH is too slow in relation to the rate of the VC4.

You must enable PPJC and NPJC performance monitoring parameters for LTE cards. See Table 5-1 on page 5-2 for a list of Cisco ONS 15454 SDH LTE cards. In CTC, the count fields for PPJC and NPJC PM parameters appear white and blank unless they are enabled on the card view Provisioning tab.

For detailed information about specific pointer justification count PM parameters, locate the card name in the following sections and review the appropriate definition.

5.4 Performance Monitoring Parameter Definitions

Table 5-2 gives definitions for each type of performance monitoring parameter found in this chapter.

Table 5-2 Performance Monitoring Parameters

Parameter	Definition
AISS-P	AIS Seconds Path (AISS-P) is a count of one-second intervals containing one or more alarm indication signal (AIS) defects.
BBE	Path Background Block Error (BBE) is an errored block not occurring as part of a severely errored second (SES).
BBE-PM	Path Monitoring Background Block Errors (BBE-PM) indicates the number of background block errors recorded in the optical transfer network (OTN) path during the PM time interval.
BBER	Path Background Block Error Ratio (BBER) is the ratio of BBE to total blocks in available time during a fixed measurement interval. The count of total blocks excludes all blocks during SESs.
BBER-PM	Path Monitoring Background Block Errors Ratio (BBER-PM) indicates the background block errors ratio recorded in the OTN path during the PM time interval.
BBER-SM	Section Monitoring Background Block Errors Ratio (BBER-SM) indicates the background block errors ratio recorded in the OTN section during the PM time interval.
BBE-SM	Section Monitoring Background Block Errors (BBE-SM) indicates the number of background block errors recorded in the optical transport network (OTN) section during the PM time interval.
BIE	The number of bit errors (BIE) corrected in the dense wavelength division multiplexing (DWDM) trunk line during the PM time interval.
BIT-EC	The number of Bit Errors Corrected (BIT-EC) in the DWDM trunk line during the PM time interval.
CGV	Code Group Violations (CGV) is a count of received code groups that do not contain a start or end delimiter.
CVCP-P	Code Violation Path (CVCP-P) is a count of CP-bit parity errors occurring in the accumulation period.
CVCP-PFE	Code Violation (CVCP-PFE) is a parameter that is counted when the three far-end block error (FEBE) bits in a M-frame are not all collectively set to 1.
CV-L	Code Violation Line (CV-L) indicates the number of coding violations occurring on the line. This parameter is a count of BPVs and EXZs occurring over the accumulation period.
CVP-P	Code Violation Path (CVP-P) is a code violation parameter for M23 applications. CVP-P is a count of P-bit parity errors occurring in the accumulation period.
DCG	Date Code Groups (DCG) is a count of received data code groups that do not contain ordered sets.
EB	Path Errored Block (EB) indicates that one or more bits are in error within a block.
ES	Path Errored Second (ES) is a one-second period with one or more errored blocks or at least one defect.

Table 5-2 Performance Monitoring Parameters (continued)

Parameter	Definition
ESCP-P	Errored Second Path (ESCP-P) is a count of seconds containing one or more CP-bit parity errors, one or more severely errored framing (SEF) defects, or one or more AIS defects. ESCP-P is defined for the C-bit parity application.
ESCP-PFE	Far-End Errored Second CP-bit Path (ESCP-PFE) is a count of one-second intervals containing one or more M-frames with the three FEBE bits not all collectively set to 1 or one or more far-end SEF/AIS defects.
ES-L	Errored Seconds Line (ES-L) is a count of the seconds containing one or more anomalies (BPV + EXZ) and/or defects (loss of signal) on the line.
ES-P	Path Errored Second (ES-P) is a one-second period with at least one defect.
ES-PM	Path Monitoring Errored Seconds (ES-PM) indicates the errored seconds recorded in the OTN path during the PM time interval.
ESP-P	Errored Second Path (ESP-P) is a count of seconds containing one or more P-bit parity errors, one or more SEF defects, or one or more AIS defects.
ESR	Path Errored Second Ratio (ESR) is the ratio of errored seconds to total seconds in available time during a fixed measurement interval.
ESR-P	Path Errored Second Ratio (ESR-P) is the ratio of errored seconds to total seconds in available time during a fixed measurement interval.
ESR-PM	Path Monitoring Errored Seconds Ratio (ESR-PM) indicates the errored seconds ratio recorded in the OTN path during the PM time interval.
ESR-SM	Section Monitoring Errored Seconds Ratio (ESR-SM) indicates the errored seconds ratio recorded in the OTN section during the PM time interval.
ES-SM	Section Monitoring Errored Seconds (ES-SM) indicates the errored seconds recorded in the OTN section during the PM time interval.
FC-PM	Path Monitoring Failure Counts (FC-PM) indicates the failure counts recorded in the OTN path during the PM time interval.
FC-SM	Section Monitoring Failure Counts (FC-SM) indicates the failure counts recorded in the OTN section during the PM time interval.
HP-BBE	High-Order Path Background Block Error (HP-BBE) is an errored block not occurring as part of an SES.
HP-BBER	High-Order Path Background Block Error Ratio (HP-BBER) is the ratio of BBE to total blocks in available time during a fixed measurement interval. The count of total blocks excludes all blocks during SESs.
HP-EB	High-Order Path Errored Block (HP-EB) indicates that one or more bits are in error within a block.
HP-ES	High-Order Path Errored Second (HP-ES) is a one-second period with one or more errored blocks or at least one defect.
HP-ESR	High-Order Path Errored Second Ratio (HP-ESR) is the ratio of errored seconds to total seconds in available time during a fixed measurement interval.
HP-NPJC-Pdet	High-Order, Negative Pointer Justification Count, Path Detected (HP-NPJC-Pdet) is a count of the negative pointer justifications detected on a particular path on an incoming SDH signal.

Table 5-2 Performance Monitoring Parameters (continued)

Parameter	Definition
HP-NPJC-Pgen	High-Order, Negative Pointer Justification Count, Path Generated (HP-NPJC-Pgen) is a count of the negative pointer justifications generated for a particular path.
HP-PJCDiff	High-Order Path Pointer Justification Count Difference (HP-PJCDiff) is the absolute value of the difference between the total number of detected pointer justification counts and the total number of generated pointer justification counts. That is, HP-PJCDiff is equal to (HP-PPJC-PGen – HP-NPJC-PGen) – (HP-PPJC-PDet – HP-NPJC-PDet).
HP-PJCS-Pdet	High-Order Path Pointer Justification Count Seconds (HP-PJCS-PDet) is a count of the one-second intervals containing one or more HP-PPJC-PDet or HP-NPJC-PDet.
HP-PJCS-Pgen	High-Order Path Pointer Justification Count Seconds (HP-PJCS-PGen) is a count of the one-second intervals containing one or more HP-PPJC-PGen or HP-NPJC-PGen.
HP-PPJC-Pdet	High-Order, Positive Pointer Justification Count, Path Detected (HP-PPJC-Pdet) is a count of the positive pointer justifications detected on a particular path on an incoming SDH signal.
HP-PPJC-Pgen	High-Order, Positive Pointer Justification Count, Path Generated (HP-PPJC-Pgen) is a count of the positive pointer justifications generated for a particular path.
HP-SES	High-Order Path Severely Errored Seconds (HP-SES) is a one-second period containing 30 percent or more errored blocks or at least one defect. SES is a subset of ES.
HP-SESR	High-Order Path Severely Errored Second Ratio (HP-SESR) is the ratio of SES to total seconds in available time during a fixed measurement interval.
HP-UAS	High-Order Path Unavailable Seconds (HP-UAS) is a count of the seconds when the VC path was unavailable. A high-order path becomes unavailable when ten consecutive seconds occur that qualify as HP-SESs, and it continues to be unavailable until ten consecutive seconds occur that do not qualify as HP-SESs.
IOS	Idle Ordered Sets (IOS) is a count of received packets containing idle ordered sets.
IPC	A count of received packets that contain errored data code groups that have start and end delimiters.
LBC-MIN	LBC-MIN is the minimum percentage of Laser Bias Current.
LBC-AVG	Laser Bias Current—Average (LBC-AVG) is the average percentage of laser bias current.
LBC-MAX	Laser Bias Current—Maximum (LBC-MAX) is the maximum percentage of laser bias current.
LBC-MIN	Laser Bias Current—Minimum (LBC-MIN) is the minimum percentage of laser bias current.
LOSS-L	Line Loss of Signal Seconds (LOSS-L) is a count of one-second intervals containing one or more LOS defects.

Table 5-2 Performance Monitoring Parameters (continued)

Parameter	Definition
LP-BBE	Low-Order Path Background Block Error (LP-BBE) is an errored block not occurring as part of an SES.
LP-BBER	Low-Order Path Background Block Error Ratio (LP-BBER) is the ratio of BBE to total blocks in available time during a fixed measurement interval. The count of total blocks excludes all blocks during SESs.
LP-EB	Low-Order Path Errored Block (LP-EB) indicates that one or more bits are in error within a block.
LP-ES	Low-Order Path Errored Second (LP-ES) is a one-second period with one or more errored blocks or at least one defect.
LP-ESR	Low-Order Path Errored Second Ratio (LP-ESR) is the ratio of errored seconds to total seconds in available time during a fixed measurement interval.
LP-SES	Low-Order Path Severely Errored Seconds (LP-SES) is a one-second period containing greater than or equal to 30 percent errored blocks or at least one defect. SES is a subset of ES.
LP-SESR	Low-Order Path Severely Errored Second Ratio (LP-SESR) is the ratio of SES to total seconds in available time during a fixed measurement interval.
LP-UAS	Low-Order Path Unavailable Seconds (LP-UAS) is a count of the seconds when the VC path was unavailable. A low-order path becomes unavailable when ten consecutive seconds occur that qualify as LP-SESs, and it continues to be unavailable until ten consecutive seconds occur that do not qualify as LP-SESs.
MS-BBE	Multiplex Section Background Block Error (MS-BBE) is an errored block not occurring as part of an SES.
MS-BBER	Multiplex Section Background Block Error Ratio (MS-BBER) is the ratio of BBE to total blocks in available time during a fixed measurement interval. The count of total blocks excludes all blocks during SESs.
MS-EB	Multiplex Section Errored Block (MS-EB) indicates that one or more bits are in error within a block.
MS-ES	Multiplex Section Errored Second (MS-ES) is a one-second period with one or more errored blocks or at least one defect.
MS-ESR	Multiplex Section Errored Second Ratio (MS-ESR) is the ratio of errored seconds to total seconds in available time during a fixed measurement interval.
MS-NPJC-Pdet	Multiplex Section Negative Pointer Justification Count, Path Detected (MS-NPJC-Pdet) is a count of the negative pointer justifications detected on a particular path on an incoming SDH signal.
MS-NPJC-Pgen	Multiplex Section Negative Pointer Justification Count, Path Generated (MS-NPJC-Pgen) is a count of the negative pointer justifications generated for a particular path.
MS-PPJC-Pdet	Multiplex Section Positive Pointer Justification Count, Path Detected (MS-PPJC-Pdet) is a count of the positive pointer justifications detected on a particular path on an incoming SDH signal.

Table 5-2 Performance Monitoring Parameters (continued)

Parameter	Definition
MS-PPJC-Pgen	Multiplex Section Positive Pointer Justification Count, Path Generated (MS-PPJC-Pgen) is a count of the positive pointer justifications generated for a particular path.
MS-PSC (1+1 protection)	In a 1+1 protection scheme for a working card, Multiplex Section Protection Switching Count (MS-PSC) is a count of the number of times service switches from a working card to a protection card plus the number of times service switches back to the working card. For a protection card, MS-PSC is a count of the number of times service switches to a working card from a protection card plus the number of times service switches back to the protection card. The MS-PSC PM is only applicable if revertive line-level protection switching is used.
MS-PSC[1] (MS-SPRing)	For a protect line in a two-fiber multiplex section-shared protection ring (MS-SPRing), Multiplex Section Protection Switching Count (MS-PSC) refers to the number of times a protection switch has occurred either to a particular span's line protection or away from a particular span's line protection. Therefore, if a protection switch occurs on a two-fiber MS-SPRing, the MS-PSC of the protection span to which the traffic is switched will increment, and when the switched traffic returns to its original working span from the protect span, the MS-PSC of the protect span will increment again.
MS-PSC-R[1]	In a four-fiber MS-SPRing, Multiplex Section Protection Switching Count-Ring (MS-PSC-R) is a count of the number of times service switches from a working line to a protection line plus the number of times it switches back to a working line. A count is only incremented if ring switching is used.
MS-PSC-S	In a four-fiber MS-SPRing, Multiplex Section Protection Switching Count-Span (MS-PSC-S) is a count of the number of times service switches from a working line to a protection line plus the number of times it switches back to the working line. A count is only incremented if span switching is used.
MS-PSC-W	For a working line in a two-fiber MS-SPRing, Multiplex Section Protection Switching Count-Working (MS-PSC-W) is a count of the number of times traffic switches away from the working capacity in the failed line and back to the working capacity after the failure is cleared. MS-PSC-W increments on the failed working line and MS-PSC increments on the active protect line. For a working line in a four-fiber MS-SPRing, MS-PSC-W is a count of the number of times service switches from a working line to a protection line plus the number of times it switches back to the working line. MS-PSC-W increments on the failed line and MS-PSC-R or MS-PSC-S increments on the active protect line.

Table 5-2 Performance Monitoring Parameters (continued)

Parameter	Definition
MS-PSD	Multiplex Section Protection Switching Duration (MS-PSD) applies to the length of time, in seconds, that service is carried on another line. For a working line, MS-PSD is a count of the number of seconds that service was carried on the protection line. For the protection line, MS-PSD is a count of the seconds that the line was used to carry service. The MS-PSD PM is only applicable if revertive line-level protection switching is used. MS-PSD increments on the active protect line and MS-PSD-W increments on the failed working line.
MS-PSD-R	In a four-fiber MS-SPRing, Multiplex Section Protection Switching Duration-Ring (MS-PSD-R) is a count of the seconds that the protection line was used to carry service. A count is only incremented if ring switching is used.
MS-PSD-S	In a four-fiber MS-SPRing, Multiplex Section Protection Switching Duration-Span (MS-PSD-S) is a count of the seconds that the protection line was used to carry service. A count is only incremented if span switching is used.
MS-PSD-W	For a working line in a two-fiber MS-SPRing, Multiplex Section Protection Switching Duration-Working (MS-PSD-W) is a count of the number of seconds that service was carried on the protection line. MS-PSD-W increments on the failed working line and PSD increments on the active protect line.
MS-SES	Multiplex Section Severely Errored Second (MS-SES) is a one-second period which contains 30 percent or more errored blocks or at least one defect. SES is a subset of ES. For more information, refer to ITU-T G.829 Section 5.1.3.
MS-SESR	Multiplex Section Severely Errored Second ratio (MS-SESR) is the ratio of SES to total seconds in available time during a fixed measurement interval.
MS-UAS	Multiplex Section Unavailable Seconds (MS-UAS) is a count of the seconds when the section was unavailable. A section becomes unavailable when ten consecutive seconds occur that qualify as MS-SESs, and it continues to be unavailable until ten consecutive seconds occur that do not qualify as MS-SESs. When the condition is entered, MS-SESs decrement and then count toward MS-UAS.
NIOS	Non-Idle Ordered Sets (NIOS) is a count of received packets containing non-idle ordered sets.
OPR	Optical Power Received (OPR) is the measure of average optical power received as a percentage of the nominal OPT.
OPR-AVG	Average Receive Optical Power (dBm).
OPR-MAX	Maximum Receive Optical Power (dBm).
OPR-MIN	Minimum Receive Optical Power (dBm).
OPT	Optical Power Transmitted (OPT) is the measure of average optical power transmitted as a percentage of the nominal OPT.
OPT-AVG	Average Transmit Optical Power (dBm).

Table 5-2 Performance Monitoring Parameters (continued)

Parameter	Definition
OPT-MAX	Maximum Transmit Optical Power (dBm).
OPT-MIN	Minimum Transmit Optical Power (dBm).
RS-BBE	Regenerator Section Background Block Error (RS-BBE) is an errored block not occurring as part of an SES.
RS-BBER	Regenerator Section Background Block Error Ratio (RS-BBER) is the ratio of BBE to total blocks in available time during a fixed measurement interval. The count of total blocks excludes all blocks during SESs.
RS-EB	Regenerator Section Errored Block (RS-EB) indicates that one or more bits are in error within a block.
RS-ES	Regenerator Section Errored Second (RS-ES) is a one-second period with one or more errored blocks or at least one defect.
RS-ESR	Regenerator Section Errored Second Ratio (RS-ESR) is the ratio of errored seconds to total seconds in available time during a fixed measurement interval.
RS-SES	Regenerator Section Severely Errored Second (RS-SES) is a one-second period which contains 30 percent or more errored blocks or at least one defect. SES is a subset of ES.
RS-SESR	Regenerator Section Severely Errored Second Ratio (RS-SESR) is the ratio of SES to total seconds in available time during a fixed measurement interval.
RS-UAS	Regenerator Section Unavailable Second (RS-UAS) is a count of the seconds when the regenerator section was unavailable. A section becomes unavailable when ten consecutive seconds occur that qualify as RS-UASs, and it continues to be unavailable until ten consecutive seconds occur that do not qualify as RS-UASs.
Rx AISS-P	Receive Path Alarm Indication Signal Seconds (AISS-P) means that an alarm indication signal occurred on the receive end of the path. This parameter is a count of seconds containing one or more AIS defects.
Rx BBE-P	Receive Path Background Block Error (BBE-P) is an errored block not occurring as part of an SES.
Rx EB-P	Receive Path Errored Block (EB-P) indicates that one or more bits are in error within a block.
Rx ES-P	Receive Path Errored Second (ES-P) is a one-second period with one or more errored blocks or at least one defect.
Rx ESR-P	Receive Path Errored Second Ratio (ESR-P) is the ratio of errored seconds to total seconds in available time during a fixed measurement interval.
Rx SES-P	Receive Path Severely Errored Seconds (SES-P) is a one-second period containing 30 percent or more errored blocks or at least one defect; SES is a subset of ES.
Rx SESR-P	Receive Path Severely Errored Second Ratio (SESR-P) is the ratio of SES to total seconds in available time during a fixed measurement interval.

Table 5-2 Performance Monitoring Parameters (continued)

Parameter	Definition
Rx UAS-P	Receive Path Unavailable Seconds (UAS-P) is a count of one-second intervals when the E-1 path is unavailable on the signal receive end. The E-1 path is unavailable when ten consecutive SESs occur. The ten SESs are included in unavailable time. After the E-1 path becomes unavailable, it becomes available when ten consecutive seconds occur with no SESs. The ten seconds with no SESs are excluded from unavailable time.
Rx BBER-P	Receive Path Background Block Error Ratio (BBER-P) is the ratio of BBE to total blocks in available time during a fixed measurement interval. The count of total blocks excludes all blocks during SESs.
SASCP-P	SEF/AIS Second (SASCP-P) is a count of one-second intervals containing one or more near-end SEF/AIS defects.
SASP-P	SEF/AIS Seconds Path (SASP-P) is a count of one-second intervals containing one or more SEFs or one or more AIS defects on the path.
SES	Severely Errored Seconds (SES) is a one-second period containing 30 percent or more errored blocks or at least one defect. SES is a subset of ES.
SESCP-P	Severely Errored Seconds CP-bit Path (SESCP-P) is a count of seconds containing more than 44 CP-bit parity errors, one or more SEF defects, or one or more AIS defects.
SESCP-PFE	Severely Errored Seconds CP-bit Path Far End (SESCP-PFE) is a count of one-second intervals containing one or more 44 M-frames with the three FEBE bits not all collectively set to 1, or with one or more far-end SEF/AIS defects.
SES-L	Severely Errored Seconds Line (SES-L) is a count of the seconds containing more than a particular quantity of anomalies (BPV + EXZ $\geq$ 44) and/or defects on the line.
SES-P	Severely Errored Seconds Path (SES-P) is a one-second period containing at least one defect. SES-P is a subset of ES-P.
SES-PFE	Far-End Path Severely Errored Seconds (SES-PFE) is a one-second period containing at least one defect. SES-PFE is a subset of ES-PFE.
SES-PM	Path Monitoring Severely Errored Seconds (SES-PM) indicates the severely errored seconds recorded in the OTN path during the PM time interval.
SESP-P	Severely Errored Seconds Path (SESP-P) is a count of seconds containing more than 44 P-bit parity violations, one or more SEF defects, or one or more AIS defects.
SESR-P	Path Severely Errored Second Ratio (SESR-P) is the ratio of SES to total seconds in available time during a fixed measurement interval.
SESR-PM	Path Monitoring Severely Errored Seconds Ratio (SESR-PM) indicates the severely errored seconds ratio recorded in the OTN path during the PM time interval.
SES-SM	Section Monitoring Severely Errored Seconds (SES-SM) indicates the severely errored seconds recorded in the OTN section during the PM time interval.

