Cisco ONS 15600 SDH Troubleshooting Guide

Product and Documentation Releases 9.1 and 9.2.1
January 2011

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: 78-19882-01

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.

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

Cisco ONS 15600 SDH Troubleshooting Guide, Releases 9.1 and 9.2.1

CONTENTS

FIGURES

TABLES

Preface

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

This section provides the following information:

- Revision History
- Document Objectives
- Audience
- Related Documentation
- Document Conventions
- Obtaining Optical Networking Information
- Obtaining Documentation and Submitting a Service Request

Revision History

Date	Notes
June 2010	• Added this Revision History Table. • Updated the table “Alarm Logical Object Type Definitions” in the chapter “Alarm Troubleshooting”.
July 2010	• Updated table in Chapter Error Messages.

Document Objectives

The *Cisco ONS 15600 SDH Troubleshooting Guide* provides troubleshooting procedures for SDH alarms and error messages, and provides symptoms and solutions for general troubleshooting problems such as CTC and hardware errors. This guide also contains hardware replacement procedures.

Use the guide in conjunction with the appropriate publications listed in the Related Documentation section.

Audience

To use this guide you should be familiar with Cisco or equivalent optical transmission equipment.

Related Documentation

Use the *Cisco ONS 15600 SDH Troubleshooting Guide* in conjunction with the following referenced Releases 9.1 and 9.2.1 publications:

- *Cisco ONS 15600 SDH Reference Manual*
  Provides detailed card specifications, hardware and software feature descriptions, network topology information, and network element defaults.
- *Cisco ONS 15600 SDH Procedure Guide*
  Provides installation, turn up, test, and maintenance procedures.
- *Cisco ONS 15454 SDH and Cisco ONS 15600 SDH TL1 Command Guide*
  Provides a full Transaction Language One (TL1) command and autonomous message set including parameters, access identifiers (AIDs), conditions, and modifiers for the Cisco ONS 15454 SDH and Cisco ONS 15600 SDH.
- *Cisco ONS 15454 SDH and Cisco ONS 15600 SDH TL1 Reference Guide*
  Provides general information, procedures, and errors for TL1 in the Cisco ONS 15454 SDH and Cisco ONS 15600 SDH.
- *Cisco ONS 15454 SDH and Cisco ONS 15600 SDH TL1 Command Quick Reference Guide*
  Provides most commonly used Transaction Language One (TL1) command and autonomous message set including parameters, access identifiers (AIDs), conditions, and modifiers for the Cisco ONS 15454 SDH and Cisco ONS 15600 SDH.
- *Cisco ONS 15454 SDH and Cisco ONS 15600 SDH TL1 for Beginners*
  Provides Transaction Language One (TL1) command and autonomous message set information for novice Cisco ONS 15454 SDH and Cisco ONS 15600 SDH TL1 users.
- *Release Notes for the Cisco ONS 15600 SDH*
  Provides caveats, closed issues, and new feature and functionality information.
- Release Notes for the Cisco ONS 15600 SDH, Release 9.1
  Provides caveats, closed issues, and new features and functionality information.
- Release Notes for the Cisco ONS 15600 SDH, Release 9.2.1
  Provides caveats, closed issues, and new features and functionality information.

For an update on End-of-Life and End-of-Sale notices, refer to http://www.cisco.com/en/US/products/hw/optical/ps4533/prod_eol_notices_list.html.

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.

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

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

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

Warning **IMPORTANT SAFETY INSTRUCTIONS**

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

SAVE THESE INSTRUCTIONS

Waarschuwing **BELANGRIJKE VEILIGHEIDSINSTRUCTIES**

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

BEWAAR DEZE INSTRUCTIES

Varoitus **TÄRKEITÄ TURVALLISUUSOHJEITA**

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

SÄILYTÄ NÄMÄ OHJEET

Attention **IMPORTANTES INFORMATIONS DE SÉCURITÉ**

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

CONSERVEZ CES INFORMATIONS

Warnung **WICHTIGE SICHERHEITSHINWEISE**

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

BEWAHREN SIE DIESE HINWEISE GUT AUF.