Table 5-2 Performance Monitoring Parameters (continued)

Parameter	Definition
Tx AISS-P	Transmit Path Alarm Indication Signal (AISS-P) means that an alarm indication signal occurred on the transmit end of the path. This parameter is a count of seconds containing one or more AIS defects.
Tx BBE-P	Transmit Path Background Block Error (BBE-P) is an errored block not occurring as part of an SES.
Tx ES-P	Transmit Path Errored Second (ES-P) is a one-second period with one or more errored blocks or at least one defect.
Tx ESR-P	Transmit Path Errored Second Ratio (ESR-P) is the ratio of errored seconds to total seconds in available time during a fixed measurement interval.
Tx SES-P	Transmit Path Severely Errored Seconds (SES-P) is a one-second period containing 30 percent or more errored blocks or at least one defect; SES is a subset of ES.
Tx SESR-P	Transmit Path Severely Errored Second Ratio (SESR-P) is the ratio of SES to total seconds in available time during a fixed measurement interval.
Tx UAS-P	Transmit Path Unavailable Seconds (UAS-P) is a count of one-second intervals when the E-1 path is unavailable on the transmit end of the signal. The E-1 path is unavailable when ten consecutive SESs occur. The ten SESs are included in unavailable time. After the E-1 path becomes unavailable, it becomes available when ten consecutive seconds occur with no SESs. The ten seconds with no SESs are excluded from unavailable time.
Tx BBER-P	Transmit Path Background Block Error Ratio (BBER-P) is the ratio of BBE to total blocks in available time during a fixed measurement interval. The count of total blocks excludes all blocks during SESs.
Tx EB-P	Transmit Path Errored Block (EB-P) indicates that one or more bits are in error within a block.
UAS	Path Unavailable Seconds (UAS) is a count of the seconds when the VC path was unavailable. A high-order path becomes unavailable when ten consecutive seconds occur that qualify as HP-SESs, and it continues to be unavailable until ten consecutive seconds occur that do not qualify as HP-SESs.
UASCP-P	Unavailable Seconds CP-bit Path (UASCP-P) is a count of one-second intervals when the DS-3 path is unavailable. A DS-3 path becomes unavailable when ten consecutive SESCP-Ps occur. The ten SESCP-Ps are included in unavailable time. After the DS-3 path becomes unavailable, it becomes available when ten consecutive seconds with no SESCP-Ps occur. The ten seconds with no SESCP-Ps are excluded from unavailable time.
UASCP-PFE	Unavailable Seconds CP-bit Far End Path (UASCP-PFE) is a count of one-second intervals when the DS-3 path becomes unavailable. A DS-3 path becomes unavailable when ten consecutive far-end CP-bit SESs occur. The ten CP-bit SESs are included in unavailable time. After the DS-3 path becomes unavailable, it becomes available when ten consecutive seconds occur with no CP-bit SESs. The ten seconds with no CP-bit SESs are excluded from unavailable time.

Table 5-2 Performance Monitoring Parameters (continued)

Parameter	Definition
UAS-P	Path Unavailable Seconds (UAS-P) is a count of the seconds when the path was unavailable. A path becomes unavailable when ten consecutive seconds occur that qualify as P-SESs, and it continues to be unavailable until ten consecutive seconds occur that do not qualify as P-SESs.
UAS-PFE	Far-End Path Unavailable Seconds (UAS-PFE) is a count of the seconds when the path was unavailable. A path becomes unavailable when ten consecutive seconds occur that qualify as P-SESs, and it continues to be unavailable until ten consecutive seconds occur that do not qualify as P-SESs.
UAS-PM	Path Monitoring Unavailable Seconds (UAS-PM) indicates the unavailable seconds recorded in the OTN path during the PM time interval.
UASP-P	Unavailable Second Path (UASP-P) is a count of one-second intervals when the DS-3 path is unavailable. A DS3 path becomes unavailable when ten consecutive SESP-Ps occur. The ten SESP-Ps are included in unavailable time. After the DS-3 path becomes unavailable, it becomes available when ten consecutive seconds with no SESP-Ps occur. The ten seconds with no SESP-Ps are excluded from unavailable time.
UAS-SM	Section Monitoring Unavailable Seconds (UAS-SM) indicates the unavailable seconds recorded in the OTN section during the PM time interval.
UNC-WORDS	The number of uncorrectable words detected in the DWDM trunk line during the PM time interval.
VPC	A count of received packets that contain non-errored data code groups that have start and end delimiters.

1. 4-fiber MS-SPRing is not supported on the STM-4 and STM4 SH 1310-4 cards; therefore, the MS-PSC-S and MS-PSC-R PM parameters do not increment.

5.5 Performance Monitoring for Electrical Cards

The following sections define performance monitoring parameters for the E1-N-14, E1-42, E3-12, and DS3i-N-12 electrical cards.

5.5.1 E1-N-14 Card and E1-42 Card Performance Monitoring Parameters

Figure 5-1 shows the signal types that support near-end and far-end PM parameters for the E1-N-14 card and the E1-42 card.

Figure 5-1 Monitored Signal Types for the E1-N-14 Card and E1-42 Card

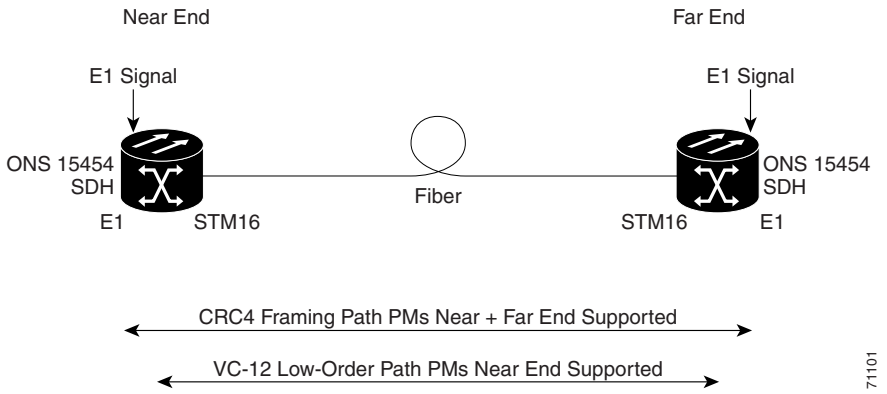
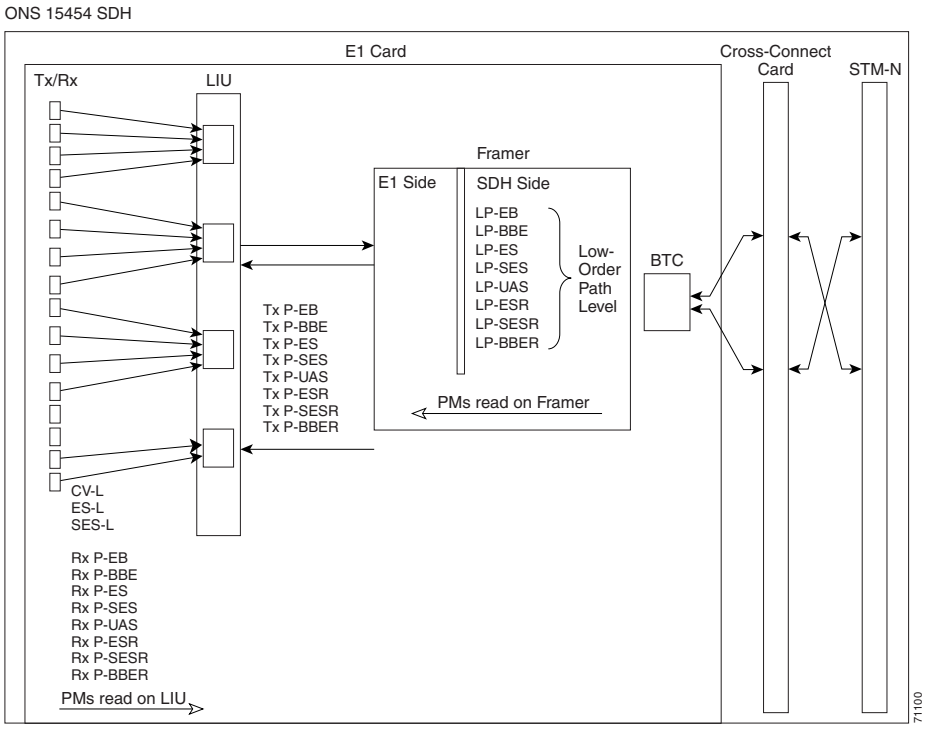


Figure 5-2 shows where overhead bytes detected on the application-specific integrated circuits (ASICs) produce performance monitoring parameters for the E1-N-14 card.

Note The E1-42 card uses the same PM read points. The only difference from Figure 5-2 is that the number of ports on the E1-42 equal 42.

Figure 5-2 PM Read Points on the E1-N-14 Card



The PM parameters for the E1-N-14 card and E1-42 card are listed in Table 5-3. The parameters are defined in Table 5-2 on page 5-4.

Table 5-3 PM Parameters for the E1-N-14 Card and E1-42 Card

Line (NE)[1]	Tx/Rx Path (NE)[2, 3]	VC12 LP (NE/FE)	Tx/Rx Path (FE)[2 3]
CV-L	AISS-P	LP-EB	AISS-PFE
ES-L	BBE-P	LP-ES	BBE-PFE
SES-L	BBER-P	LP-SES	BBER-PFE
LOSS-L	EB-P	LP-UAS	EB-PFE
	ES-P	LP-BBE	ES-PFE
	ESR-P	LP-ESR	ESR-PFE
	SES-P	LP-SESR	SES-PFE
	SESR-P	LP-BBER	SESR-PFE
	UAS-P		UAS-PFE

1. SDH path PMs do not increment unless IPPM is enabled. See the "5.2 Intermediate-Path Performance Monitoring" section on page 5-2.
2. Transmit and receive CEPT and CRC4 framing path PM parameters for the near-end and far-end E1-N-14 and E1-42 cards.
3. Under the Provisioning > Threshold tab, the E1-N-14 card and the E1-42 card have user-defined thresholds for the E-1 Rx path PM parameters. In the Threshold tab, they are displayed as EB, BBE, ES, SES, and UAS without the Rx prefix.

5.5.2 E3-12 Card Performance Monitoring Parameters

Figure 5-3 shows the signal types that support near-end and far-end PM parameters for the E3-12 card. Figure 5-4 shows where overhead bytes detected on the ASICs produce performance monitoring parameters for the E3-12 card.

Figure 5-3 Monitored Signal Types for the E3-12 Card

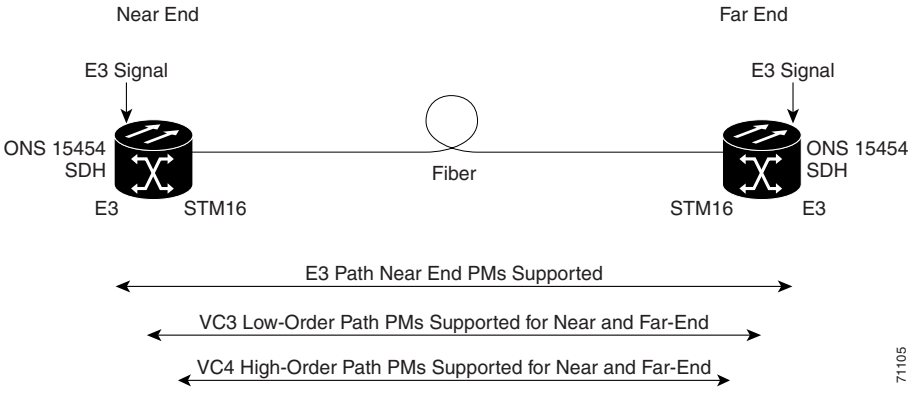
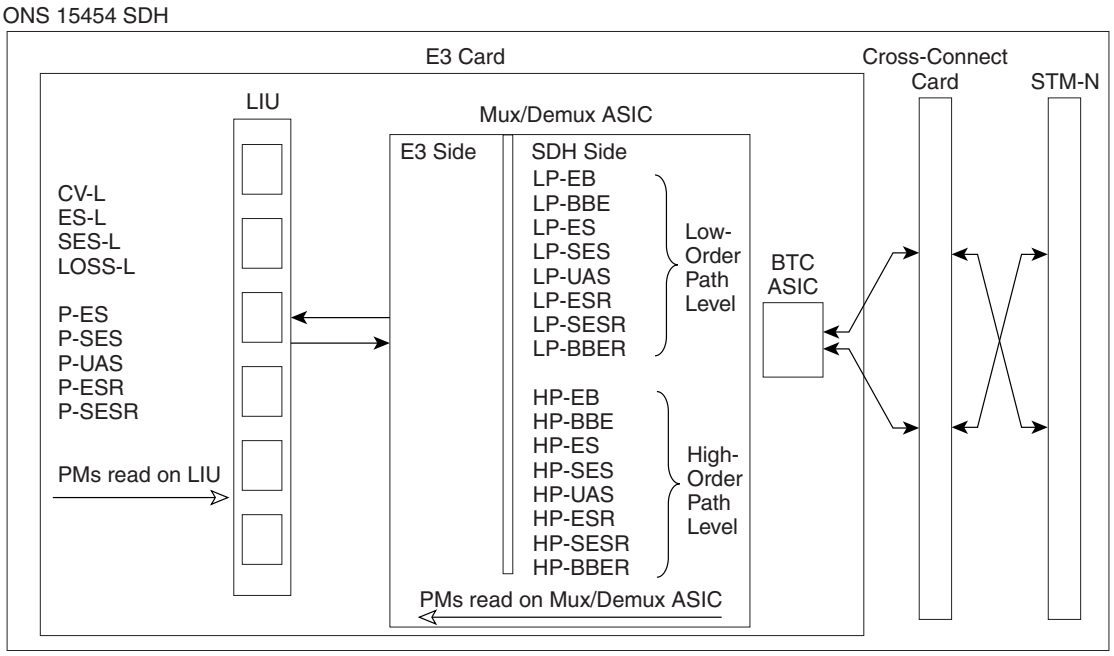


Figure 5-4 PM Read Points on the E3-12 Card



The PM parameters for the E3-12 card are listed in Table 5-4. The parameters are defined in Table 5-2 on page 5-4.

Table 5-4 PM Parameters for the E3-12 Card

Line (NE)	Path (NE)	VC3 Low-End Path (NE/FE)	VC4 HP Path (NE/FE)
CV-L	ES-P	LP-BBE	HP-BBE
ES-L	ESR-P	LP-BBER	HP-BBER
SES-L	SES-P	LP-EB	HP-EB
LOSS-L	SESR-P	LP-ES	HP-ES
	UAS-P	LP-ESR	HP-ESR
		LP-SES	HP-SES
		LP-SESR	HP-SESR
		LP-UAS	HP-UAS

5.5.3 DS3i-N-12 Card Performance Monitoring Parameters

Figure 5-5 shows the signal types that support near-end and far-end PM parameters for the DS3i-N-12 card. Figure 5-6 shows where overhead bytes detected on the ASICs produce performance monitoring parameters for the DS3i-N-12 card.

Figure 5-5 Monitored Signal Types for the DS3i-N-12 Card

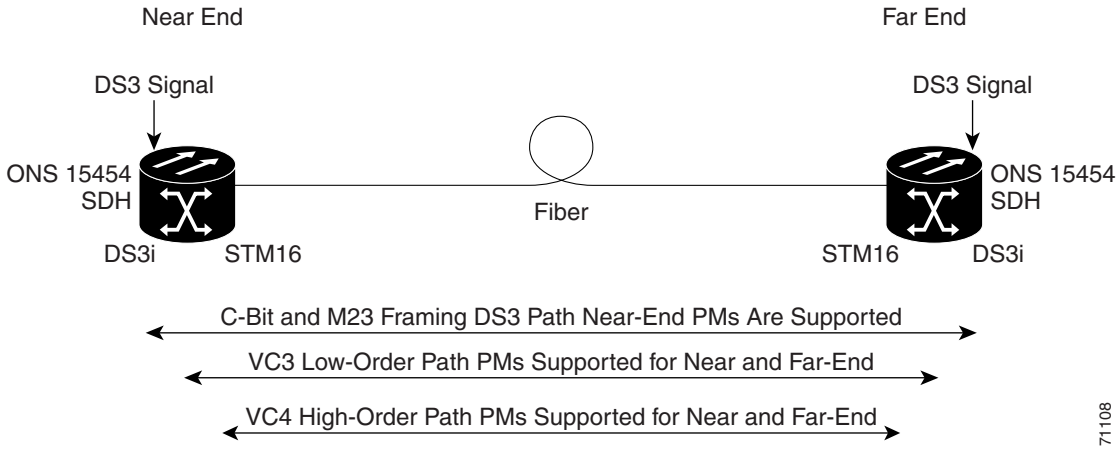
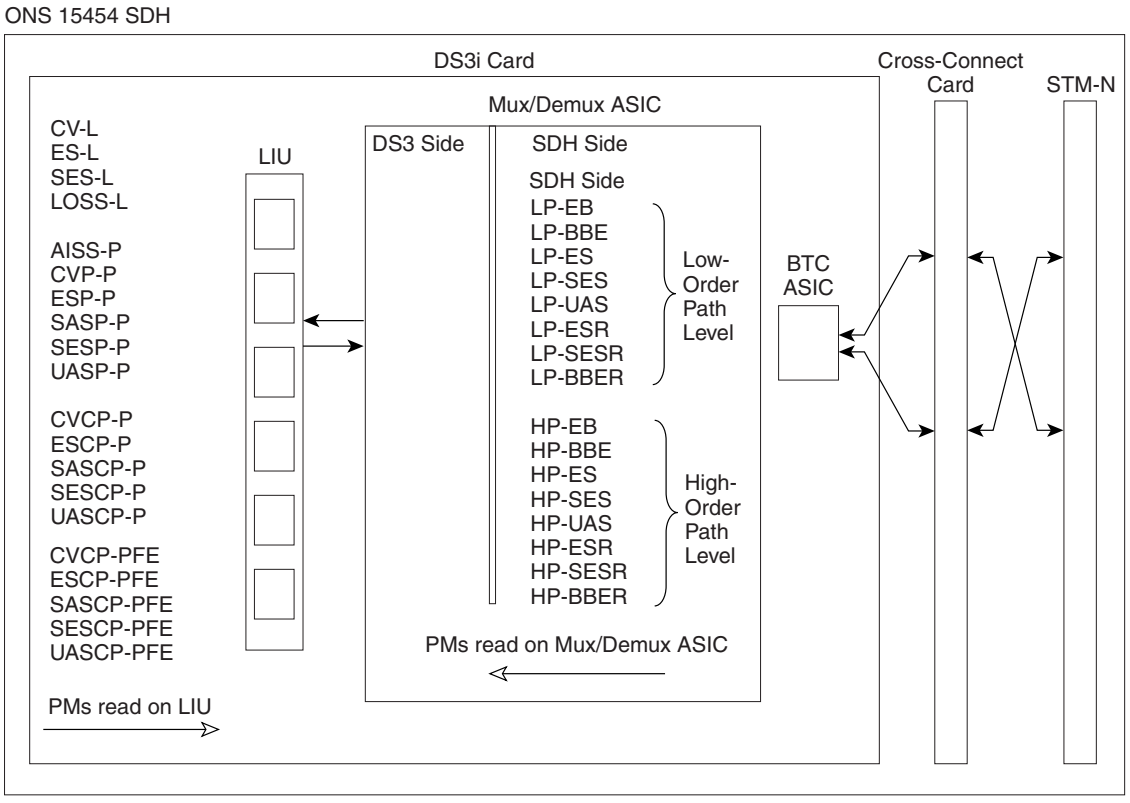


Figure 5-6 PM Read Points on the DS3i-N-12 Card



The PM parameters for the DS3i-N-12 card are listed in Table 5-5. The parameters are defined in Table 5-2 on page 5-4.

Table 5-5 DS3i-N-12 Card PMs

Line (NE)	Path (NE)[1, 2]	Path (FE)[1, 2]	VC3 Low-End Path (NE/FE)	VC4 HP Path (NE/FE)
CV-L	AISS-P	CVCP-PFE	LP-BBE	HP-BBE
ES-L	CVP-P	ESCP-PFE	LP-BBER	HP-BBER
SES-L	ESP-P	SASCP-PFE	LP-EB	HP-EB
LOSS-L	SASP-P[3]	SESCP-PFE	LP-ES	HP-ES
	SESP-P	UASCP-PFE	LP-ESR	HP-ESR
	UASP-P		LP-SES	HP-SES
	CVCP-P		LP-SESR	HP-SESR
	ESCP-P		LP-UAS	HP-UAS
	SASP-P			
	SESCP-P			
	UASCP-P			

1. C-Bit and M23 framing path PM parameters
2. The C-bit PMs (PMs that contain the text "CP-P") are applicable only if line format is C-bit.
3. DS3i-N-12 cards support SAS-P only on the Rx path.

5.6 Performance Monitoring for Ethernet Cards

The following sections define performance monitoring parameters and definitions for the E-Series, G-Series, and ML-Series Ethernet cards.

5.6.1 E-Series Ethernet Card Performance Monitoring Parameters

CTC provides Ethernet performance information, including line-level parameters, port bandwidth consumption, and historical Ethernet statistics. The E-Series Ethernet performance information is divided into the Statistics, Utilization, and History tabbed windows within the card view Performance tab window. The following sections describe PM parameters provided for the E100T-G and E1000-2 Ethernet cards.

5.6.1.1 E-Series Ethernet Statistics Window

The Ethernet statistics window lists Ethernet parameters at the line level. The Statistics window provides buttons to change the statistical values shown. The Baseline button resets the displayed statistics values to zero. The Refresh button manually refreshes statistics. Auto-Refresh sets a time interval at which automatic refresh occurs.

Table 5-6 defines the E-Series Ethernet card statistics parameters.