Avvertenza **IMPORTANTI ISTRUZIONI SULLA SICUREZZA**

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

CONSERVARE QUESTE ISTRUZIONI

Advarsel **VIKTIGE SIKKERHETSINSTRUKSJONER**

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

TA VARE PÅ DISSE INSTRUKSJONENE

Aviso

INSTRUÇÕES IMPORTANTES DE SEGURANÇA

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

GUARDE ESTAS INSTRUÇÕES

¡Advertencia!

INSTRUCCIONES IMPORTANTES DE SEGURIDAD

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

GUARDE ESTAS INSTRUCCIONES

Varning!

VIKTIGA SÄKERHETSANVISNINGAR

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

SPARA DESSA ANVISNINGAR

FONTOS BIZTONSÁGI ELOÍRÁSOK

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

ORIZZE MEG EZEKET AZ UTASÍTÁSOKAT!

Предупреждение

ВАЖНЫЕ ИНСТРУКЦИИ ПО СОБЛЮДЕНИЮ ТЕХНИКИ БЕЗОПАСНОСТИ

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

СОХРАНИТЕ ЭТИ ИНСТРУКЦИИ

警告 重要的安全性说明

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

请保存这些安全性说明

警告 安全上の重要な注意事項

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

これらの注意事項を保管しておいてください。

주의 중요 안전 지침

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

이 지시 사항을 보관하십시오.

Aviso **INSTRUÇÕES IMPORTANTES DE SEGURANÇA**

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

GUARDE ESTAS INSTRUÇÕES

Advarsel **VIGTIGE SIKKERHEDSANVISNINGER**

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

GEM DISSE ANVISNINGER

تحذير **إرشادات الأمان الهامة**

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

قم بحفظ هذه الإرشادات

Upozorenje

VAŽNE SIGURNOSNE NAPOMENE

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

SAČUVAJTE OVE UPUTE

Upozornění

DŮLEŽITÉ BEZPEČNOSTNÍ POKYNY

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

USCHOVEJTE TYTO POKYNY

Προειδοποίηση

ΣΗΜΑΝΤΙΚΕΣ ΟΔΗΓΙΕΣ ΑΣΦΑΛΕΙΑΣ

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

ΦΥΛΑΞΤΕ ΑΥΤΕΣ ΤΙΣ ΟΔΗΓΙΕΣ

אזהרה

הוראות בטיחות חשובות

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

שמור הוראות אלה

Opomena

ВАЖНИ БЕЗБЕДНОСНИ НАПАТСТВИЈА

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

ЧУВАЈТЕ ГИ ОВИЕ НАПАТСТВИЈА

Ostrzeżenie **WAŻNE INSTRUKCJE DOTYCZĄCE BEZPIECZEŃSTWA**

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

NINIEJSZE INSTRUKCJE NALEŻY ZACHOWAĆ

Upozornenie **DÔLEŽITÉ BEZPEČNOSTNÉ POKYNY**

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

USCHOVAJTE SI TENTO NÁVOD

Obtaining Optical Networking Information

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

Where to Find Safety and Warning Information

For safety and warning information, refer to the *Cisco Optical Transport Products Safety and Compliance Information* document that accompanied the product. This publication describes the international agency compliance and safety information for the Cisco ONS 15310-MA SDH system. It also includes translations of the safety warnings that appear in the ONS 15310-MA SDH 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.

Cisco ONS Documentation Roadmap for Release 9.2.1

To quickly access publications of Cisco ONS, Release 9.2.1, see the Cisco ONS Documentation Roadmap for Release 9.2.1.

CHAPTER 1

General Troubleshooting

This chapter provides procedures for troubleshooting the most common problems encountered when operating a Cisco ONS 15600 SDH. To troubleshoot specific ONS 15600 SDH alarms, see Chapter 2, "Alarm Troubleshooting." If you cannot find what you are looking for, contact the Cisco Technical Assistance Center (1 800 553-2447).