Table 5-6 E-Series Ethernet Statistics Parameters

Parameter	Meaning
Link Status	Link integrity indicator (up means present, and down means not present).
Rx Packets	Number of packets received since the last counter reset.
Rx Bytes	Number of bytes received since the last counter reset.
Tx Packets	Number of packets transmitted since the last counter reset.

Table 5-6 E-Series Ethernet Statistics Parameters (continued)

Parameter	Meaning
Tx Bytes	Number of bytes transmitted since the last counter reset.
Rx Total Errors	Total number of receive errors.
Rx FCS	Number of packets with a frame check sequence (FCS) error. FCS errors indicate frame corruption during transmission.
Rx Alignment	Number of packets with alignment errors (received incomplete frames).
Rx Runts	Measures undersized packets with bad cyclic redundancy check (CRC) errors.
Rx Shorts	Measures undersized packets with good CRC errors.
Rx Oversized + Jabbers	Measures oversized packets and jabbers. Size is greater than 1522 errors regardless of CRC errors.
Rx Giants	Number of packets received that are greater than 1518 bytes in length for untagged interfaces and 1522 bytes for tagged interfaces.
Tx Collisions	Number of transmit packets that are collisions; the port and the attached device transmitting at the same time caused collisions.
Tx Late Collisions	Number of frames that were not transmitted since they encountered a collision outside of the normal collision window. Normally, late collision events should occur only rarely, if at all.
Tx Excessive Collisions	Number of consecutive collisions.
Tx Deferred	Number of packets deferred.

5.6.1.2 E-Series Ethernet Utilization Window

The Utilization window shows the percentage of transmit (Tx) and receive (Rx) line bandwidth used by the Ethernet ports during consecutive time segments. The Mode field displays the real-time mode status, such as “100 Full,” which is the mode setting configured on the E-Series port. However, if the E-Series port is set to autonegotiate the mode (Auto), this field shows the result of the link negotiation between the E-Series and the peer Ethernet device attached directly to the E-Series port.

The Utilization window provides an Interval menu that enables you to set time intervals of 1 minute, 15 minutes, 1 hour, and 1 day. Line utilization is calculated with the following formulas:

Rx = (inOctets + inPkts * 20) * 8 / 100% interval * maxBaseRate

Tx = (outOctets + outPkts * 20) * 8 / 100% interval * maxBaseRate

The interval is defined in seconds. The maxBaseRate is defined by raw bits per second in one direction for the Ethernet port (that is, 1 Gbps). STS circuit maxBaseRates are shown in Table 5-7.

Table 5-7 MaxBaseRate for VC Circuits

STS	maxBaseRate
VC3	51840000
VC4	155000000
VC42C	311000000
VC44C	622000000

Note Line utilization numbers express the average of ingress and egress traffic as a percentage of capacity.

Note The E-Series Ethernet card is a Layer 2 device or switch and supports Trunk Utilization statistics. The Trunk Utilization statistics are similar to the Line Utilization statistics, but shows the percentage of circuit bandwidth used rather than the percentage of line bandwidth used. The Trunk Utilization statistics are accessed through the card view Maintenance tab.

5.6.1.3 E-Series Ethernet History Window

The Ethernet History window lists past Ethernet statistics for the previous time intervals. Depending on the selected time interval, the History window displays the statistics for each port for the number of previous time intervals as shown in Table 5-8. The parameters are defined in Table 5-6 on page 5-18.

Table 5-8 Ethernet Statistics History per Time Interval

Time Interval	Number of Intervals Displayed
1 minute	60 previous time intervals
15 minutes	32 previous time intervals
1 hour	24 previous time intervals
1 day (24 hours)	7 previous time intervals

5.6.2 G-Series Ethernet Card Performance Monitoring Parameters

CTC provides Ethernet performance information, including line-level parameters, port bandwidth consumption, and historical Ethernet statistics. The G-Series Ethernet performance information is divided into the Statistics, Utilization, and History tabbed windows within the card view Performance tab window. The following sections describe PM parameters provided for the G1000-4 and G1K-4 Ethernet cards.

5.6.2.1 G-Series Ethernet Statistics Window

The Ethernet Statistics window lists Ethernet parameters at the line level. The Statistics window provides buttons to change the statistical values shown. The Baseline button resets the displayed statistics values to zero. The Refresh button manually refreshes statistics. Auto-Refresh sets a time interval at which automatic refresh occurs. The G-Series Statistics window also has a Clear button. The Clear button sets the values on the card to zero, but does not reset the G-Series card.

Table 5-9 defines the G-Series Ethernet card statistics parameters.

Table 5-9 G-Series Ethernet Statistics Parameters

Parameter	Meaning
Time Last Cleared	A time stamp indicating the last time statistics were reset.
Link Status	Indicates whether the Ethernet link is receiving a valid Ethernet signal (carrier) from the attached Ethernet device; up means present, and down means not present.
Rx Packets	Number of packets received since the last counter reset.
Rx Bytes	Number of bytes received since the last counter reset.
Tx Packets	Number of packets transmitted since the last counter reset.
Tx Bytes	Number of bytes transmitted since the last counter reset.
Rx Total Errors	Total number of receive errors.
Rx FCS	Number of packets with a FCS error. FCS errors indicate frame corruption during transmission.
Rx Alignment	Number of packets with received incomplete frames.
Rx Runts	Measures undersized packets with bad CRC errors.
Rx Shorts	Measures undersized packets with good CRC errors.
Rx Jabbers	Total number of frames received that exceed the 1548-byte maximum and contain CRC errors.
Rx Giants	Number of packets received that are greater than 1530 bytes in length.
Rx Pause Frames	Number of received Ethernet IEEE 802.3z pause frames.
Tx Pause Frames	Number of transmitted IEEE 802.3z pause frames.
Rx Pkts Dropped Internal Congestion	Number of received packets dropped due to overflow in G-Series frame buffer.
Tx Pkts Dropped Internal Congestion	Number of transmit queue drops due to drops in the G-Series frame buffer.
HDLC Errors	High-level data link control (HDLC) errors received from SDH/SONET. Do not use the HDLC errors counter to count the number of frames dropped because of HDLC errors, because each frame can fragment into several smaller frames during HDLC error conditions and spurious HDLC frames can also be generated. If HDLC error counters are incrementing when no SDH path problems should be present, it might indicate a problem with the quality of the SDH path. For example, a SDH protection switch generates a set of HLDC errors. But the actual values of these counters are less significant than the fact they are changing.
Rx Unicast Packets	Number of unicast packets received since the last counter reset.
Tx Unicast Packets	Number of unicast packets transmitted.
Rx Multicast Packets	Number of multicast packets received since the last counter reset.
Tx Multicast Packets	Number of multicast packets transmitted.
Rx Broadcast Packets	Number of broadcast packets received since the last counter reset.
Tx Broadcast Packets	Number or broadcast packets transmitted.

5.6.2.2 G-Series Ethernet Utilization Window

The Utilization window shows the percentage of Tx and R) line bandwidth used by the Ethernet ports during consecutive time segments. The Mode field displays the real-time mode status, such as "100 Full," which is the mode setting configured on the G-Series port. However, if the G-Series port is set to autonegotiate the mode (Auto), this field shows the result of the link negotiation between the G-Series and the peer Ethernet device attached directly to the G-Series port.

The Utilization window provides an Interval menu that enables you to set time intervals of 1 minute, 15 minutes, 1 hour, and 1 day. Line utilization is calculated with the following formulas:

Rx = (inOctets + inPkts * 20) * 8 / 100% interval * maxBaseRate

Tx = (outOctets + outPkts * 20) * 8 / 100% interval * maxBaseRate

The interval is defined in seconds. The maxBaseRate is defined by raw bits per second in one direction for the Ethernet port (that is, 1 Gbps). The maxBaseRate for G-Series VC is shown in Table 5-7 on page 5-19.

Note Line utilization numbers express the average of ingress and egress traffic as a percentage of capacity.

Note Unlike E-Series cards, G-Series cards do not have a display of Trunk Utilization statistics, because G-Series cards are not Layer 2 devices.

5.6.2.3 G-Series Ethernet History Window

The Ethernet History window lists past Ethernet statistics for the previous time intervals. Depending on the selected time interval, the History window displays the statistics for each port for the number of previous time intervals as shown in Table 5-8. The parameters are defined in Table 5-9 on page 5-21.

5.6.3 ML-Series Ethernet Card Performance Monitoring Parameters

CTC provides Ethernet performance information for line-level parameters and historical Ethernet statistics. The ML-Series Ethernet performance information is divided into the Ether Ports and Packet over SONET/SDH (POS) Ports tabbed windows within the card view Performance tab window. The following sections describe PM parameters provided for the ML100T-12 and ML1000-2 Ethernet cards.

5.6.3.1 ML-Series Ether Ports Parameters

The Ether Ports window lists Ethernet PM parameter values for each Ethernet port on the card. Auto-Refresh sets a time interval at which automatic refresh will occur. The PM values are a snapshot captured at the time intervals selected in the Auto-Refresh field. Historical PM values are not stored or displayed.

Table 5-10 defines the ML-Series Ethernet card Ether Ports PM parameters.

Table 5-10 ML-Series Ether Ports PM Parameters

Parameter	Meaning
Link Status	Indicates whether the Ethernet link is receiving a valid Ethernet signal (carrier) from the attached Ethernet device; up means present, and down means not present.
ifInOctets	Indicates the number of bytes received since the last counter reset.
rxTotalPackets	Indicates the number of packets received.
ifInUcastPkts	Indicates the number of unicast packets received since the last counter reset.
ifInMulticast Pkts	Indicates the number of multicast packets received since the last counter reset.
ifInBroadcast Pkts	Indicates the number of broadcast packets received since the last counter reset.
ifInDiscards	Indicates the number of inbound packets which were chosen to discard, though no errors had been detected. This prevents them from moving to a higher-layer protocol. A possible reason for discarding such packets is to free up buffer space.
ifOutOctets	Indicates the number of bytes transmitted since the last counter reset.
txTotalPkts	Indicates the number of transmitted packets.
ifOutUcast Pkts	Indicates the number of unicast packets transmitted.
ifOutMulticast Pkts	Indicates the number of multicast packets transmitted.
ifOutBroadcast Pkts	Indicates the number or broadcast packets transmitted.
dot3StatsAlignmentErrors	Indicates the count of frames received on a particular interface that are not an integral number of octets in length and do not pass the FCS check.
dot3StatsFCSErrors	Indicates the count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check.
etherStatsUndersizePkts	Indicates the total number of packets received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.
etherStatsOversizePkts	Indicates the total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed. Note that for tagged interfaces, this number becomes 1522 bytes.
etherStatsJabbers	Indicates the total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad FCS with an integral number of octets (FCS error) or a bad FCS with a nonintegral number of octets (alignment error).
etherStatsCollissions	Indicates the number of transmit packets that are collisions; the port and the attached device transmitting at the same time caused collisions.
etherStatsDropEvents	Indicates the number of received frames dropped at the port level.
rx PauseFrames	Indicates the number of received Ethernet IEEE 802.3z pause frames.

Table 5-10 ML-Series Ether Ports PM Parameters (continued)

Parameter	Meaning
mediaIndStatsOversize Dropped	Indicates the number of received oversized packages that are dropped.
mediaIndStatsTxFramesToo Long	Indicates the number of received frames that are too long. The maximum is the programmed maximum frame size (for virtual storage access network [VSAN] support); if the maximum frame size is set to default, then the maximum is the 2112 byte payload plus the 36 byte header, which is a total of 2148 bytes.

5.6.3.2 ML-Series POS Ports Parameters

The POS Ports window lists PM parameter values for each POS port on the card. The parameters displayed depend on the framing mode employed by the ML-Series card. The two framing modes for the POS port on the ML-Series card are HDLC and frame-mapped generic framing procedure (GFP-F). For more information on provisioning a framing mode, refer to the *Cisco ONS 15454 SDH Procedure Guide*.

Auto-Refresh sets a time interval at which automatic refresh will occur. The PM values are a snapshot captured at the time intervals selected in the Auto-Refresh field. Historical PM values are not stored or displayed.

Table 5-11 defines the ML-Series Ethernet card POS Ports parameters for HDLC mode.

Table 5-11 ML-Series POS Ports Parameters for HDLC Mode

Parameter	Meaning
ifInOctets	Indicates the number of bytes received since the last counter reset.
rxTotalPkts	Indicates the number of packets received.
ifOutOctets	Indicates the number of bytes transmitted since the last counter reset.
tx TotalPkts	Indicates the number of transmitted packets.
etherStatsDropEvents	Indicates the number of received frames dropped at the port level.
rxPktsDropped Internal Congestion	Indicates the number of received packets dropped due to overflow in frame buffer.
mediaIndStatsRxFrames Truncated	Indicates the number of received frames with length of 36 bytes or less.
ifInOctets	Indicates the number of bytes received since the last counter reset.
mediaIndStatsRxFramesToo Long	Indicates the number of received frames that are too long. The maximum is the programmed maximum frame size (for VSAN support); if the maximum frame size is set to default, then the maximum is the 2112 byte payload plus the 36 byte header, which is a total of 2148 bytes.
mediaIndStatsRxFramesBad CRC	Indicates the number of received frames with CRC error.
mediaIndStatsRxShortPkts	Indicates the number of received packets that are too small.
hdlcInOctets	Indicates the number of bytes received (from the SONET/SDH path) prior to the bytes undergoing HLDC decapsulation by the policy engine.

Table 5-11 ML-Series POS Ports Parameters for HDLC Mode (continued)

Parameter	Meaning
hdlcRxAborts	Indicates the number of received packets aborted on input.
hdlcOutOctets	Indicates the number of bytes transmitted (to the SONET/SDH path) after the bytes undergoing HLDC encapsulation by the policy engine.

Table 5-12 defines the ML-Series Ethernet card POS Ports parameters for GFP-F mode.

Table 5-12 ML-Series POS Ports Parameters for GFP-F Mode

Parameter	Meaning
etherStatsDropEvents	Indicates the number of received frames dropped at the port level.
rx PktsDroppedInternal Congestion	Indicates the number of received packets dropped due to overflow in frame buffer.
gfpStatsRxFrame	Indicates the number of received GFP frames.
gfpStatsTxFrame	Indicates the umber of transmitted GFP frames.
gfpStatsRxOctets	Indicates the number of GFP bytes received.
gfpStatsTxOctets	Indicates the number of GFP bytes transmitted.
gfpStatsRxSBitErrors	Indicates the sum of all single bit errors. These are correctable in the GFP CORE HDR at the GFP-T receiver.
gfpStatsRxMBitErrors	Indicates the sum of all the multiple bit errors. These are uncorrectable in the GFP CORE HDR at the GFP-T receiver.
gfpStatsRxTypeInvalid	Indicates the number of receive packets dropped due to Client Data Frame user payload identifier (UPI) error.
gfpStatsRxCRCErrors	Indicates the number of packets received with a payload FCS error.
gfpStatsLFDRaised	Indicates the count of core HEC CRC multiple bit errors. **Note** This count is only of eHec multiple bit errors when in frame. This can be looked at as a count of when the state machine goes out of frame.
gfpStatsCSFRaised	Indicates the number of GFP client signal fail frames detected at the GFP-T receiver.
mediaIndStatsRxFrames Truncated	Indicates the number of received frames that are too long. The maximum is the programmed maximum frame size (for VSAN support). If the maximum frame size is set to default, then the size is the 2112 byte payload plus the 36 byte header, which is a total of 2148 bytes.
mediaIndStatsRxFramesToo Long	Indicates the number of received frames with a CRC error.
mediaIndStatsRxShortPkts	Indicates the number of received packets that are too small.

5.6.4 CE-Series Ethernet Card Performance Monitoring Parameters

CTC provides Ethernet performance information for line-level parameters and historical Ethernet statistics. The CE-Series Ethernet performance information is divided into the Ether Ports and POS Ports tabbed windows within the card view Performance tab window. The following sections describe PM parameters provided for the CE-100T-8 Ethernet card.

5.6.4.1 CE-Series Ether Ports Statistics Parameters

The Ethernet Ether Ports Statistics window lists Ethernet parameters at the line level. The Statistics window provides buttons to change the statistical values shown. The Baseline button resets the displayed statistics values to zero. The Refresh button manually refreshes statistics. Auto-Refresh sets a time interval at which automatic refresh occurs. The CE-Series Statistics window also has a Clear button. The Clear button sets the values on the card to zero, but does not reset the CE-Series card.

During each automatic cycle, whether auto-refreshed or manually refreshed (using the Refresh button), statistics are added cumulatively and are not immediately adjusted to equal total received packets until testing ends. To see the final PM count totals, allow a few moments for the PM window statistics to finish testing and update fully. PM counts are also listed in the CE-Series card Performance > History window.

Table 5-13 defines the CE-Series Ethernet card Ether Ports PM parameters.

Table 5-13 CE-Series Ether Ports PM Parameters

Parameter	Meaning
Time Last Cleared	Specifies a time stamp indicating the last time statistics were reset.
Link Status	Indicates whether the Ethernet link is receiving a valid Ethernet signal (carrier) from the attached Ethernet device. Up denotes present, and Down denotes not present.
ifInOctets	Indicates the number of bytes received since the last counter reset.
rxTotalPkts	Indicates the number of received packets.
ifInUcastPkts	Indicates the number of unicast packets received since the last counter reset.
ifInMulticastPkts	Indicates the number of multicast packets received since the last counter reset.
ifInBroadcastPkts	Indicates the number of broadcast packets received since the last counter reset.
ifInDiscards	Indicates the number of inbound packets that were chosen to be discarded, although no errors had been detected. This is to prevent them moving to a higher-layer protocol. A possible reason for discarding such packets is to free up buffer space.
ifInErrors	Indicates the number of inbound packets (or transmission units) that contain errors that prevent them from being delivered to a higher-layer protocol.
ifOutOctets	Indicates the number of bytes transmitted since the last counter reset.
txTotalPkts	Indicates the number of transmitted packets.
ifOutUcastPkts	Indicates the number of unicast packets transmitted.
ifOutMulticastPkts	Indicates the number of multicast packets transmitted.

Table 5-13 CE-Series Ether Ports PM Parameters (continued)

Parameter	Meaning
ifOutBroadcastPkts	Indicates the number of broadcast packets transmitted.
dot3StatsAlignmentErrors	Indicates the count of frames received on a particular interface that are not an integral number of octets in length and do not pass the FCS check.
dot3StatsFCSErrors	Indicates the count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check.
dot3StatsSingleCollisionFrames	Indicates the count of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision.
dot3StatsFrameTooLong	Indicates the count of frames received on a particular interface that exceed the maximum permitted frame size.
etherStatsUndersizePkts	Indicates the total number of packets received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.
etherStatsFragments	Indicates the total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets) and had either a bad FCS with an integral number of octets (FCS error) or a bad FCS with a nonintegral number of octets (alignment error). **Note** It is entirely normal for etherStatsFragments to increment. This is because it counts both runts (which are normal occurrences due to collisions) and noise hits.
etherStatsPkts64Octets	Indicates the total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).
etherStatsPkts65to127Octets	Indicates the total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
etherStatsPkts128to255Octets	Indicates the total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
etherStatsPkts256to511Octets	Indicates the total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
etherStatsPkts512to1023Octets	Indicates the total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
etherStatsPkts1024to1518 Octets	Indicates the total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).
etherStatsBroadcastPkts	Indicates the total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets.

Table 5-13 CE-Series Ether Ports PM Parameters (continued)

Parameter	Meaning
etherStatsMulticastPkts	Indicates the total number of good packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.
etherStatsOversizePkts	Indicates the total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed. Note that for tagged interfaces, this number becomes 1522 bytes.
etherStatsJabbers	Indicates the total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad FCS with an integral number of octets (FCS error) or a bad FCS with a nonintegral number of octets (alignment error).
etherStatsOctets	Indicates the total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets.
etherStatsCollisions	Indicates the number of transmit packets that are collisions; the port and the attached device transmitting at the same time caused collisions.
etherStatsCRCAlignErrors	Indicates the total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad FCS with an integral number of octets (FCS error) or a bad FCS with a nonintegral number of octets (alignment error).
etherStatsDropEvents	Indicates the number of received frames dropped at the port level.

5.6.4.2 CE-Series Card Ether Ports Utilization Parameters

The Ether Ports Utilization window shows the percentage of Tx and Rx line bandwidth used by the Ethernet ports during consecutive time segments. The Utilization window provides an Interval menu that enables you to set time intervals of 1 minute, 15 minutes, 1 hour, and 1 day. Line utilization is calculated with the following formulas:

Rx = (inOctets + inPkts * 20) * 8 / 100% interval * maxBaseRate

Tx = (outOctets + outPkts * 20) * 8 / 100% interval * maxBaseRate

The interval is defined in seconds. The maxBaseRate is defined by raw bits per second in one direction for the Ethernet port (that is, 1 Gbps). The maxBaseRate for CE-Series Ethernet cards is shown in Table 5-7 on page 5-19.

5.6.4.3 CE-Series Card Ether Ports History Parameters

The Ethernet Ether Ports History window lists past Ethernet statistics for the previous time intervals. Depending on the selected time interval, the History window displays the statistics for each port for the number of previous time intervals as shown in Table 5-8 on page 5-20. The parameters are those defined in Table 5-13 on page 5-26.