For an update on End-of-Life and End-of-Sale notices, refer to http://cisco.com/en/US/products/hw/optical/ps4533/prod_eol_notices_list.html.

This chapter begins with the following sections on network problems:

- 1.1 Network Troubleshooting Tests, 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 network acceptance tests, refer to the *Cisco ONS 15600 SDH Procedure Guide*.

- 1.2 Troubleshooting Optical Circuit Paths With Loopbacks, page 1-6—Explains how to perform the tests described in the "1.1 Network Troubleshooting Tests" section on page 1-2 for STM-N ports and cards.
- 1.3 Troubleshooting an Ethernet Circuit Path With Loopbacks, page 1-29—Explains how to perform the tests described in the "1.1 Network Troubleshooting Tests" section on page 1-2 for Gigabit Ethernet (GIGE) ASAP card ports.

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

- 1.4 Using CTC Diagnostics, page 1-48—Provides procedures for testing LED operation and downloading a machine-readable diagnostic information file to be used by Technical Support.
- 1.5 Restoring the Database to a Previous or Original Configuration, page 1-51—Provides troubleshooting for node operation errors that might require procedures to restore software data or restoring the node to the default setup.
- 1.6 PC Connectivity Troubleshooting, page 1-52—Provides troubleshooting procedures for PC and network connectivity to the ONS 15600 SDH.
- 1.7 CTC Operation Troubleshooting, page 1-59—Provides troubleshooting procedures for Cisco Transport Controller (CTC) login or operation problems.
- 1.8 Circuits and Timing, page 1-69—Provides troubleshooting procedures for circuit creation, error reporting, and timing reference errors and alarms.
- 1.9 Fiber and Cabling, page 1-72—Provides troubleshooting procedures for fiber and cabling connectivity errors.

- 1.10 Power Supply Problems, page 1-77—Provides troubleshooting information for common power supply issues.

1.1 Network Troubleshooting Tests

Use loopbacks to test newly created circuits before running live traffic or to logically locate the source of a network failure. All ONS 15600 SDH optical (STM-N) cards allow loopbacks.

Caution On optical cards, a loopback can be applied only if the port state is Locked,maintenance for facility, terminal, and payload loopbacks, and the circuit state is Locked,maintenance for cross-connect loopbacks.

Note Do not use loopbacks to verify circuit switch times or traffic hits because it could exceed 60 msec. For switch times, a test set should be placed at both ends of the circuits.

Note When an entity is put in the administrative state, the ONS 15600 SDH suppresses all standing alarms on that entity. All alarms and events appear on the Conditions tab. You can change this behavior for the LPBKFACILITY, LPBKPAYLD, and LPBKTERMINAL alarms. To display these alarms on the Alarms tab, set the NODE.general.ReportLoopbackConditionsOnPortsInLocked,maintenance to TRUE on the NE Defaults tab.

1.1.1 Facility Loopbacks

The following sections give general information about facility loopback operations and specific information about ONS 15600 SDH card loopback activity.

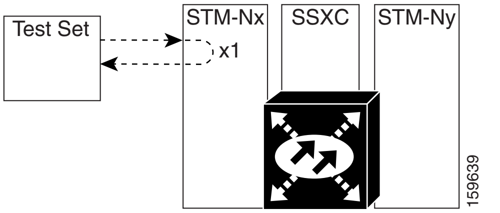
1.1.1.1 General Behavior

A facility loopback tests the line interface unit (LIU) of an ASAP card or STM-16 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 or the cabling plant as the potential cause of a network problem. To test an STM-N port or Ethernet port, connect an optical test set to the port and perform a facility loopback. Alternately, use a loopback or hairpin circuit on a card that is farther along the circuit path.

Note CTC sometimes calls a facility loopback a facility (line) loopback. This is done to clarify the direction that the loopback signal travels, that is, out from the facility toward the span.