5.6.4.4 CE-Series POS Ports Statistics Parameters

The Ethernet POS Ports statistics window lists Ethernet POS parameters at the line level. Table 5-14 defines the CE-Series Ethernet card POS Ports parameters.

Table 5-14 CE-Series POS Ports Statistics Parameters

Parameter	Meaning
Time Last Cleared	Specifies a time stamp indicating the last time statistics were reset.
Link Status	Indicates whether the Ethernet link is receiving a valid Ethernet signal (carrier) from the attached Ethernet device; up means present, and down means not present.
ifInOctets	Indicates the number of bytes received since the last counter reset.
rxTotalPkts	Indicates the number of received packets.
ifInDiscards	Indicates the number of inbound packets that were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
ifInErrors	Indicates the number of inbound packets (or transmission units) that contained errors preventing them from being deliverable to a higher-layer protocol.
ifOutOctets	Indicates the number of bytes transmitted since the last counter reset.
txTotalPkts	Indicates the number of transmitted packets.
ifOutOversizePkts	Indicates the packets greater than 1518 bytes that were transmitted out of a port.
gfpStatsRxSBitErrors	Indicates the sum of all the single bit errors. In the GFP CORE HDR at the GFP-T receiver, these are correctable.
gfpStatsRxMBitErrors	Indicates the sum of all the multiple bit errors. In the GFP CORE HDR at the GFP-T receiver, these are uncorrectable.
gfpStatsRxTypeInvalid	Indicates the number of receive packets dropped due to Client Data Frame UPI error.
gfpStatsRxCRCErrors	Indicates the number of packets received with a payload FCS error.
gfpStatsRxCIDInvalid	Indicates the number of received packets with invalid CID.
gfpStatsCSFRaised	Indicates the number of GFP client signal fail frames detected at the GFP-T receiver.
ifInPayloadCrcErrors	Indicates the received payload CRC errors.
ifOutPayloadCrcErrors	Indicates the transmitted payload CRC errors.

5.6.4.5 CE-Series Card POS Ports Utilization Parameters

The POS Ports Utilization window shows the percentage of Tx and Rx line bandwidth used by the POS ports during consecutive time segments. The Utilization window provides an Interval menu that enables you to set time intervals of 1 minute, 15 minutes, 1 hour, and 1 day. Line utilization is calculated with the following formulas:

Rx = (inOctets * 8) / (interval * maxBaseRate)

Tx = (outOctets * 8) / (interval * maxBaseRate)

The interval is defined in seconds. The maxBaseRate is defined by raw bits per second in one direction for the Ethernet port (that is, 1 Gbps). The maxBaseRate for CE-Series cards is shown in Table 5-7 on page 5-19.

Note Line utilization numbers express the average of ingress and egress traffic as a percentage of capacity.

5.6.4.6 CE-Series Card Ether Ports History Parameters

The Ethernet POS Ports History window lists past Ethernet POS Ports statistics for the previous time intervals. Depending on the selected time interval, the History window displays the statistics for each port for the number of previous time intervals as shown in Table 5-14 on page 5-29. The parameters are defined in Table 5-8 on page 5-20.

5.7 Performance Monitoring for Optical Cards

The following sections define performance monitoring parameters and definitions for the OC3 IR 4/STM1 SH 1310 card, the OC3 IR/STM1 SH 1310-8 card, the OC12 IR/STM4 SH 1310, OC12 LR/STM4 LH 1310 card, the OC12 LR/STM4 LH 1550 card, the OC12 IR/STM4 SH 1310-4 card, the OC48 IR/STM16 SH AS 1310 card, OC48 LR/STM16 LH AS 1550 card, the OC48 ELR/STM16 EH 100 GHz card, the OC192 SR/STM64 IO 1310 card, the OC192 IR/STM64 SH 1550 card, OC192 LR/STM 64 LH 1550 card, the OC192 LR/STM64 LH ITU 15xx.xx, OC192 SR1/STM64IO Short Reach card, and the OC192/STM64 Any Reach card.

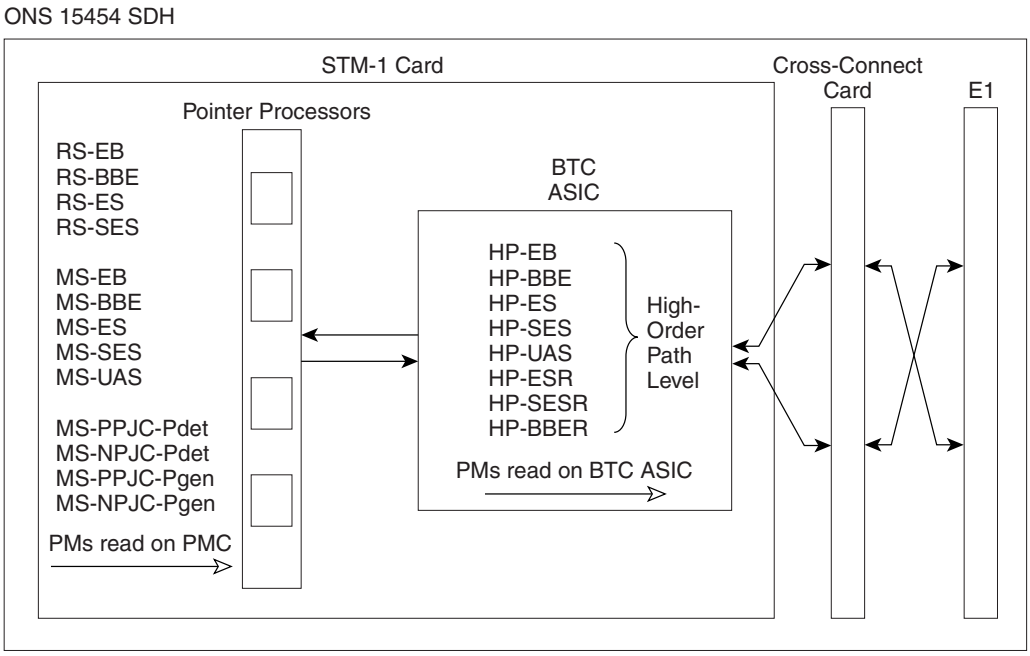
On all STM-N optical cards, errors are calculated in bits instead of blocks for B1 and B3. This means there could possibly be a slight difference between what is inserted and what is reported on CTC. In STM4, for example, there are approximately 15,000 to 30,000 bits per block (per ITU-T-G.826). If there were two bit errors within that block, the standard would require reporting one block error whereas the STM-N cards would have reported two bit errors.

When a tester inputs only single errors during testing, this issue would not appear because a tester is not fast enough to induce two errors within a single block. However, if the test is performed with an error rate, certain error rates could cause two or more errors in a block. For example, since the STM4 is roughly 622 Mbps and the block in the STM4 has 15,000 bits, there would be about 41,467 blocks in a second. If the tester inputs a $10e^{-4}$ error rate, that would create 62,200 errors per second. If the errors are distributed uniformly, then CTC could potentially report two bit errors within a single block. On the other hand, if the error ratio is $10e^{-5}$, then there will be 6,220 errors per second. If the errors are not distributed uniformly, then CTC might report one bit error within a single block. In summary, if the errors are distributed equally, then a discrepancy with the standard might be seen when a tester inputs $10e^{-4}$ or $10e^{-3}$ error rates.

5.7.1 STM-1 Card Performance Monitoring Parameters

Figure 5-7 shows where overhead bytes detected on the ASICs produce performance monitoring parameters for the OC3 IR 4/STM1 SH 1310 card and the OC3 IR/STM1 SH 1310-8 card.

Figure 5-7 PM Read Points on the STM-1 Cards



The PM parameters for the STM-1 and STM1 SH 1310-8 cards are listed in Table 5-15. The parameters are defined in Table 5-2 on page 5-4.

Table 5-15 PM Parameters for the STM-1 and STM1 SH 1310-8 Cards

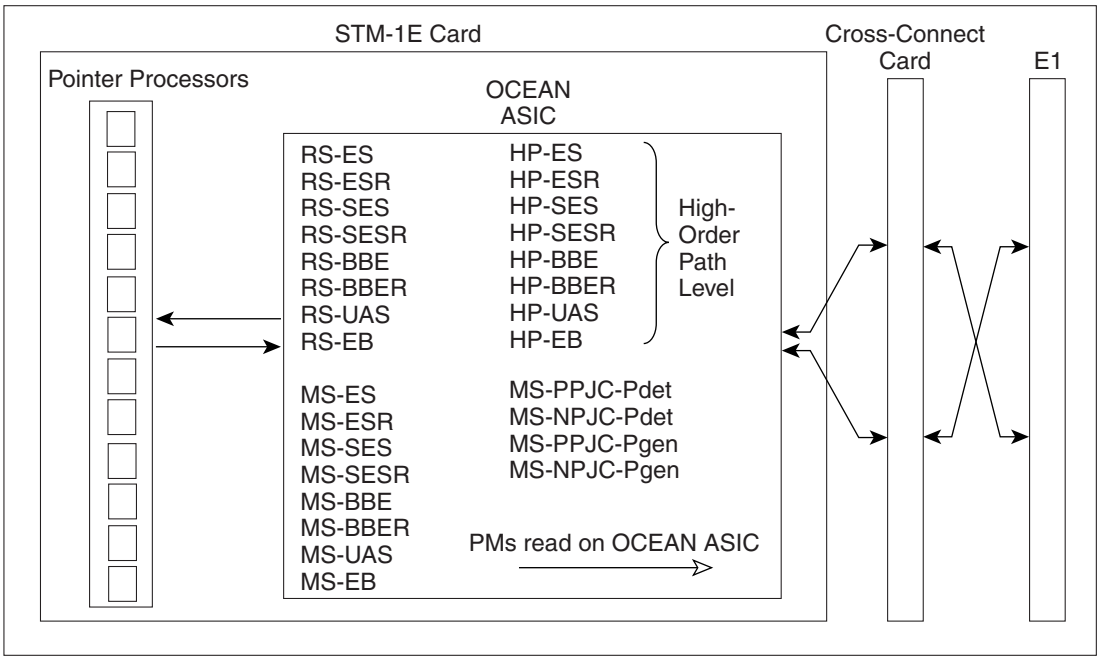
RS (NE)	MS (NE/FE)	1+1 LMSP (NE)[1, 2]	PJC (NE)[3]	VC4 and VC4-*Xc* HP Path (NE/FE[4])[5]
RS-BBE	MS-BBE	MS-PSC (1+1)	HP-PPJC-Pdet	HP-BBE
RS-EB	MS-EB	MS-PSD	HP-NPJC-Pdet	HP-BBER
RS-ES	MS-ES		HP-PPJC-Pgen	HP-EB
RS-SES	MS-SES		HP-NPJC-Pgen	HP-ES
	MS-UAS		HP-PJCS-Pdet	HP-ESR
			HP-PJCS-Pgen	HP-SES
			HP-PJCDiff	HP-SESR
				HP-UAS

1. For information about troubleshooting subnetwork connection protection (SNCP) switch counts, refer to "Alarm Troubleshooting" in the *Cisco ONS 15454 SDH Troubleshooting Guide*. For information about creating circuits that perform a switch, refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15454 SDH Reference Manual.*
2. MS-SPRing is not supported on the STM-1 card and STM-1E card; therefore, the MS-PSD-W, MS-PSD-S, and MS-PSD-R PM parameters do not increment.
3. In CTC, the count fields for the HP-PPJC and HP-NPJC PM parameters appear white and blank unless they are enabled on the Provisioning > Line tab. See the "5.3 Pointer Justification Count Performance Monitoring" section on page 5-3.
4. Far-end high-order VC4 and VC4-*Xc* path PM parameters do not apply to the STM1-4 card.
5. SDH path PM parameters do not increment unless IPPM is enabled. See the "5.2 Intermediate-Path Performance Monitoring" section on page 5-2.

5.7.2 STM-1E Card Performance Monitoring Parameters

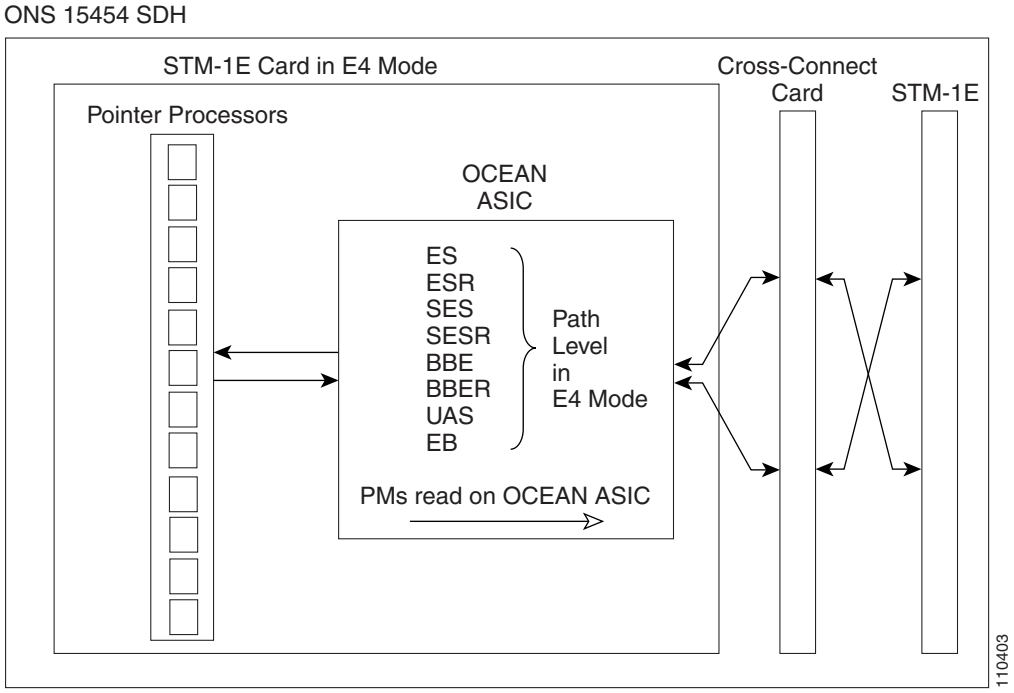
Figure 5-8 shows where overhead bytes detected on the ASICs produce performance monitoring parameters for the STM-1E card.

Figure 5-8 PM Read Points on the STM-1E Cards



Ports 9 to 12 can be provisioned as E4 framed from the Provisioning > Ports tabs. Figure 5-9 shows the VC4 performance monitoring parameters in E4 mode.

Figure 5-9 PM Read Points on the STM-1E Cards in E4 Mode



The PM parameters for the STM-1E cards are listed in Table 5-16. The parameters are defined in Table 5-2 on page 5-4.

Table 5-16 PM Parameters for the STM-1E Cards

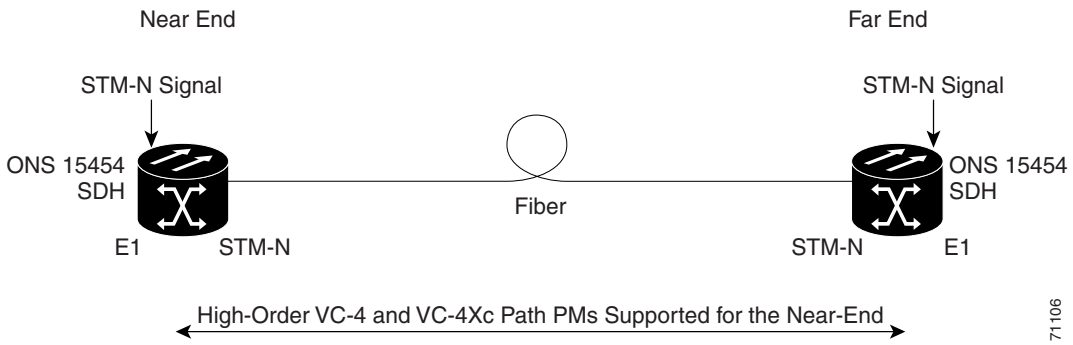
RS (NE)	MS (NE/FE)	PJC (NE)[1, 2]	VC4 and VC4-Xc HP Path (NE)[3]	VC4 and VC4-Xc Path for E4 Mode (NE)
RS-BBE	MS-BBE	HP-PPJC-Pdet	HP-BBER	BBE
RS-BBER	MS-BBER	HP-NPJC-Pdet	HP-BBER	BBER
RS-EB	MS-EB	HP-PPJC-Pgen	HP-EB	EB
RS-ES	MS-ES	HP-NPJC-Pgen	HP-ES	ES
RS-ESR	MS-ESR		HP-ESR	ESR
RS-SES	MS-SES		HP-SES	SES
RS-SESR	MS-SESR		HP-SESR	SESR
UAS-SR			HP-UAS	UAS

1. In CTC, the count fields for PPJC and NPJC PM parameters appear white and blank unless they are enabled on the Provisioning > OC3 Line tabs. See the "5.3 Pointer Justification Count Performance Monitoring" section on page 5-3.
2. For information about troubleshooting SNCP switch counts, refer to "Alarm Troubleshooting" in the *Cisco ONS 15454 SDH Troubleshooting Guide*.
3. SDH path PM parameters do not increment unless IPPM is enabled. See the "5.2 Intermediate-Path Performance Monitoring" section on page 5-2.

5.7.3 STM-4 Card Performance Monitoring Parameters

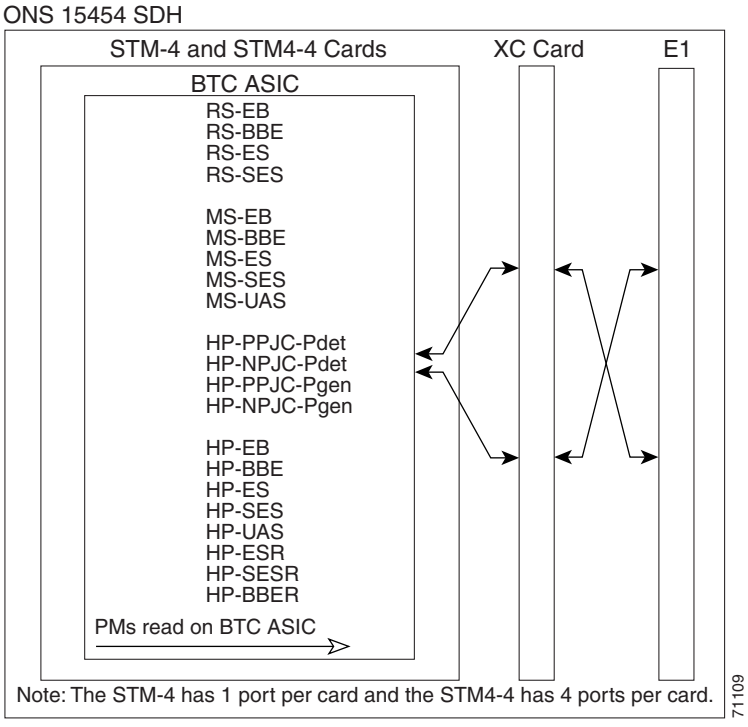
Figure 5-10 shows the signal types that support near-end and far-end PM parameters for the OC12 IR/STM4 SH 1310, OC12 LR/STM4 LH 1310 card, the OC12 LR/STM4 LH 1550 card, and the OC12 IR/STM4 SH 1310-4 card. Figure 5-11 shows where overhead bytes detected on the ASICs produce performance monitoring parameters for the

Figure 5-10 Monitored Signal Types for the STM-4 Cards



Note PM parameters on the protect VC4 are not supported for MS-SPRing.

Figure 5-11 PM Read Points on the STM-4 Cards



The PM parameters for the STM-4 cards are described in Table 5-17. The parameters are defined in Table 5-2 on page 5-4.

Table 5-17 PM Parameters for STM-4 Cards

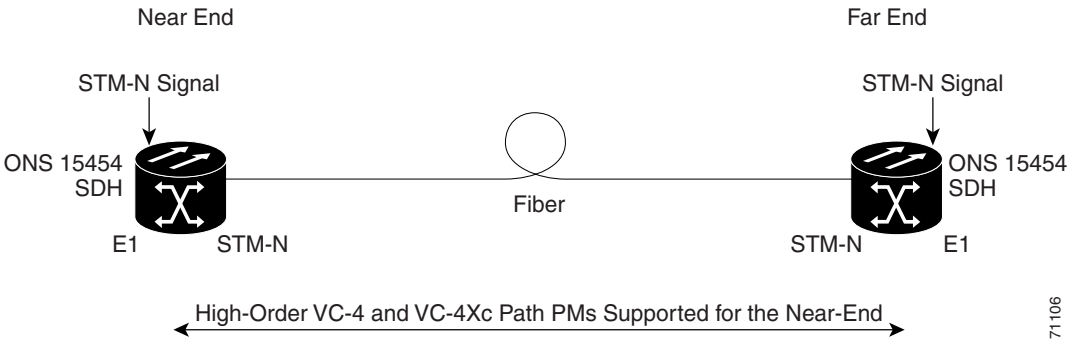
RS (NE/FE)	MS (NE/FE)	PSC (NE)[1]	PJC (NE)[2]	VC4 and VC4-Xc HP Path (NE)[3]
RS-BBE	MS-BBE	MS-PSC (1+1)	HP-PPJC-Pdet	HP-BBE
RS-EB	MS-EB	MS-PSC (MS-SPRing)	HP-NPJC-Pdet	HP-BBER
RS-ES	MS-ES	MS-PSD	HP-PPJC-Pgen	HP-EB
RS-SES	MS-SES	MS-PSC-W	HP-NPJC-Pgen	HP-ES
	MS-UAS	MS-PSD-W		HP-ESR
		MS-PSC-S		HP-SES
		MS-PSD-S		HP-SESR
		MS-PSC-R		HP-UAS
		MS-PSD-R		

1. For information about troubleshooting SNCP switch counts, refer to t"Alarm Troubleshooting" in the *Cisco ONS 15454 SDH Troubleshooting Guide*. For information about creating circuits that perform a switch, refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15454 SDH Reference Manual.*
2. In CTC, the count fields for HP-PPJC and HP-NPJC PM parameters appear white and blank unless they are enabled on the Provisioning > Line tab. See the "5.3 Pointer Justification Count Performance Monitoring" section on page 5-3.
3. SDH path PM parameters do not increment unless IPPM is enabled. See the "5.2 Intermediate-Path Performance Monitoring" section on page 5-2.