Figure 1-1 shows a facility/payload loopback on an STM-N port.

Figure 1-1 Facility/Payload Loopback Process on an STM-N Port



Caution Before performing a facility loopback on an STM-N port, be sure the ASAP 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. Issuing a second DCC is not necessary if you are directly connected to the ONS 15600 SDH containing the loopbacked ASAP card.

1.1.1.2 Card Behavior

Loopbacks either terminate or bridge the loopback signal. 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.

The loopback itself is listed in the Conditions window. For example, the window would list the LPBKFACILITY condition for a tested port. (The Alarms window will show AS-MT, which means that alarms are suppressed on the facility during loopback.) In Software Release 8.0, an option in node defaults allows you to specify that loopback conditions be reported as alarms, even though the port or circuit is Locked,maintenance.

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 alarm indication signal (AIS) 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. For more information about placing ports into alternate states for testing, refer to the “Change Card Settings” chapter of the *Cisco ONS 15600 SDH Procedure Guide.*

Caution A lockout of protection must be executed before putting a two-fiber or four-fiber MS-SP Ring span into a facility loopback state. That is, a span lockout of one side (such as the east side) of a two-fiber MS-SP Ring 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 MS-SP Ring 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 Payload Loopbacks

The payload loopback is similar to a facility loopback but occurs on STM-64 cards. Another difference is that a payload loopback terminates and regenerates section and line overhead, while a facility loopback passes section and line overhead through, untouched. The STM-16 card executes a facility loopback by looping the signal back just before the framer chip. The STM-64 card cannot do this because of the differences in the design. To execute a loopback on an STM-64 card, the loopback signal passes through the framer chip and then terminates and regenerates line and section overhead. Since STM-64 card line and section overhead is terminated and regenerated, this type of loopback is called a payload loopback.

1.1.3 Terminal Loopbacks

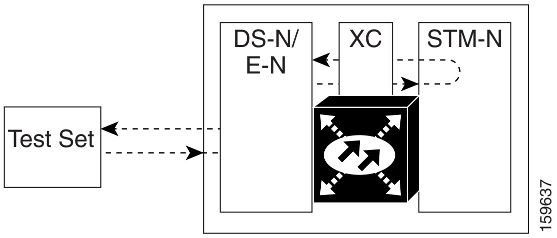
The following sections give general information about ASAP card terminal loopback operations.

1.1.3.1 General Behavior

A terminal loopback tests a circuit path as it passes through the SSXC card and loops back from the card with the loopback. Figure 1-2 shows a terminal loopback on an ASAP card. The test-set traffic enters the optical or Ethernet port and travels through the cross-connect card to the optical port. A terminal loopback turns the signal around before it reaches the LIU and sends it back through the SSXC card to the card. This test verifies that the SSXC card and terminal circuit paths are valid, but does not test the LIU on the optical card.

Note CTC sometimes calls a terminal loopback a terminal (inward) loopback. This is done to clarify the direction that the loopback signal travels, that is, inward toward the facility.

Figure 1-2 Terminal Loopback Path on an ASAP Card



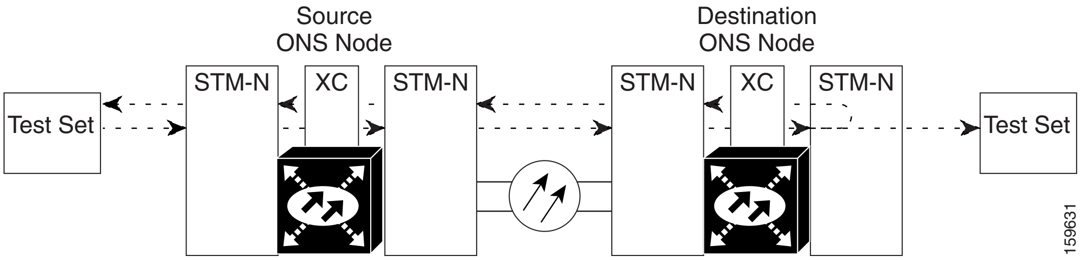
1.1.3.2 Card Behavior

ONS 15600 SDH terminal port loopbacks can either terminate or bridge the signal. (Some ONS 15600 SDH cards bridge the loopback signal, while others terminate it.)

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

An STM-N terminal loopback example is shown in Figure 1-3.

Figure 1-3 Terminal Loopback on an STM-N Card with Bridged Signal



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

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

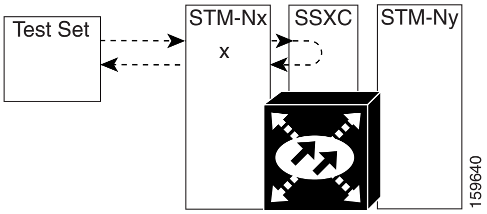
- If an electrical or optical port is in the Locked-enabled,disabled service state, it injects an AIS signal upstream and downstream.
- When an optical or Ethernet port is placed in the Locked-enabled, maintenance service state before loopback testing, the port clears the AIS signal upstream and downstream unless there is a service-affecting defect that would also cause an AIS signal to be injected. For more information about placing ports into alternate states for testing, refer to the "Change Card Settings" chapter of the *Cisco ONS 15600 SDH Procedure Guide*.

Caution A lockout of protection must be executed before putting a two-fiber or four-fiber MS-SP Ring span into a terminal loopback state. That is, a span lockout of one side (such as the east side) of a two-fiber MS-SP Ring 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 MS-SP Ring 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.

1.1.4 Cross-Connect (XC) Loopbacks

An XC loopback tests an SDH virtual container (VC) circuit path as it passes through an SSXC 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. Testing with facility or terminal loopbacks often involve taking down the whole line; however, an XC loopback allows you to create a loopback on any embedded channel at supported payloads of VC3 granularity and higher. For example, you can place a loopback on a single VC3, VC4, VC4-2c, etc. on an optical facility without interrupting the other VC circuits. Figure 1-4 shows the XC loopback path.

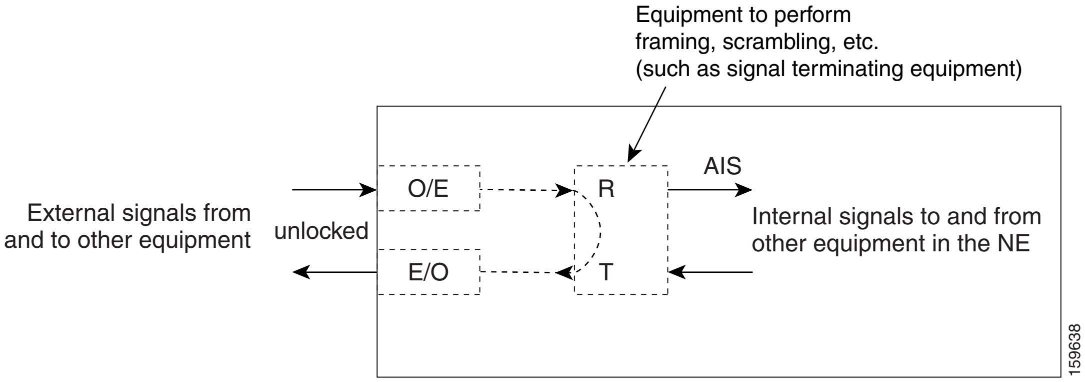
Figure 1-4 Cross-Connect Loopback Path on an STM-N Port



This test can be conducted locally or remotely through the CTC interface without on-site personnel. It takes place on an STM-16, STM-64, or ASAP port and tests the traffic path on that VC circuit through the port and SSXC. 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 AIS-P. The signal path and AIS injection are shown in Figure 1-5.