5.7.4 STM-16 and STM-64 Card Performance Monitoring Parameters

Figure 5-12 shows the signal types that support near-end and far-end PM parameters for the OC48 IR/STM16 SH AS 1310 card, the OC48 LR/STM16 LH AS 1550 card, the OC48 ELR/STM16 EH 100 GHz card, the OC192 SR/STM64 IO 1310 card, the OC192 IR/STM64 SH 1550 card, the OC192 LR/STM 64 LH 1550 card, the OC192 LR/STM64 LH ITU 15xx.xx card, the OC192 SR1/STM64IO Short Reach card, and the OC192/STM64 Any Reach card.

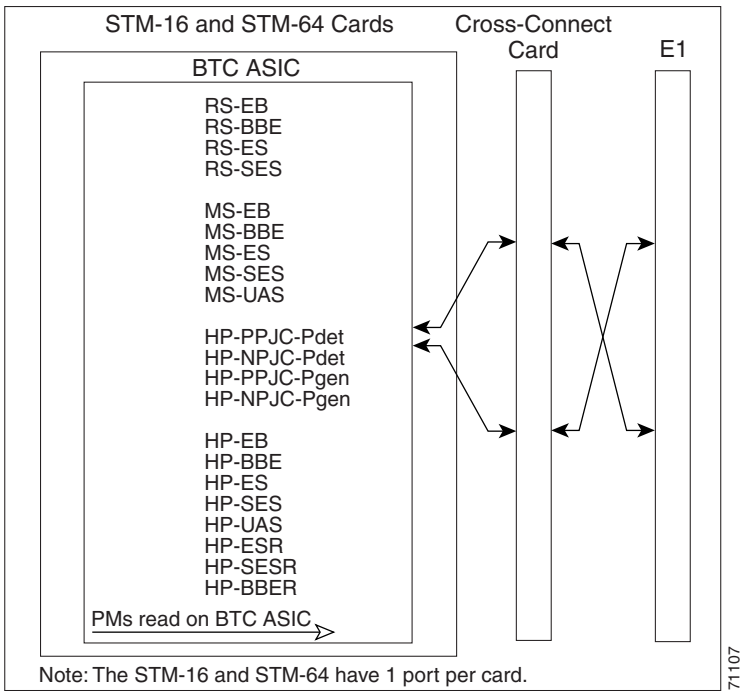
Figure 5-12 Monitored Signal Types for STM-16 and STM-64 Cards



Note PM parameters on the protect VC4 are not supported for MS-SPRing.

Figure 5-13 shows where overhead bytes detected on the ASICs produce performance monitoring parameters for STM-16 and STM-64 cards.

Figure 5-13 PM Read Points on STM-16 and STM-64 Cards



The PM parameters for STM-16 and STM-64 cards are listed Table 5-18.

Table 5-18 PM Parameters for STM-16 and STM-64 Cards

RS (NE/FE)	MS (NE/FE)	PSC (NE)[1]	PJC (NE)[2]	VC4 and VC4-Xc HP Path (NE)[3]
RS-BBE	MS-BBE	MS-PSC (1+1)	HP-PPJC-Pdet	HP-BBE
RS-EB	MS-EB	MS-PSC (MS-SPRing)	HP-NPJC-Pdet	HP-BBER
RS-ES	MS-ES	MS-PSD	HP-PPJC-Pgen	HP-EB
RS-SES	MS-SES	MS-PSC-W	HP-NPJC-Pgen	HP-ES
	MS-UAS	MS-PSD-W	HP-PJCDiff	HP-ESR
		MS-PSC-S	HP-PJCS-Pdet	HP-SES
		MS-PSD-S	HP-PJCS-Pgen	HP-SESR
		MS-PSC-R		HP-UAS
		MS-PSD-R		

1. For information about troubleshooting SNCP switch counts, refer to "Alarm Troubleshooting" in the *Cisco ONS 15454 SDH Troubleshooting Guide*. For information about creating circuits that perform a switch, refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15454 SDH Reference Manual*.
2. In CTC, the count fields for HP-PPJC and HP-NPJC PM parameters appear white and blank unless they are enabled on the Provisioning > Line tab. See the "5.3 Pointer Justification Count Performance Monitoring" section on page 5-3.
3. SDH path PM parameters do not increment unless IPPM is enabled. See the "5.2 Intermediate-Path Performance Monitoring" section on page 5-2.

5.7.5 MRC-12 Card Performance Monitoring Parameters

This section lists performance monitoring parameters for the mutirate card, also known as the MRC-12. card.

Figure 5-21 shows where overhead bytes detected on the ASICs produce performance monitoring parameters for the MRC-12 card.

Figure 5-14 PM Read Points for the MRC-12 Card

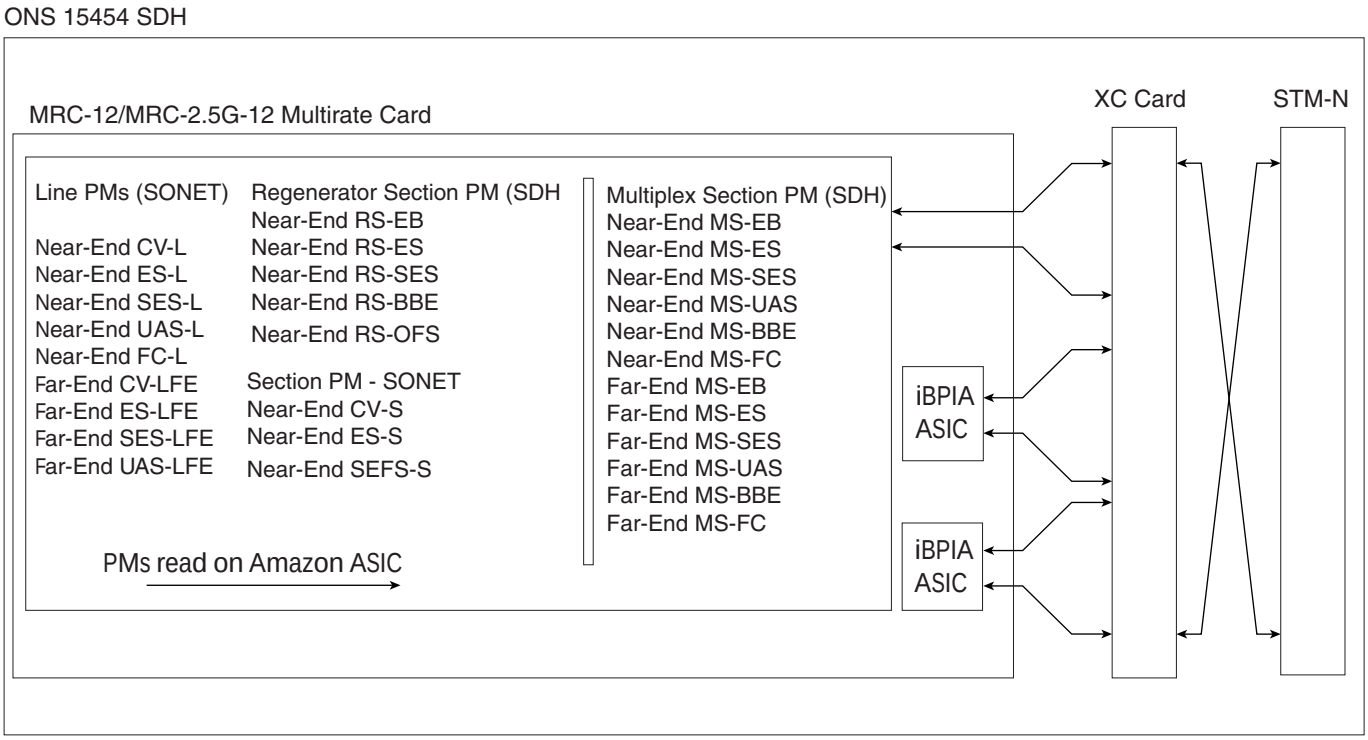


Table 5-19 lists the PM parameters for MRC-12 cards.

Table 5-19 MRC-12 Card PMs

Regenerator Section (NE)	Multiplex Section (NE)	Multiplex Section (FE)
RS-EB	MS-EB	MS-EB
RS-ES	MS-ES	MS-ES
RS-SES	MS-SES	MS-SES
RS-BBE	MS-UAS	MS-UAS
RS-OFS	MS-BBE	MS-BBE
	MS-FC	MS-FC

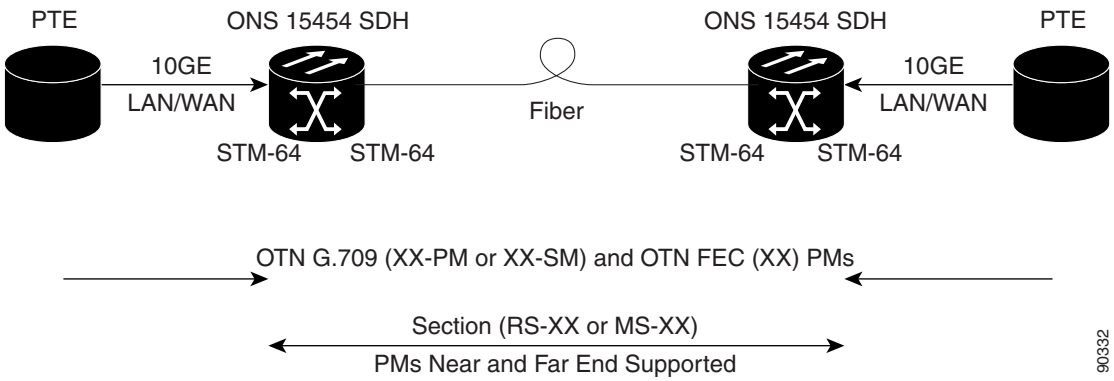
5.8 Performance Monitoring for Transponder and Muxponder Cards

This section lists performance monitoring parameters for transponder cards (TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, and TXP_MR_10E), and muxponder cards (MXP_2.5G_10G, MXP_25G_10E, MXP_MR_2.5G, and MXPP_MR_2.5G).

5.8.1 TXP_MR_10G Card Performance Monitoring Parameters

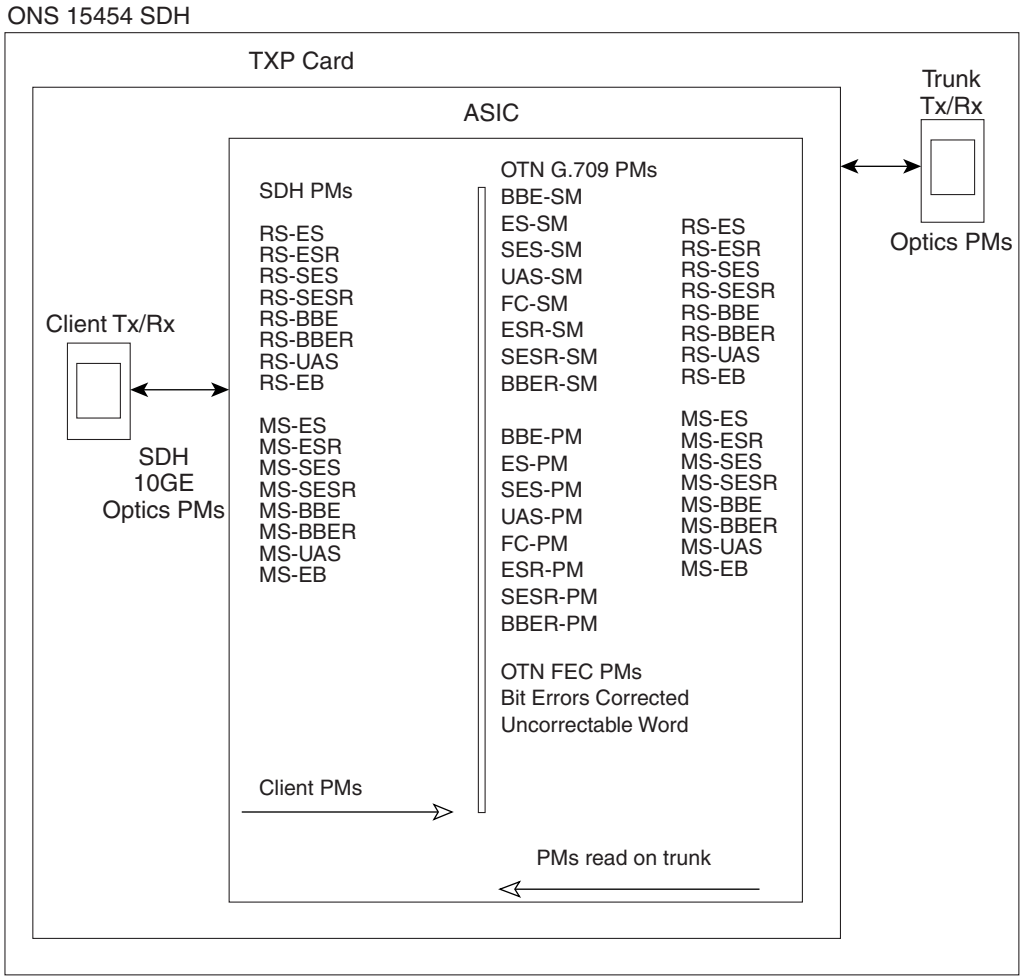
Figure 5-15 shows the signal types that support near-end and far-end PM parameters. Figure 5-16 on page 5-39 shows where overhead bytes detected on the ASICs produce performance monitoring parameters for the TXP_MR_10G card.

Figure 5-15 Monitored Signal Types for TXP_MR_10G Cards



Note The XX in Figure 5-15 on page 5-38 represents all PMs listed in Table 5-20 on page 5-40 with the given suffix and/or prefix.

Figure 5-16 PM Read Points on TXP_MR_10G Cards



The PM parameters for the TXP_MR_10G cards are described in Table 5-20. The parameters are defined in Table 5-2 on page 5-4.

Table 5-20 PM Parameters for TXP_MR_10G Cards

RS (NE/FE)	MS (NE/FE)	Physical Optics	OTN Layer (NE and FE)[1]	FEC (NE)[1]
RS-BBE	MS-BBE	LBC-AVG	ES-PM	BIT-EC
RS-BBER	MS-BBER	LBC-MAX	ES-SM	UNC-WORDS
RS-EB	MS-EB	LBC-Min	ESR-PM	
RS-ES	MS-ES	OPR-AVG	ESR-SM	
RS-ESR	MS-ESR	OPR-MAX	SES-PM	
RS-SES	MS-SES	OPR-MIN	SES-SM	
RS-SESR	MS-SESR	OPT-AVG	SESR-PM	
RS-UAS	MS-UAS	OPT-MAX	SESR-SM	
		OPT-MIN	UAS-PM	
			UAS-SM	
			BBE-PM	
			BBE-SM	
			BBER-PM	
			BBER-SM	
			FC-PM	
			FC-SM	

1. Applicable to optical channel (OCH) facility.

The Ethernet PM parameters for the TXP_MR_10G cards are described in Table 5-21.

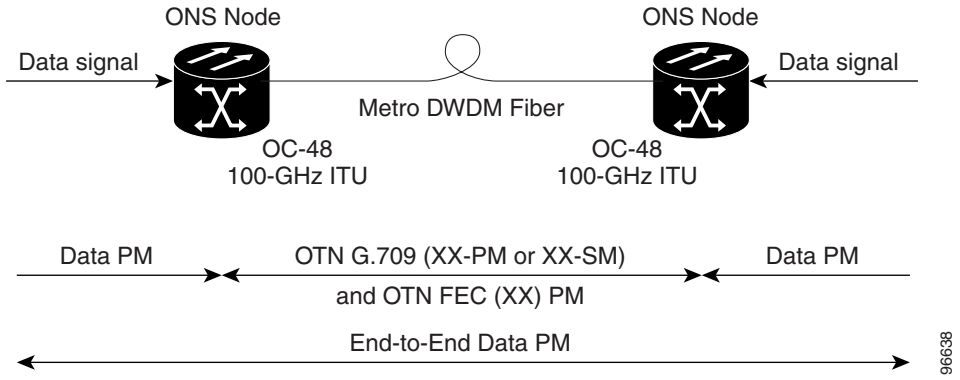
Table 5-21 Near-End or Far-End PM Parameters for Ethernet Payloads on TXP_MR_10G Cards

Parameter	Definition
Rx Packets	Number of packets received since the last counter reset.
Rx Bytes	Number of bytes received since the last counter reset.
Tx Packets	Number of packets transmitted since the last counter reset.
Tx Bytes	Number of bytes transmitted since the last counter reset.
Rx Total Errors	Total number of receive errors.
Rx FCS	Number of packets with an FCS error.
Rx Runts	Total number of frames received that are less than 64 bytes in length and have a CRC error.
Rx Jabbers	Total number of frames received that exceed the maximum 1548 bytes and contain CRC errors.
Rx Pause Frames	Number of received pause frames.
Rx Control Frames	A count of MAC control frames passed by the MAC sublayer to the MAC control sublayer.
Rx Unknown Opcode Frames	A count of MAC control frames received that contain an opcode that is not supported by the device.

5.8.2 TXP_MR_2.5G and TXPP_MR_2.5G Card Performance Monitoring Parameters

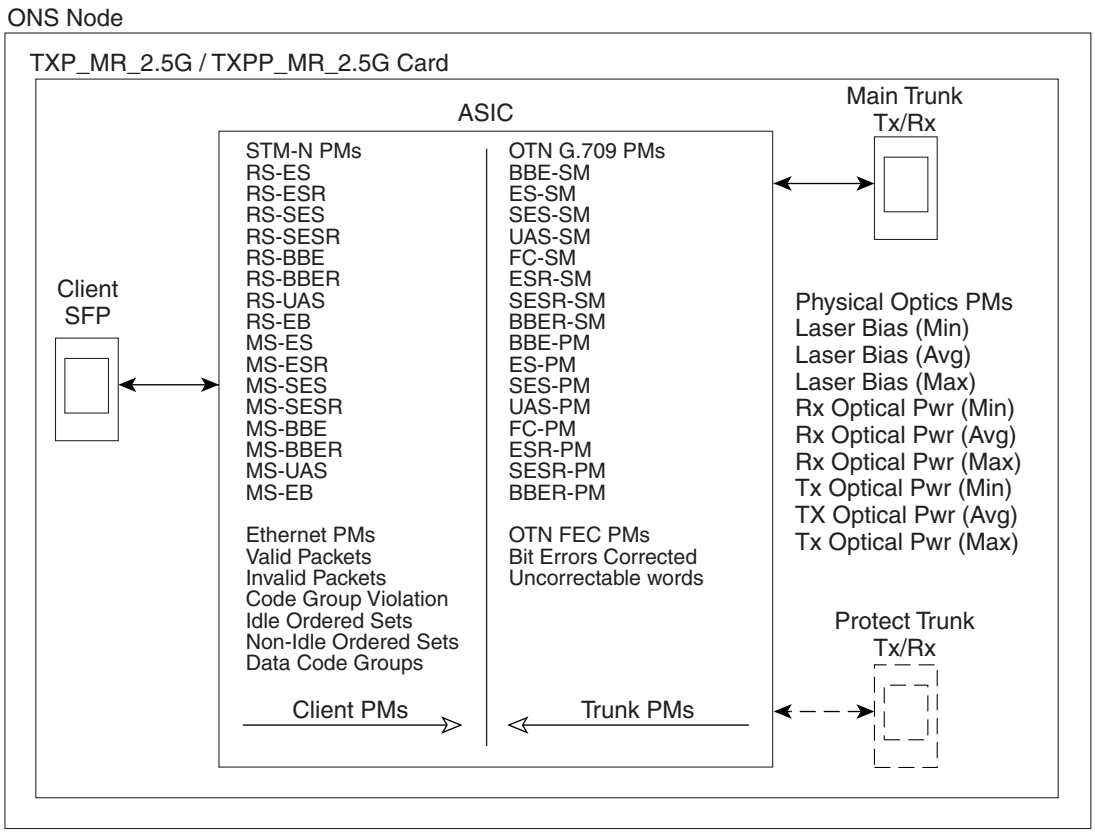
Figure 5-17 shows the signal types that support near-end and far-end PM parameters. Figure 5-18 shows where overhead bytes detected on the ASICs produce performance monitoring parameters for the TXP_MR_2.5G and TXPP_MR_2.5G cards.

Figure 5-17 Monitored Signal Types for TXP_MR_2.5G and TXPP_MR_2.5G Cards



Note The XX in Figure 5-17 represents all PMs listed in Table 5-22 with the given prefix and/or suffix.