Figure 1-5 Network Element with SDH Cross-Connect Loopback Function


Equipment to perform
framing, scrambling, etc.
(such as signal terminating equipment)
External signals from
and to other equipment
unlocked
O/E
E/O
R
T
AIS
Internal signals to and from
other equipment in the NE
159638

Note If a terminal or facility loopback exists on a port, you cannot create an XC loopback on it.

Note When testing STM-64 signals with jitter analyzers, be sure to verify with the manufacturer that you are using the most current test equipment. Some test equipment has demonstrated false high jitter readings caused by accumulated jitter dependencies within the test equipment.

1.2 Troubleshooting Optical Circuit Paths With Loopbacks

Facility loopbacks or payload loopbacks, terminal loopbacks, and cross-connect (XC) 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 STM-16, STM-64, and ASAP optical ports. (For instructions on ASAP Ethernet ports, go to the "1.3 Troubleshooting an Ethernet Circuit Path With Loopbacks" section on page 1-29.) The example in this section tests an STM-N circuit on a three-node MS-SPRing. Using a series of facility, cross-connect, and terminal 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.

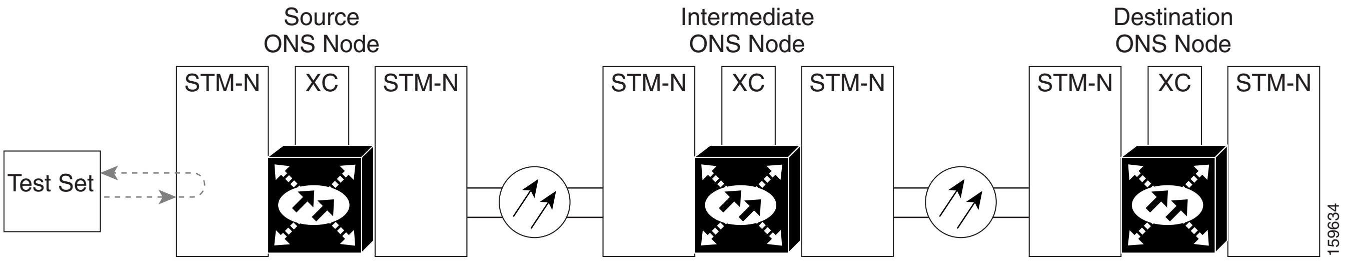
1. A facility (or payload) loopback on the source-node STM-N port
2. A terminal loopback on the source-node STM-N port
3. A cross-connect loopback on the source STM-N port
4. A facility (or payload) loopback on the intermediate-node STM-N port
5. A terminal loopback on the intermediate-node STM-N port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

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

1.2.1 Perform a Facility Loopback or Payload Loopback on a Source-Node Optical Port

The STM-16 card or ASAP card optical port facility loopback test is performed on the node source port in the network circuit. Likewise for the STM-64 payload loopback. In the testing situation used in this example, the source optical port in the source node. Completing a successful facility loopback on this port isolates the optical port as a possible failure point. Figure 1-6 shows an example of a facility loopback on a circuit source STM-N port.

Figure 1-6 Facility Loopback on a Circuit Source STM-N Port



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

Note Facility and payload loopbacks require on-site personnel.

Complete the "Create the Facility Loopback or Payload Loopback on the Source Optical Port" procedure on page 1-8.

Create the Facility Loopback or Payload Loopback on the Source Optical Port

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

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

Use appropriate cabling to attach the transmit (Tx) and receive (Rx) terminals of the optical test set to the port you are testing. The Tx and Rx terminals connect to the same port. Adjust the test set accordingly. (Refer to manufacturer instructions for test-set use.)

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

Step 3 Take the port out of service:

a. Click the **Maintenance** > **Line** (or **Maintenance** > **Optical** > **Line)** tabs.

b. Choose **Locked,maintenance** from the Admin State column for the port being tested. If multiple ports are available, select the appropriate row for the desired port.

c. Click **Apply**.

Step 4 Create the loopback. On the **Maintenance** tab, click the correct subtab:

- For an STM-16 card or STM-64 card, click the **Loopback** > **Port** tabs.
- For an ASAP card, click the **Optical** > **Loopback** > **Port** tabs.