Figure 5-18 PM Read Points on TXP_MR_2.5G and TXPP_MR_2.5G Cards



The PM parameters for the TXP_MR_2.5G and TXPP_MR_2.5G cards are described in Table 5-22. The parameters are defined in Table 5-2 on page 5-4.

Table 5-22 PM Parameters for STM-1, STM-4, and STM-16 Payloads on TXP_MR_2.5G and TXPP_MR_2.5G Cards

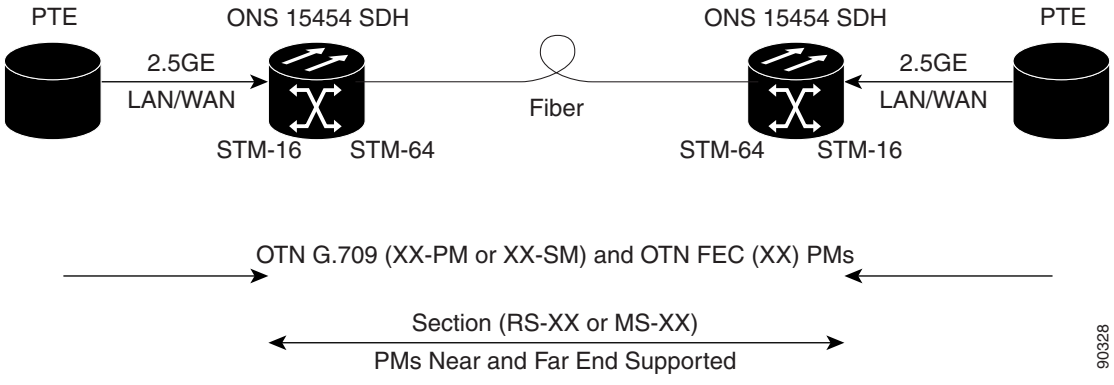
RS (NE/FE)	MS (NE/FE)	Physical Optics	8B10B (NE/FE)	OTN Layer (NE and FE)[1]	FEC (NE/FE)
RS-BBE	MS-BBE	LBC-AVG	CGV	ES-PM	BIT-EC
RS-BBER	MS-BBERM	LBC-MAX	DCG	ES-SM	UNC-WORDS
RS-EB	S-BBER	LBC-Min	IOS	ESR-PM	
RS-ES	MS-EB	OPR-AVG	IPC	ESR-SM	
RS-ESR	MS-ES	OPR-MAX	NIOS	SES-PM	
RS-SES	MS-ESR	OPR-MIN	VPC	SES-SM	
RS-SESR	MS-SES	OPT-AVG		SESR-PM	
RS-UAS	MS-SESR	OPT-MAX		SESR-SM	
	MS-UAS	OPT-MIN		UAS-PM	
				UAS-SM	
				BBE-PM	
				BBE-SM	
				BBER-PM	
				BBER-SM	
				FC-PM	
				FC-SM	

1. Enterprise System Connection (ESCON), DV6000, SDI/D1 video, and high definition television (HDTV) client signals are unframed payload data types. If the configured payload data type is unframed, line threshold provisioning and performance monitoring are not available.

5.8.3 MXP_2.5G_10G, MXP_MR_2.5G, MXPP_MR_2.5G, MXP_2.5G_10E, and TXP_MR_10E Card Performance Monitoring Parameters

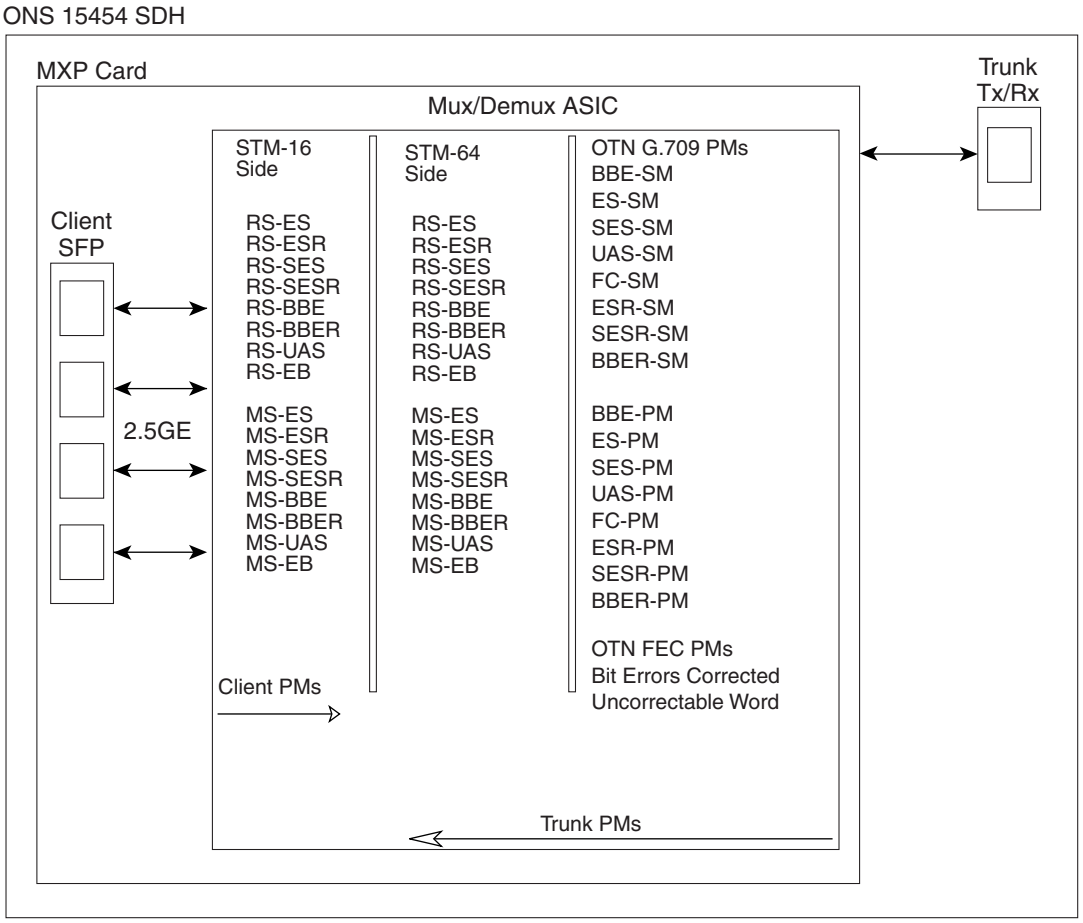
Figure 5-19 shows the signal types that support near-end and far-end PM parameters. Figure 5-20 on page 5-44 shows where overhead bytes detected on the ASICs produce performance monitoring parameters for the MXP_2.5G_10G, MXP_MR_2.5G, MXPP_MR_2.5G, MXP_2.5G_10E, and TXP_MR_10E cards.

Figure 5-19 Monitored Signal Types for MXP_2.5G_10G, MXP_MR_2.5G, MXPP_MR_2.5G, MXP_2.5G_10E, and TXP_MR_10E Cards



Note The XX in Figure 5-19 on page 5-43 represents all PMs listed in Table 5-23 on page 5-45 with the given prefix and/or suffix.

Figure 5-20 PM Read Points for MXP_2.5G_10G, MXP_MR_2.5G, MXPP_MR_2.5G, MXP_2.5G_10E, and TXP_MR_10E cards



The PM parameters for the MXP_2.5G_10G, MXP_MR_2.5G, MXPP_MR_2.5G, MXP_2.5G_10E, and TXP_MR_10E cards are described in Table 5-23. The parameters are defined in Table 5-2 on page 5-4.

Table 5-23 PM Parameters

RS (NE/FE)	MS (NE/FE)	Physical Optics	OTN Layer (NE and FE)	FEC (NE/FE)
RS-BBE	MS-BBE	LBC-AVG	ES-PM	BIT-EC
RS-BBER	MS-BBER	LBC-MAX	ES-SM	UNC-WORDS
RS-EB	MS-EB	LBC-MIN	ESR-PM	
RS-ES	MS-ES	OPR-AVG	ESR-SM	
RS-ESR	MS-ESR	OPR-MAX	SES-PM	
RS-SES	MS-SES	OPR-MIN	SES-SM	
RS-SESR	MS-SESR	OPT-AVG	SESR-PM	
RS-UAS	MS-UAS	OPT-MAX	SESR-SM	
		OPT-MIN	UAS-PM	
			UAS-SM	
			BBE-PM	
			BBE-SM	
			BBER-PM	
			BBER-SM	
			FC-PM	
			FC-SM	

5.9 Performance Monitoring for the Fibre Channel Card

The following sections define PM parameters and definitions for the FC_MR-4 card.

5.9.1 FC_MR-4 Card Performance Monitoring Parameters

CTC provides FC_MR-4 performance information, including line-level parameters, port bandwidth consumption, and historical statistics. The FC_MR-4 card performance information is divided into the Statistics, Utilization, and History tabbed windows within the card view Performance tab window.

5.9.1.1 FC_MR-4 Statistics Window

The Statistics window lists parameters at the line level. The Statistics window provides buttons to change the statistical values shown. The Baseline button resets the displayed statistics values to zero. The Refresh button manually refreshes statistics. Auto-Refresh sets a time interval at which automatic refresh occurs. The Statistics window also has a Clear button. The Clear button sets the values on the card to zero. All counters on the card are cleared.

Table 5-24 defines the FC_MR-4 card statistics parameters.

Table 5-24 FC_MR-4 Statistics Parameters

Parameter	Meaning
Time Last Cleared	A time stamp indicating the last time statistics were reset.
Link Status	Indicates whether the Fibre Channel link is receiving a valid Fibre Channel signal (carrier) from the attached Fibre Channel device; up means present, and down means not present.
Rx Frames	A count of the number of Fibre Channel frames received without errors.

Table 5-24 FC_MR-4 Statistics Parameters (continued)

Parameter	Meaning
Rx Bytes	A count of the number of bytes received without error for the Fibre Channel payload.
Tx Frames	A count of the number of transmitted Fibre Channel frames.
Tx Bytes	A count of the number of bytes transmitted from the Fibre Channel frame.
8b/10b Errors	A count of 10b errors received by the serial/deserializer (serdes 8b/10b).
Encoding Disparity Errors	A count of the disparity errors received by serdes.
Link Recoveries	A count of the FC_MR-4 software-initiated link recovery attempts toward the FC line side because of SDH protection switches.
Rx Frames bad CRC	A count of the received Fibre Channel frames with errored CRCs.
Tx Frames bad CRC	A count of the transmitted Fibre Channel frames with errored CRCs.
Rx Undersized Frames	A count of the received Fibre Channel frames < 36 bytes including CRC, start of frame (SOF), and end of frame (EOF).
Rx Oversized Frames	A count of the received Fibre Channel frames that are more than 2116 bytes of the payload. Four bytes are allowed for supporting VSAN tags sent.
GFP Rx HDR Single-bit Errors	A count of GFP single bit errors in the core header error check (CHEC).
GFP Rx HDR Multi-bit Errors	A count of GFP multibit errors in CHEC.
GGFP Rx Frames Invalid Type	A count of GFP invalid UPI field in the type field.
GFP Rx Superblk CRC Errors	A count of superblock CRC errors in the transparent GFP frame.

5.9.1.2 FC_MR-4 Utilization Window

The Utilization window shows the percentage of Tx and Rx line bandwidth used by the ports during consecutive time segments. The Utilization window provides an Interval menu that enables you to set time intervals of 1 minute, 15 minutes, 1 hour, and 1 day. Line utilization is calculated with the following formulas:

Rx = (inOctets + inPkts * 24) * 8 / 100% interval * maxBaseRate

Tx = (outOctets + outPkts * 24) * 8 / 100% interval * maxBaseRate

The interval is defined in seconds. The maxBaseRate is defined by raw bits per second in one direction for the port (that is, 1 Gbps or 2 Gbps). The maxBaseRate for FC_MR-4 cards is shown in Table 5-25.

Table 5-25 maxBaseRate for STS Circuits

STS	maxBaseRate
STS-24	850000000
STS-48	850000000 x 2[1]

1. For 1 Gigabit of bit rate being transported, there is only 850 Mbps of actual data because of 8b->10b conversion. Similarly, for 2 G of bit rate being transported there is only 850 Mbps x 2 of actual data.

Note Line utilization numbers express the average of ingress and egress traffic as a percentage of capacity.

5.9.1.3 FC_MR-4 History Window

The History window lists past FC_MR-4 statistics for the previous time intervals. Depending on the selected time interval, the History window displays the statistics for each port for the number of previous time intervals as shown in Table 5-26. The parameters are defined in Table 5-8 on page 5-20.

Table 5-26 FC_MR-4 History Statistics per Time Interval

Time Interval	Number of Intervals Displayed
1 minute	60 previous time intervals
15 minutes	32 previous time intervals
1 hour	24 previous time intervals
1 day (24 hours)	7 previous time intervals

5.10 Performance Monitoring for DWDM Cards

The following sections define performance monitoring parameters and definitions for the OPT-PRE, OPT-BST, 32WSS, 32MUX, 32MUX-O, 32DMX, 32DMX-O, 4MD-xx.x, AD-1C-xx.x, AD-2C-xx.x, AD-4C-xx.x, AD-1B-xx.x, AD-4B-xx.x, OSCM, and OSC-CSM DWDM cards.

5.10.1 Optical Amplifier Card Performance Monitoring Parameters

The PM parameters for the OPT-PRE and OPT-BST cards are listed in Table 5-27.

Table 5-27 Optical PM Parameters for OPT-PRE, and OPT-BST Cards

Optical Line	Optical Amplifier Line
OPT	OPR

5.10.2 Multiplexer and Demultiplexer Card Performance Monitoring Parameters

The PM parameters for the 32MUX-O and 32DMX-O cards are listed in Table 5-28.

Table 5-28 Optical PMs for 32MUX-O and 32DMX-O Cards

Optical Channel	Optical Line
OPR	OPT

5.10.3 4MD-xx.x Card Performance Monitoring Parameters

The PM parameters for the 4MD-xx.x cards are listed in Table 5-29.

Table 5-29 Optical PMs for 4MD-xx.x Cards

Optical Channel	Optical Band
OPR	OPT

5.10.4 OADM Channel Filter Card Performance Monitoring Parameters

The PM parameters for the AD-1C-xx.x, AD-2C-xx.x, and AD-4C-xx.x cards are listed in Table 5-30.

Table 5-30 Optical PMs for AD-1C-xx.x, AD-2C-xx.x, and AD-4C-xx.x Cards

Optical Channel	Optical Line
OPR	OPT

5.10.5 OADM Band Filter Card Performance Monitoring Parameters

The PM parameters for the AD-1B-xx.x and AD-4B-xx.x cards are listed in Table 5-31.

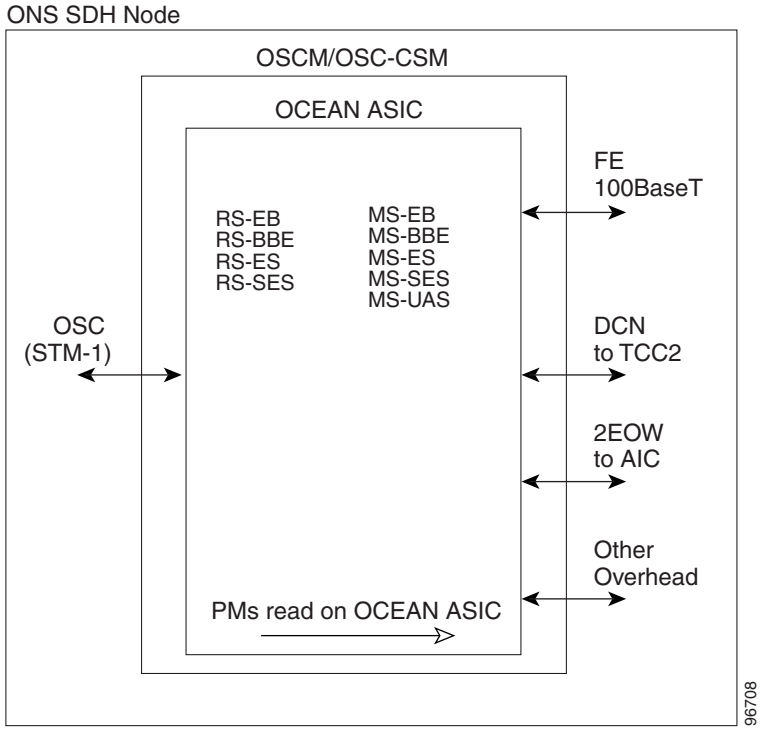
Table 5-31 Optical PMs for AD-1B-xx.x and AD-4B-xx.x Cards

Optical Line	Optical Band
OPR	OPT

5.10.6 Optical Service Channel Card Performance Monitoring Parameters

Figure 5-21 shows where overhead bytes detected on the ASICs produce performance monitoring parameters for the OSCM and OSC-CSM cards.

Figure 5-21 PM Read Points on OSCM and OSC-CSM Cards



The PM parameters for the OSCM and OSC-CSM cards are listed in Table 5-32.

Table 5-32 OSCM and OSC-CSM Card PMs

RS (NE)	MS (NE/FE)	Optics (NE)
RS-BBE	MS-BBE	OPT
RS-EB	MS-EB	
RS-ES	MS-ES	
RS-SES	MS-SES	
	MS-UAS	

SNMP

This chapter explains Simple Network Management Protocol (SNMP) as implemented by the Cisco ONS 15454 SDH.

For SNMP setup information, refer to the *Cisco ONS 15454 SDH Procedure Guide*.

Chapter topics include:

6.1 SNMP Overview

SNMP is an application-layer communication protocol that allows ONS 15454 SDH network devices to exchange management information among these systems and with other devices outside the network. Through SNMP, network administrators can manage network performance, find and solve network problems, and plan network growth.

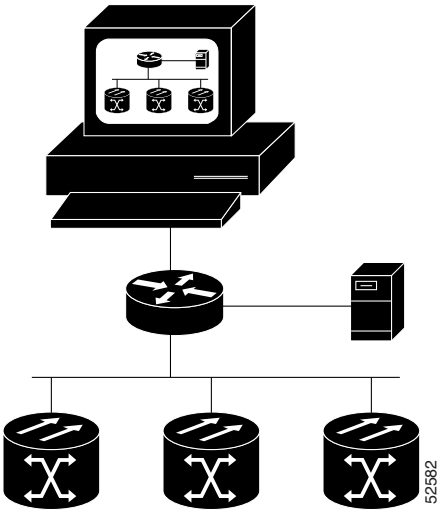
The ONS 15454 SDH uses SNMP for asynchronous event notification to a network management system (NMS). ONS SNMP implementation uses standard Internet Engineering Task Force (IETF) management information bases (MIBs) to convey node-level inventory, fault, and performance management information for generic read-only management of electrical, SDH, and Ethernet technologies. SNMP allows a generic SNMP manager such as HP OpenView Network Node Manager (NNM) or Open Systems Interconnection (OSI) NetExpert to be utilized for limited management functions.

The Cisco ONS 15454 SDH supports SNMP Version 1 (SNMPv1) and SNMP Version 2c (SNMPv2c). Both of these versions share many features, but SNMPv2c includes additional protocol operations and 64-bit performance monitoring support. This chapter describes both versions and gives SNMP configuration parameters for the ONS 15454 SDH.

Note The CERENT-MSDWDM-MIB.mib, CERENT-FC-MIB.mib, and CERENT-GENERIC-PM-MIB.mib in the CiscoV2 directory support 64-bit performance monitoring counters. The SNMPv1 MIB in the CiscoV1 directory does not contain 64-bit performance monitoring counters, but supports the lower and higher word values of the corresponding 64-bit counter. The other MIB files in the CiscoV1 and CiscoV2 directories are identical in content and differ only in format.

Figure 6-1 illustrates the basic layout idea of an SNMP-managed network.

Figure 6-1 Basic Network Managed by SNMP

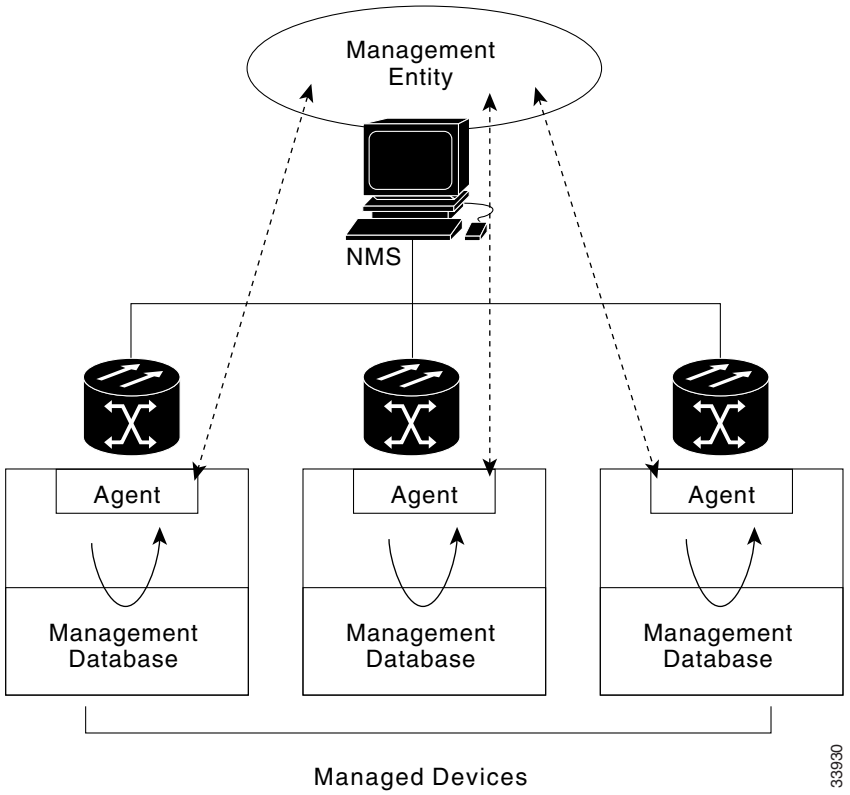


6.2 Basic SNMP Components

In general terms, an SNMP-managed network consists of a management system, agents, and managed devices.