Step 5 Choose the loopback type:

Note If multiple ports are available, choose the row associated with the correct port and then configure the loopback.

- For an STM-16 card, click **Facility** in the Loopback Type column.
- For an STM-64 card, click **Payload** in the Loopback Type column.
- For an ASAP card, click **Facility** in the Loopback Type column.

Step 6 Click **Apply**.

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

Note It is normal for the "LPBKFACILITY (STMN)" condition on page 2-87 or the "LPBKTERMINAL (GIGE)" condition on page 2-88 to appear during loopback setup. The condition clears when you remove the loopback.

Step 8 Complete the "Test and Clear the Facility Loopback or Payload Loopback Circuit" procedure on page 1-8.

Test and Clear the Facility Loopback or Payload 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 loopback:

a. Click the **Maintenance > Loopback > Port** (or **Maintenance > Optical > Loopback > Port**) tabs.

b. Choose the appropriate state (**Unlocked**; **Locked,disabled**; **Locked,maintenance**; **Unlocked,automaticInservice**) from the Admin State column for the port being tested. If multiple ports are available, select the appropriate row for the desired port. (The new administrative state will override the loopback.)

c. Click **Apply**.

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

Step 4 Complete the "Test the Optical Card" procedure on page 1-9.

Test the Optical Card

Step 1 Complete the "Replace an I/O Card" procedure on page 2-133 for the suspected bad card and replace it with a known-good one.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the procedures in the "2.8.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-121. For more information, refer to the "Maintain the Node" chapter of the *Cisco ONS 15600 SDH Procedure Guide*.

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 returned materials authorization (RMA) process. Contact Cisco Technical Support (1 800 553-2447).

Step 4 Complete the "Replace an I/O Card" procedure on page 2-133 for the faulty card.

Step 5 Clear the facility loopback:

Step 6 If the test set indicates a good circuit, no further testing is necessary with the facility or payload loopback. Clear the loopback:

a. Click the **Maintenance > Loopback > Port** (or **Maintenance > Optical > Loopback > Port**) tabs.

b. Choose the appropriate state (**Unlocked**; **Locked,disabled**; **Locked,maintenance**; **Unlocked,automaticInservice**) from the Admin State column for the port being tested. If multiple ports are available, select the appropriate row for the desired port. (The new administrative state will override the loopback.)

c. Click **Apply**.

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

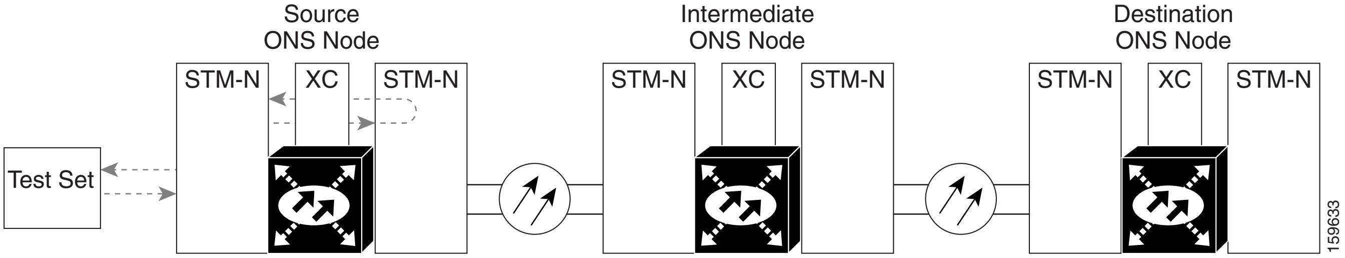
Step 7 Complete the "1.2.2 Perform a Terminal Loopback on a Source-Node Optical Port" procedure on page 1-10.