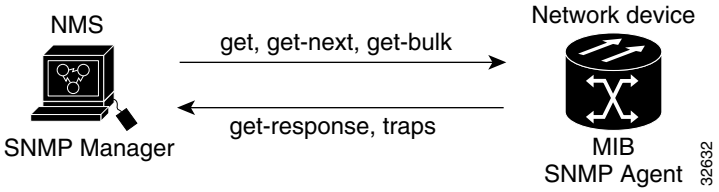
A management system such as HP OpenView executes monitoring applications and controls managed devices. Management systems execute most of the management processes and provide the bulk of memory resources used for network management. A network might be managed by one or more management systems. Figure 6-2 illustrates the relationship between the network manager, SNMP agent, and the managed devices.

Figure 6-2 Example of the Primary SNMP Components



An agent (such as SNMP) residing on each managed device translates local management information data, such as performance information or event and error information caught in software traps, into a readable form for the management system. Figure 6-3 illustrates SNMP agent get-requests that transport data to the network management software.

Figure 6-3 Agent Gathering Data from a MIB and Sending Traps to the Manager



The SNMP agent captures data from management information bases, or MIBs, which are device parameter and network data repositories, or from error or change traps.

A managed element—such as a router, access server, switch, bridge, hub, computer host, or network element (such as an ONS 15454 SDH)—is accessed through the SNMP agent. Managed devices collect and store management information, making it available via SNMP to other management systems having the same protocol compatibility.

6.3 SNMP External Interface Requirement

Since all SNMP requests come from a third-party application, the only external interface requirement is that a third-party SNMP client application can upload RFC 3273 SNMP MIB variables in the etherStatsHighCapacityTable, etherHistoryHighCapacityTable, or mediaIndependentTable.

6.4 SNMP Version Support

The ONS 15454 SDH supports SNMPv1 and SNMPv2c traps and get requests. SNMP MIBs define alarms, traps, and status. Through SNMP, NMS applications can query a management agent for data from functional entities such as Ethernet switches and SDH multiplexers using a supported MIB.

Note ONS 15454 SDH MIB files in the CiscoV1 and CiscoV2 directories are almost identical in content except for the difference in 64-bit performance monitoring features. The CiscoV2 directory contains three MIBs with 64-bit performance monitoring counters:. CERENT-MSDWDM-MIB.mib, CERENT-FC-MIB.mib, and CERENT-GENERIC-PM-MIB.mib The CiscoV1 directory does not contain any 64-bit counters, but it does support the lower and higher word values used in 64-bit counters. The two directories also have somewhat different formats.

6.5 SNMP Message Types

The ONS 15454 SDH SNMP agent communicates with an SNMP management application using SNMP messages. Table 6-1 describes these messages.

Table 6-1 ONS 15454 SDH SNMP Message Types

Operation	Description
get-request	Retrieves a value from a specific variable.
get-next-request	Retrieves the value following the named variable; this operation is often used to retrieve variables from within a table. With this operation, an SNMP manager does not need to know the exact variable name. The SNMP manager searches sequentially to find the needed variable from within the MIB.
get-response	Replies to a get-request, get-next-request, get-bulk-request, or set-request sent by an NMS.
get-bulk-request	Fills the get-response with up to the max-repetition number of get-next interactions, similar to a get-next-request.
set-request	Provides remote network monitoring (RMON) MIB.
trap	Indicates that an event has occurred. An unsolicited message is sent by an SNMP agent to an SNMP manager.

6.6 SNMP Management Information Bases

Section 6.6.1 lists IETF-standard MIBs that are implemented in the ONS 15454 SDH and shows their compilation order. Section 6.6.2 lists proprietary MIBs for the ONS 15454 SDH and shows their compilation order. Section 6.6.3 contains information about the generic threshold and performance monitoring MIBs that can be used to monitor any network element (NE) contained in the network.

6.6.1 IETF-Standard MIBS for ONS 15454 SDH

Table 6-2 lists the IETF-standard MIBs implemented in the ONS 15454 SDH SNMP agents.

First compile the MIBs in Table 6-2. Compile the Table 6-3 MIBs next.

Caution If you do not compile MIBs in the correct order, one or more might not compile correctly.

Table 6-2 IETF Standard MIBs Implemented in the ONS 15454 SDH System

RFC[1] Number	Module Name	Title/Comments
—	IANAifType-MIB.mib	Internet Assigned Numbers Authority (IANA) ifType
1213	RFC1213-MIB-rfc1213.mib	Management Information Base for Network
1907	SNMPV2-MIB-rfc1907.mib	Management of TCP/IP-based Internets: MIB-II Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)
1253	RFC1253-MIB-rfc1253.mib	OSPF Version 2 Management Information Base
1493	BRIDGE-MIB-rfc1493.mib	Definitions of Managed Objects for Bridges (This defines MIB objects for managing MAC bridges based on the IEEE 802.1D-1990 standard between Local Area Network [LAN] segments.)
2819	RMON-MIB-rfc2819.mib	Remote Network Monitoring Management Information Base
2737	ENTITY-MIB-rfc2737.mib	Entity MIB (Version 2)
2233	IF-MIB-rfc2233.mib	Interfaces Group MIB using SMIv2
2358	EtherLike-MIB-rfc2358.mib	Definitions of Managed Objects for the Ethernet-like Interface Types
2493	PerfHist-TC-MIB-rfc2493.mib	Textual Conventions for MIB Modules Using Performance History Based on 15 Minute Intervals
2495	DS1-MIB-rfc2495.mib	Definitions of Managed Objects for the DS1, E1, DS2 and E2 Interface Types
2496	DS3-MIB-rfc2496.mib	Definitions of Managed Object for the DS3/E3 Interface Type
2558	SONET-MIB-rfc2558.mib	Definitions of Managed Objects for the SONET/SDH Interface Type

Table 6-2 IETF Standard MIBs Implemented in the ONS 15454 SDH System (continued)

RFC[1] Number	Module Name	Title/Comments
2674	P-BRIDGE-MIB-rfc2674.mib Q-BRIDGE-MIB-rfc2674.mib	Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions
3273	HC-RMON-MIB	The MIB module for managing remote monitoring device implementations, augmenting the original RMON MIB as specified in RFC 2819 and RFC 1513 and RMON-2 MIB as specified in RFC 2021

1. RFC = Request for Comment

The size of mediaIndependentOwner is limited to 32 characters.

6.6.2 Proprietary ONS 15454 SDH MIBS

Each ONS system is shipped with a software CD containing applicable proprietary MIBs. Table 6-3 lists the proprietary MIBs for the ONS 15454 SDH.

Table 6-3 ONS 15454 SDH Proprietary MIBs

MIB Number	Module Name
1	CERENT-GLOBAL-REGISTRY.mib
2	CERENT-TC.mib
3	CERENT-454.mib
4	CERENT-GENERIC.mib (not applicable to ONS 15454 SDH)
5	CISCO-SMI.mib
6	CISCO-VOA-MIB.mib
7	CERENT-MSDWDM-MIB.mib
8	CISCO-OPTICAL-MONITOR-MIB.mib
9	CERENT-HC-RMON-MIB.mib
10	CERENT-ENVMON-MIB.mib
11	CERENT-GENERIC-PM-MIB.mib

Note If you cannot compile the proprietary MIBs correctly, log into the Technical Support Website at http://www.cisco.com/techsupport or call Cisco TAC (800) 553-2447.

Note When SNMP indicates that the wavelength is unknown, it means that the corresponding card (MXP_2.5G_10E, TXP_MR_10E, MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G) works with the first tunable wavelength.

6.6.3 Generic Threshold and Performance Monitoring MIBs

In Release 6.0, a new MIB called CERENT-GENERIC-PM-MIB allows network management stations (NMS) to use a single, generic MIB for accessing threshold and performance monitoring data of different interface types. The MIB is generic in the sense that it is not tied to any particular kind of interface. The MIB objects can be used to obtain threshold values, current performance monitoring (PM) counts, and historic PM statistics for each kind of monitor and any supported interval at the near end and far end.

Previously existing MIBs in the ONS 15454 SDH system provide some of these counts. For example, SDH interface 15-minute current PM counts and historic PM statistics are available using the SDH-MIB. DS-1 and DS-3 counts and statistics are available through the DS1-MIB and DS-3 MIB respectively. The generic MIB provides these types of information and also fetches threshold values and single-day statistics. In addition, the MIB supports optics and dense wavelength division multiplexing (DWDM) threshold and performance monitoring information.

The CERENT-GENERIC-PM-MIB is organized into three different tables:

- cerentGenericPmThresholdTable
- cerentGenericPmStatsCurrentTable
- cerentGenericPmStatsIntervalTable

The cerentGenericPmThresholdTable is used to obtain the threshold values for the monitor types. It is indexed based on the interface index (cerentGenericPmThresholdIndex), monitor type (cerentGenericPmThresholdMonType), location (cerentGenericPmThresholdLocation), and time period (cerentGenericPmThresholdPeriod). The syntax of cerentGenericPmThresholdMonType is type cerentMonitorType, defined in CERENT-TC.mib. The syntax of cerentGenericPmThresholdLocation is type cerentLocation, defined in CERENT-TC.mib. The syntax of cerentGenericPmThresholdPeriod is type cerentPeriod, defined in CERENT-TC.mib.

Threshold values can be provided in 64-bit and 32-bit formats. (For more information about 64-bit counters, see the "6.10.2 HC-RMON-MIB Support" section on page 6-18.) The 64-bit values in cerentGenericPmThresholdHCValue can be used with agents that support SNMPv2. The two 32-bit values (cerentGenericPmThresholdValue and cerentGenericPmThresholdOverFlowValue) can be used by NMSs that only support SNMPv1. The objects compiled in the cerentGenericPmThresholdTable are shown in Table 6-4.

Table 6-4 cerentGenericPmThresholdTable

Index Objects	Information Objects
cerentGenericPmThresholdIndex	cerentGenericPmThresholdValue
cerentGenericPmThresholdMonType	cerentGenericPmThresholdOverFlowValue
cerentGenericPmThresholdLocation	cerentGenericPmThresholdHCValue
cerentGenericPmThresholdPeriod	—

The second table within the MIB, cerentGenericPmStatsCurrentTable, compiles the current performance monitoring (PM) values for the monitor types. The table is indexed based on interface index (cerentGenericPmStatsCurrentIndex), monitor type (cerentGenericPmStatsCurrentMonType), location (cerentGenericPmStatsCurrentLocation) and time period (cerentGenericPmStatsCurrentPeriod). The syntax of cerentGenericPmStatsCurrentIndex is type cerentLocation, defined in CERENT-TC.mib. The syntax of cerentGenericPmStatsCurrentMonType is type cerentMonitor, defined in CERENT-TC.mib. The syntax of cerentGenericPmStatsCurrentPeriod is type cerentPeriod, defined in CERENT-TC.mib.

The cerentGenericPmStatsCurrentTable validates the current PM value using the cerentGenericPmStatsCurrentValid object and registers the number of valid intervals with historical PM statistics in the cerentGenericPmStatsCurrentValidIntervals object.

PM values are provided in 64-bit and 32-bit formats. The 64-bit values in cerentGenericPmStatsCurrentHCValue can be used with agents that support SNMPv2. The two 32-bit values (cerentGenericPmStatsCurrentValue and cerentGenericPmStatsCurrentOverFlowValue) can be used by NMS that only support SNMPv1. The cerentGenericPmStatsCurrentTable is shown in Table 6-5.

Table 6-5 cerentGenericPmStatsCurrentTable

Index Objects	Informational Objects
cerentGenericPmStatsCurrentIndex	cerentGenericPmStatsCurrentValue
cerentGenericPmStatsCurrentMonType	cerentGenericPmStatsCurrentOverFlowValue
cerentGenericPmStatsCurrentLocation	cerentGenericPmStatsCurrentHCValue
cerentGenericPmStatsCurrentPeriod	cerentGenericPmStatsCurrentValidData
—	cerentGenericPmStatsCurrentValidIntervals

The third table in the MIB, cerentGenericPmStatsIntervalTable, obtains historic PM values for the monitor types. This table is indexed based on the interface index, monitor type, location, time period, and interval number. It validates the current PM value in the cerentGenericPmStatsIntervalValid object.

This table is indexed based on interface index (cerentGenericPmStatsIntervalIndex), monitor type (cerentGenericPMStatsIntervalMonType), location (cerentGenericPmStatsIntervalLocation), and period (cerentGenericPmStatsIntervalPeriod). The syntax of cerentGenericPmStatsIntervalIndex is type cerentLocation, defined in CERENT-TC.mib. The syntax of cerentGenericPmStatsIntervalMonType is type cerentMonitor, defined in CERENT-TC.mib. The syntax of cerentGernicPmStatsIntervalPeriod is type cerentPeriod, defined in CERENT-TC.mib.

The table provides historic PM values in 64-bit and 32-bit formats. The 64-bit values contained in the cerentGenericPmStatsIntervalHCValue table can be used with SNMPv2 agents. The two 32-bit values (cerentGenericPmStatsIntervalValue and cerentGenericPmStatsIntervalOverFlowValue) can be used by SNMPv1 NMS. The cerentGenericPmStatsIntervalTable is shown in Table 6-6.

Table 6-6 cerentGenericPmStatsIntervalTable

Index Objects	Informational Objects
cerentGenericPmStatsIntervalIndex	cerentGenericPmStatsIntervalValue
cerentGenericPmStatsIntervalMonType	cerentGenericPmStatsIntervalOverFlowValue
cerentGenericPmStatsIntervalLocation	cerentGenericPmStatsIntervalHCValue
cerentGenericPmStatsIntervalPeriod	cerentGenericPmStatsIntervalValidData
cerentGenericPmStatsIntervalNumber	—

6.7 SNMP Trap Content

The ONS 15454 SDH generates all alarms and events, such as raises and clears, as SNMP traps. These contain the following information:

- Object IDs that uniquely identify each event with information about the generating entity (the slot or port; synchronous transport signal [STS] and Virtual Tributary [VT]; bidirectional line switched ring [BLSR], Spanning Tree Protocol [STP], etc.).
- Severity and service effect of the alarm (critical, major, minor, or event; service-affecting or non-service affecting).
- Date and time stamp showing when the alarm occurred.

6.7.1 Generic and IETF Traps

The ONS 15454 SDH supports the generic IETF traps listed in Table 6-7.

Table 6-7 ONS 15454 SDH Traps

Trap	From RFC No. MIB	Description
coldStart	RFC1907-MIB	Agent up, cold start.
warmStart	RFC1907-MIB	Agent up, warm start.
authenticationFailure	RFC1907-MIB	Community string does not match.
newRoot	RFC1493/ BRIDGE-MIB	Sending agent is the new root of the spanning tree.
topologyChange	RFC1493/ BRIDGE-MIB	A port in a bridge has changed from Learning to Forwarding or Forwarding to Blocking.
entConfigChange	RFC2737/ ENTITY-MIB	The entLastChangeTime value has changed.
dsx1LineStatusChange	RFC2495/ DS1-MIB	The value of an instance of dsx1LineStatus has changed. The trap can be used by an NMS to trigger polls. When the line status change results from a higher-level line status change (for example, a DS-3), no traps for the DS-1 are sent.
dsx3LineStatusChange	RFC2496/ DS3-MIB	The value of an instance of dsx3LineStatus has changed. This trap can be used by an NMS to trigger polls. When the line status change results in a lower-level line status change (for example, a DS-1), no traps for the lower-level are sent.
risingAlarm	RFC2819/ RMON-MIB	The SNMP trap that is generated when an alarm entry crosses the rising threshold and the entry generates an event that is configured for sending SNMP traps.
fallingAlarm	RFC2819/ RMON-MIB	The SNMP trap that is generated when an alarm entry crosses the falling threshold and the entry generates an event that is configured for sending SNMP traps.

6.7.2 Variable Trap Bindings

Each SNMP trap contains variable bindings that are used to create the MIB tables. ONS 15454 SDH traps and variable bindings are listed in Table 6-8. For each group (such as Group A), all traps within the group are associated with all of its variable bindings.

Table 6-8 ONS 15454 SDH SNMPv2 Trap Variable Bindings

Group	Trap Name(s) Associated with	Variable Binding Number	SNMPv2 Variable Bindings	Description
A	dsx1LineStatusChange (from RFC 2495)	(1)	dsx1LineStatus	This variable indicates the line status of the interface. It contains loopback, failure, received alarm and transmitted alarm information.
		(2)	dsx1LineStatusLastChange	The value of MIB II's sysUpTime object at the time this DS1 entered its current line status state. If the current state was entered prior to the last proxy-agent re-initialization, the value of this object is zero.
		(3)	cerent454NodeTime	The time that an event occurred.
		(4)	cerent454AlarmState	The alarm severity and service-affecting status. Severities are Minor, Major, and Critical. Service-affecting statuses are Service-Affecting and Non-Service Affecting.
		(5)	snmpTrapAddress	The address of the SNMP trap.
B	dsx3LineStatusChange (from RFC 2496)	(1)	dsx3LineStatus	This variable indicates the line status of the interface. It contains loopback state information and failure state information.
		(2)	dsx3LineStatusLastChange	The value of MIB II's sysUpTime object at the time this DS3/E3 entered its current line status state. If the current state was entered prior to the last re-initialization of the proxy-agent, then the value is zero.
		(3)	cerent454NodeTime	The time that an event occurred.

Table 6-8 ONS 15454 SDH SNMPv2 Trap Variable Bindings (continued)

Group	Trap Name(s) Associated with	Variable Binding Number	SNMPv2 Variable Bindings	Description
B (cont.)		(4)	cerent454AlarmState	The alarm severity and service-affecting status. Severities are Minor, Major, and Critical. Service-affecting statuses are Service-Affecting and Non-Service Affecting.
		(5)	snmpTrapAddress	The address of the SNMP trap.
C	coldStart (from RFC 1907)	(1)	cerent454NodeTime	The time that the event occurred.
	warmStart (from RFC 1907)	(2)	cerent454AlarmState	The alarm severity and service-affecting status. Severities are Minor, Major, and Critical. Service-affecting statuses are Service-Affecting and Non-Service Affecting.
	newRoot (from RFC)	(3)	snmpTrapAddress	The address of the SNMP trap.
	topologyChange (from RFC)		—	—
	entConfigChange (from RFC 2737)		—	—
	authenticationFailure (from RFC 1907)		—	—
D1	risingAlarm (from RFC 2819)	(1)	alarmIndex	This variable uniquely identifies each entry in the alarm table. When an alarm in the table clears, the alarm indexes change for each alarm listed.
		(2)	alarmVariable	The object identifier of the variable being sampled.
		(3)	alarmSampleType	The method of sampling the selected variable and calculating the value to be compared against the thresholds.
		(4)	alarmValue	The value of the statistic during the last sampling period.

Table 6-8 ONS 15454 SDH SNMPv2 Trap Variable Bindings (continued)

Group	Trap Name(s) Associated with	Variable Binding Number	SNMPv2 Variable Bindings	Description
D1 (cont.)		(5)	alarmRisingThreshold	When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single event is generated. A single event is also generated if the first sample after this entry is greater than or equal to this threshold.
		(6)	cerent454NodeTime	The time that an event occurred.
		(7)	cerent454AlarmState	The alarm severity and service-affecting status. Severities are Minor, Major, and Critical. Service-affecting statuses are Service-Affecting and Non-Service Affecting.
		(8)	snmpTrapAddress	The address of the SNMP trap.
D2	fallingAlarm (from RFC 2819)	(1)	alarmIndex	This variable uniquely identifies each entry in the alarm table. When an alarm in the table clears, the alarm indexes change for each alarm listed.
		(2)	alarmVariable	The object identifier of the variable being sampled.
		(3)	alarmSampleType	The method of sampling the selected variable and calculating the value to be compared against the thresholds.
		(4)	alarmValue	The value of the statistic during the last sampling period.
		(5)	alarmFallingThreshold	When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, a single event is generated. A single is also generated if the first sample after this entry is less than or equal to this threshold.
		(6)	cerent454NodeTime	The time that an event occurred.

Table 6-8 ONS 15454 SDH SNMPv2 Trap Variable Bindings (continued)

Group	Trap Name(s) Associated with	Variable Binding Number	SNMPv2 Variable Bindings	Description
D2 (cont.)		(7)	cerent454AlarmState	The alarm severity and service-affecting status. Severities are Minor, Major, and Critical. Service-affecting statuses are Service-Affecting and Non-Service Affecting.
		(8)	snmpTrapAddress	The address of the SNMP trap.
E	failureDetectedExternal ToTheNE (from CERENT-454-mib)	(1)	cerent454NodeTime	The time that an event occurred.
		(2)	cerent454AlarmState	The alarm severity and service-affecting status. Severities are Minor, Major, and Critical. Service-affecting statuses are Service-Affecting and Non-Service Affecting.
		(3)	cerent454AlarmObjectType	The entity that raised the alarm. The NMS should use this value to decide which table to poll for further information about the alarm.
		(4)	cerent454AlarmObjectIndex	Every alarm is raised by an object entry in a specific table. This variable is the index of objects in each table; if the alarm is interface-related, this is the index of the interface in the interface table.
		(5)	cerent454AlarmSlotNumber	The slot of the object that raised the alarm. If a slot is not relevant to the alarm, the slot number is zero.
		(6)	cerent454AlarmPortNumber	The port of the object that raised the alarm. If a port is not relevant to the alarm, the port number is zero.
		(7)	cerent454AlarmLineNumber	The object line that raised the alarm. If a line is not relevant to the alarm, the line number is zero.
		(8)	cerent454AlarmObjectName	The TL1-style user-visible name that uniquely identifies an object in the system.

Table 6-8 ONS 15454 SDH SNMPv2 Trap Variable Bindings (continued)

Group	Trap Name(s) Associated with	Variable Binding Number	SNMPv2 Variable Bindings	Description
E (cont.)		(9)	cerent454AlarmAdditionalInfo	Additional information for the alarm object. In the current version of the MIB, this object contains provisioned description for alarms that are external to the NE. If there is no additional information, the value is zero.
		(10)	snmpTrapAddress	The address of the SNMP trap.
F	performanceMonitorThresholdCrossingAlert (from CERENT-454-mib)	(1)	cerent454NodeTime	The time that an event occurred.
		(2)	cerent454AlarmState	The alarm severity and service-affecting status. Severities are Minor, Major, and Critical. Service-affecting statuses are Service-Affecting and Non-Service Affecting.
		(3)	cerent454AlarmObjectType	The entity that raised the alarm. The NMS should use this value to decide which table to poll for further information about the alarm.
		(4)	cerent454AlarmObjectIndex	Every alarm is raised by an object entry in a specific table. This variable is the index of objects in each table; if the alarm is interface-related, this is the index of the interface in the interface table.
		(5)	cerent454AlarmSlotNumber	The slot of the object that raised the alarm. If a slot is not relevant to the alarm, the slot number is zero.
		(6)	cerent454AlarmPortNumber	The port of the object that raised the alarm. If a port is not relevant to the alarm, the port number is zero.
		(7)	cerent454AlarmLineNumber	The object line that raised the alarm. If a line is not relevant to the alarm, the line number is zero.
		(8)	cerent454AlarmObjectName	The TL1-style user-visible name that uniquely identifies an object in the system.
		(9)	cerent454ThresholdMonitorType	This object indicates the type of metric being monitored.

Table 6-8 ONS 15454 SDH SNMPv2 Trap Variable Bindings (continued)

Group	Trap Name(s) Associated with	Variable Binding Number	SNMPv2 Variable Bindings	Description
F (cont.)		(10)	cerent454ThresholdLocation	Indicates whether the event occurred at the near- or far end.
		(11)	cerent454ThresholdPeriod	Indicates the sampling interval period.
		(12)	cerent454ThresholdSetValue	The value of this object is the threshold provisioned by the NMS.
		(13)	cerent454ThresholdCurrentValue	—
		(14)	cerent454ThresholdDetectType	—
		(15)	snmpTrapAddress	The address of the SNMP trap.
G	All other traps (from CERENT-454-MIB) not listed above	(1)	cerent454NodeTime	The time that an event occurred.
		(2)	cerent454AlarmState	The alarm severity and service-affecting status. Severities are Minor, Major, and Critical. Service-affecting statuses are Service-Affecting and Non-Service Affecting.
		(3)	cerent454AlarmObjectType	The entity that raised the alarm. The NMS should use this value to decide which table to poll for further information about the alarm.
		(4)	cerent454AlarmObjectIndex	Every alarm is raised by an object entry in a specific table. This variable is the index of objects in each table; if the alarm is interface-related, this is the index of the interface in the interface table.
		(5)	cerent454AlarmSlotNumber	The slot of the object that raised the alarm. If a slot is not relevant to the alarm, the slot number is zero.
		(6)	cerent454AlarmPortNumber	The port of the object that raised the alarm. If a port is not relevant to the alarm, the port number is zero.
		(7)	cerent454AlarmLineNumber	The object line that raised the alarm. If a line is not relevant to the alarm, the line number is zero.

Table 6-8 ONS 15454 SDH SNMPv2 Trap Variable Bindings (continued)

Group	Trap Name(s) Associated with	Variable Binding Number	SNMPv2 Variable Bindings	Description
G (cont.)		(8)	cerent454AlarmObjectName	The TL1-style user-visible name that uniquely identifies an object in the system.
		(9)	snmpTrapAddress	The address of the SNMP trap.

6.8 SNMP Community Names

Community names are used to group SNMP trap destinations. All ONS 15454 SDH trap destinations can be provisioned as part of SNMP communities in Cisco Transport Controller (CTC). When community names are assigned to traps, the ONS 15454 SDH treats the request as valid if the community name matches one that is provisioned in CTC. In this case, all agent-managed MIB variables are accessible to that request. If the community name does not match the provisioned list, SNMP drops the request.

6.9 Proxy Over Firewalls

SNMP and NMS applications have traditionally been unable to cross firewalls used for isolating security risks inside or from outside networks. Release 6.0 CTC enables network operations centers (NOCs) to access performance monitoring data such as remote monitoring (RMON) statistics or autonomous messages across firewalls by using an SMP proxy element installed on a firewall.

The application-level proxy transports SNMP protocol data units (PDU) between the NMS and NEs, allowing requests and responses between the NMS and NEs and forwarding NE autonomous messages to the NMS. The proxy agent requires little provisioning at the NOC and no additional provisioning at the NEs.

The firewall proxy is intended for use in a gateway network element-end network element (GNE-ENE) topology with many NEs through a single NE gateway. Up to 64 SNMP requests (such as get, getnext, or getbulk) are supported at any time behind single or multiple firewalls. The proxy interoperates with common NMS such as HP-OpenView.

For security reasons, the SNMP proxy feature must be enabled at all receiving and transmitting NEs to function. For instructions to do this, refer to the *Cisco ONS 15454 SDH Procedure Guide*.

6.10 Remote Monitoring

The ONS 15454 SDH incorporates RMON to allow network operators to monitor Ethernet card performance and events. The RMON thresholds are user-provisionable in CTC. Refer to the *Cisco ONS 15454 SDH Procedure Guide* for instructions. Note that otherwise, RMON operation is invisible to the typical CTC user.

ONS 15454 SDH system RMON is based on the IETF-standard MIB RFC 2819 and includes the following five groups from the standard MIB: Ethernet Statistics, History Control, Ethernet History, Alarm, and Event.

6.10.1 64-Bit RMON Monitoring over DCC

The ONS 15454 SDH DCC is implemented over the IP protocol, which is not compatible with Ethernet. The system builds Ethernet equipment History and Statistics tables using HDLC statistics that are gathered over the DCC (running point-to-point protocol, or PPP). This release adds RMON DCC monitoring (for both IP and Ethernet) to monitor the health of remote DCC connections.

In, R6.0, the implementation contains two MIBS for DCC interfaces. They are:

- cMediaIndependentTable—standard, rfc3273; the proprietary extension of the HC-RMON MIB used for reporting statistics
- cMediaIndependentHistoryTable—proprietary MIB used to support history

6.10.1.1 Row Creation in MediaIndependentTable

The SetRequest PDU for creating a row in the mediaIndependentTable should contain all the values required to activate a row in a single set operation along with an assignment of the status variable to createRequest (2). The SetRequest PDU for entry creation must have all the object IDs (OIDs) carrying an instance value of 0. That is, all the OIDs should be of the type OID.0.

In order to create a row, the SetRequest PDU should contain the following:

- mediaIndependentDataSource and its desired value
- mediaIndependentOwner and its desired value
- mediaIndependentStatus with a value of createRequest (2)

The mediaIndependentTable creates a row if the SetRequest PDU is valid according to the above rules. When the row is created, the SNMP agent decides the value of mediaIndependentIndex. This value is not sequentially allotted or contiguously numbered. It changes when an Ethernet interface is added or deleted. The newly created row will have mediaIndependentTable value of valid (1).

If the row already exists, or if the SetRequest PDU values are insufficient or do not make sense, the SNMP agent returns an error code.

Note mediaIndependentTable entries are not preserved if the SNMP agent is restarted.

The mediaIndependentTable deletes a row if the SetRequest PDU contains a mediaIndependentStatus with a value of invalid (4). The varbind's OID instance value identifies the row for deletion. You can recreate a deleted row in the table if desired.

6.10.1.2 Row Creation in cMediaIndependentHistoryControlTable

SNMP row creation and deletion for the cMediaIndependentHistoryControlTable follows the same processes as for the MediaIndependentTable; only the variables differ.

In order to create a row, the SetRequest PDU should contain the following:

- cMediaIndependentHistoryControlDataSource and its desired value
- cMediaIndependentHistoryControlOwner and its desired value
- cMediaIndependentHistoryControlStatus with a value of createRequest (2)

6.10.2 HC-RMON-MIB Support

For the ONS 15454 SDH, the implementation of the high-capacity remote monitoring information base (HC-RMON-MIB, or RFC 3273) enables 64-bit support of existing RMON tables. This support is provided with the etherStatsHighCapacityTable and the etherHistoryHighCapacityTable. An additional table, the mediaIndependentTable, and an additional object, hcRMONCapabilities, are also added for this support. All of these elements are accessible by any third-party SNMP client having RFC 3273 support.

6.10.3 Ethernet Statistics RMON Group

The Ethernet Statistics group contains the basic statistics monitored for each subnetwork in a single table called the etherStatsTable.

6.10.3.1 Row Creation in etherStatsTable

The SetRequest PDU for creating a row in this table should contain all the values needed to activate a row in a single set operation, and an assigned status variable to createRequest. The SetRequest PDU object ID (OID) entries must all carry an instance value, or type OID, of 0.

In order to create a row, the SetRequest PDU should contain the following:

- The etherStatsDataSource and its desired value
- The etherStatsOwner and its desired value (size of this value is limited to 32 characters)
- The etherStatsStatus with a value of createRequest (2)

The etherStatsTable creates a row if the SetRequest PDU is valid according to the above rules. When the row is created, the SNMP agent decides the value of etherStatsIndex. This value is not sequentially allotted or contiguously numbered. It changes when an Ethernet interface is added or deleted. The newly created row will have etherStatsStatus value of valid (1).

If the etherStatsTable row already exists, or if the SetRequest PDU values are insufficient or do not make sense, the SNMP agent returns an error code.

Note EtherStatsTable entries are not preserved if the SNMP agent is restarted.

6.10.3.2 Get Requests and GetNext Requests

Get requests and getNext requests for the etherStatsMulticastPkts and etherStatsBroadcastPkts columns return a value of zero because the variables are not supported by ONS 15454 SDH Ethernet cards.

6.10.3.3 Row Deletion in etherStatsTable

To delete a row in the etherStatsTable, the SetRequest PDU should contain an etherStatsStatus “invalid” value (4). The OID marks the row for deletion. If required, a deleted row can be recreated.

6.10.3.4 64-Bit etherStatsHighCapacity Table

The Ethernet statistics group contains 64-bit statistics in the etherStatsHighCapacityTable, which provides 64-bit RMON support for the HC-RMON-MIB. The etherStatsHighCapacityTable is an extension of the etherStatsTable that adds 16 new columns for performance monitoring data in 64-bit format. There is a one-to-one relationship between the etherStatsTable and etherStatsHighCapacityTable when rows are created or deleted in either table.

6.10.4 History Control RMON Group

The History Control group defines sampling functions for one or more monitor interfaces in the historyControlTable. The values in this table, as specified in RFC 2819, are derived from the historyControlTable and etherHistoryTable.

6.10.4.1 History Control Table

The RMON is sampled at one of four possible intervals. Each interval, or period, contains specific history values (also called buckets). Table 6-9 lists the four sampling periods and corresponding buckets.

The historyControlTable maximum row size is determined by multiplying the number of ports on a card by the number of sampling periods. For example, an ONS 15454 SDH E100 card contains 24 ports, which multiplied by periods allows 96 rows in the table. An E1000 card contains 14 ports, which multiplied by four periods allows 56 table rows.

Table 6-9 RMON History Control Periods and History Categories

Sampling Periods (historyControlValue Variable)	Total Values, or Buckets (historyControl Variable)
15 minutes	32
24 hours	7
1 minute	60
60 minutes	24

6.10.4.2 Row Creation in historyControlTable

The SetRequest PDU must be able to activate a historyControlTable row in one single-set operation. In order to do this, the PDU must contain all needed values and have a status variable value of 2 (createRequest). All OIDs in the SetRequest PDU should be type OID.0 type for entry creation.

To create a creation SetRequest PDU for the historyControlTable, the following values are required:

- The historyControlDataSource and its desired value
- The historyControlBucketsRequested and it desired value
- The historyControlInterval and its desired value
- The historyControlOwner and its desired value
- The historyControlStatus with a value of createRequest (2)

The historyControlBucketsRequested OID value is ignored because the number of buckets allowed for each sampling period, based upon the historyControlInterval value, is already fixed as listed in Table 6-9.

The historyControlInterval value cannot be changed from the four allowed choices. If you use another value, the SNMP agent selects the closest smaller time period from the set buckets. For example, if the set request specifies a 25-minute interval, this falls between the 15-minute (32 bucket) variable and the 60-minute (24 bucket) variable. The SNMP agent automatically selects the lower, closer value, which is 15 minutes, so it allows 32 buckets.

If the SetRequest PDU is valid, a historyControlTable row is created. If the row already exists, or if the SetRequest PDU values do not make sense or are insufficient, the SNMP agent does not create the row and returns an error code.

6.10.4.3 Get Requests and GetNext Requests

These PDUs are not restricted.

6.10.4.4 Row Deletion in historyControl Table

To delete a row from the table, the SetRequest PDU should contain a historyControlStatus value of 4 (invalid). A deleted row can be recreated.

6.10.5 Ethernet History RMON Group

The ONS 15454 SDH implements the etherHistoryTable as defined in RFC 2819. The group is created within the bounds of the historyControlTable and does not deviate from the RFC in its design.

64-bit Ethernet history for the HC-RMON-MIB is implemented in the etherHistoryHighCapacityTable, which is an extension of the etherHistoryTable. The etherHistoryHighCapacityTable adds four columns for 64-bit performance monitoring data. These two tables have a one-to-one relationship. Adding or deleting a row in one table will effect the same change in the other.

6.10.6 Alarm RMON Group

The Alarm group consists of the alarmTable, which periodically compares sampled values with configured thresholds and raises an event if a threshold is crossed. This group requires the implementation of the event group, which follows this section.

6.10.6.1 Alarm Table

The NMS uses the alarmTable to determine and provision network performance alarmable thresholds.

6.10.6.2 Row Creation in alarmTable

To create a row in the alarmTable, the SetRequest PDU must be able to create the row in one single-set operation. All OIDs in the SetRequest PDU should be type OID.0 type for entry creation. The table has a maximum number of 256 rows.

To create a creation SetRequest PDU for the alarmTable, the following values are required:

- The alarmInterval and its desired value
- The alarmVariable and its desired value
- The alarmSampleType and its desired value

- The alarmStartupAlarm and its desired value
- The alarmOwner and its desired value
- The alarmStatus with a value of createRequest (2)

If the SetRequest PDU is valid, a historyControlTable row is created. If the row already exists, or if the SetRequest PDU values do not make sense or are insufficient, the SNMP agent does not create the row and returns an error code.

In addition to the required values, the following restrictions must be met in the SetRequest PDU:

- The alarmOwner is a string of length 32 characters.
- The alarmRisingEventIndex always takes value 1.
- The alarmFallingEventIndex always takes value 2.
- The alarmStatus has only two values supported in SETs: createRequest (2) and invalid (4).
- The AlarmVariable is of the type OID.ifIndex, where ifIndex gives the interface this alarm is created on and OID is one of the OIDs supported in Table 6-10.

Table 6-10 OIDs Supported in the Alarm Table

No.	Column Name	OID	Status
1	ifInOctets	{1.3.6.1.2.1.2.2.1.10}	—
2	IfInUcastPkts	{1.3.6.1.2.1.2.2.1.11}	—
3	ifInMulticastPkts	{1.3.6.1.2.1.31.1.1.1.2}	Unsupported in E100/E1000
4	ifInBroadcastPkts	{1.3.6.1.2.1.31.1.1.1.3}	Unsupported in E100/E1000
5	ifInDiscards	{1.3.6.1.2.1.2.2.1.13}	Unsupported in E100/E1000
6	ifInErrors	{1.3.6.1.2.1.2.2.1.14}	—
7	ifOutOctets	{1.3.6.1.2.1.2.2.1.16}	—
8	ifOutUcastPkts	{1.3.6.1.2.1.2.2.1.17}	—
9	ifOutMulticastPkts	{1.3.6.1.2.1.31.1.1.1.4}	Unsupported in E100/E1000
10	ifOutBroadcastPkts	{1.3.6.1.2.1.31.1.1.1.5}	Unsupported in E100/E1000
11	ifOutDiscards	{1.3.6.1.2.1.2.2.1.19}	Unsupported in E100/E1000
12	Dot3StatsAlignmentErrors	{1.3.6.1.2.1.10.7.2.1.2}	—
13	Dot3StatsFCSErrors	{1.3.6.1.2.1.10.7.2.1.3}	—
14	Dot3StatsSingleCollisionFrames	{1.3.6.1.2.1.10.7.2.1.4}	—
15	Dot3StatsMultipleCollisionFrames	{1.3.6.1.2.1.10.7.2.1.5}	—
16	Dot3StatsDeferredTransmissions	{1.3.6.1.2.1.10.7.2.1.7}	—
17	Dot3StatsLateCollisions	{1.3.6.1.2.1.10.7.2.1.8}	—
18	Dot3StatsExcessiveCollisions	{13.6.1.2.1.10.7.2.1.9}	—
19	Dot3StatsFrameTooLong	{1.3.6.1.2.1.10.7.2.1.13}	—
20	Dot3StatsCarrierSenseErrors	{1.3.6.1.2.1.10.7.2.1.11}	Unsupported in E100/E1000
21	Dot3StatsSQETestErrors	{1.3.6.1.2.1.10.7.2.1.6}	Unsupported in E100/E1000
22	etherStatsUndersizePkts	{1.3.6.1.2.1.16.1.1.1.9}	—
23	etherStatsFragments	{1.3.6.1.2.1.16.1.1.1.11}	—

Table 6-10 OIDs Supported in the Alarm Table (continued)

No.	Column Name	OID	Status
24	etherStatsPkts64Octets	{1.3.6.1.2.1.16.1.1.1.14}	—
25	etherStatsPkts65to127Octets	{1.3.6.1.2.1.16.1.1.1.15}	—
26	etherStatsPkts128to255Octets	{1.3.6.1.2.1.16.1.1.1.16}	—
27	etherStatsPkts256to511Octets	{1.3.6.1.2.1.16.1.1.1.17}	—
28	etherStatsPkts512to1023Octets	{1.3.6.1.2.1.16.1.1.1.18}	—
29	etherStatsPkts1024to1518Octets	{1.3.6.1.2.1.16.1.1.1.19}	—
30	EtherStatsBroadcastPkts	{1.3.6.1.2.1.16.1.1.1.6}	—
31	EtherStatsMulticastPkts	{1.3.6.1.2.1.16.1.1.1.7}	—
32	EtherStatsOversizePkts	{1.3.6.1.2.1.16.1.1.1.10}	—
33	EtherStatsJabbers	{1.3.6.1.2.1.16.1.1.1.12}	—
34	EtherStatsOctets	{1.3.6.1.2.1.16.1.1.1.4}	—
35	EtherStatsCollisions	{1.3.6.1.2.1.16.1.1.1.13}	—
36	EtherStatsCollisions	{1.3.6.1.2.1.16.1.1.1.8}	—
37	EtherStatsDropEvents	{1.3.6.1.2.1.16.1.1.1.3}	Unsupported in E100/E1000 and G1000

6.10.6.3 Get Requests and GetNext Requests

These PDUs are not restricted.

6.10.6.4 Row Deletion in alarmTable

To delete a row from the table, the SetRequest PDU should contain an alarmStatus value of 4 (invalid). A deleted row can be recreated. Entries in this table are preserved if the SNMP agent is restarted.

6.10.7 Event RMON Group

The Event group controls event generation and notification. It consists of two tables: the eventTable, which is a read-only list of events to be generated, and the logTable, which is a writable set of data describing a logged event. The ONS 15454 SDH implements the logTable as specified in RFC 2819.

6.10.7.1 Event Table

The eventTable is read-only and unprovisionable. The table contains one row for rising alarms and another for falling ones. This table has the following restrictions:

- The eventType is always log-and-trap (4).
- The eventCommunity value is always a zero-length string, indicating that this event causes the trap to be despatched to all provisioned destinations.
- The eventOwner column value is always “monitor.”
- The eventStatus column value is always valid(1).

6.10.7.2 Log Table

The logTable is implemented exactly as specified in RFC 2819. The logTable is based upon data that is locally cached in a controller card. If there is a controller card protection switch, the existing logTable is cleared and a new one is started on the newly active controller card. The table contains as many rows as provided by the alarm controller.

Numerics

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

X