1.2.2 Perform a Terminal Loopback on a Source-Node Optical Port

The terminal loopback test is only available on ASAP card optical and Ethernet ports. (This section will only address the optical ports; Ethernet ports are covered in 1.3 Troubleshooting an Ethernet Circuit Path With Loopbacks, page 1-29.) Terminal loopbacks are not available on STM-16 or STM-64 cards.

To create a terminal loopback, create a bidirectional circuit originating on the node source optical port and looping back on the node source optical 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 1-7 shows an example of a terminal loopback on a source optical port.

Figure 1-7 Terminal Loopback on a Source-Node STM-N Port



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

Note Terminal loopbacks require on-site personnel.

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

Create the Terminal Loopback on a Source-Node Optical Port

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

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

a. If you just completed the "1.2.1 Perform a Facility Loopback or Payload Loopback on a Source-Node Optical Port" procedure on page 1-7 for an optical port, leave the optical test set hooked up.

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

c. Adjust the test set accordingly. (Refer to manufacturer instructions for test-set use.)

Step 2 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_PATH_CIRCUIT, and circuit number, such as 1.

c. Click **Next**.

d. In the next Circuit Creation dialog box, give the circuit an easily identifiable name such as Opt1toOpt2.

e. Leave the Bidirectional check box checked.

f. Click **Next**.

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

h. Click **Next**.

i. In the Circuit Creation destination dialog box, use the same Node, card Slot, Port, and VC 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 3 Confirm that the newly created circuit appears on the Circuits tab list as a two-way circuit.

Note It is normal for the "LPBKTERMINAL (STMN)" condition on page 2-88 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. In node view, double-click the ASAP card.

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

c. Select **Locked,maintenance** from the Admin State column. If there are multiple available circuits, select the row appropriate for the desired port.

d. Select **Terminal** from the Loopback Type column.

e. Click **Apply**.

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

Step 5 Complete the "Test and Clear the Terminal Loopback Circuit" procedure on page 1-11.

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 ASAP in the source node.

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

b. Choose the appropriate state (**Unlocked**; **Locked,disabled**; **Locked,maintenance**; **Unlocked,automaticInservice**) from the Admin State column for the port being tested. If multiple ports are available, select the appropriate row for the desired port. (The new administrative state will override the loopback.)

c. Click **Apply**.

d. 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 ASAP Card" procedure on page 1-12.

Test the ASAP Card

Step 1 Determine whether you are experiencing trouble on a single SFP (PPM), on all PPMs within a 4PIO (PIM), or on all 4PIO used in that ASAP card. If there is only partial failure, you might be able to replace this part rather than the entire card.

Step 2 If the errors are being observed on one port but not all ports of the ASAP, you might only need to replace that SFP (PPM). Remove the errored SFP (PPM) and replace it with a known-good SFP (PPM) by completing the procedures for this in the "Install Cards and Fiber-Optic Cable" chapter of the *Cisco ONS 15600 SDH Procedure Guide*.

Step 3 If all SFPs (PPMs) on a particular 4PIO (PIM) are experiencing problems, the 4PIO (PIM) is indicated. Remove this 4PIO (PIM) and replace it with a known-good one using the procedures for this in the "Install Cards and Fiber-Optic Cable" chapter of the *Cisco ONS 15600 SDH Procedure Guide*.

Step 4 If the trouble still is not located, complete the "Replace an I/O Card" procedure on page 2-133 for the suspected bad ASAP card and replace it with a known-good one.

Step 5 Resend test traffic on the loopback circuit with a known-good card.

Step 6 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. Contact Cisco Technical Support (1 800 553-2447).

Step 7 Complete the "Replace an I/O Card" procedure on page 2-133 for the defective card.

Step 8 Clear the terminal loopback on the port before testing the next segment of the network circuit path:

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

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

b. Choose the appropriate state (**Unlocked**; **Locked,disabled**; **Locked,maintenance**; **Unlocked,automaticInservice**) from the Admin State column for the port being tested. If multiple ports are available, select the appropriate row for the desired port. (The new administrative state will override the loopback.)

c. Click **Apply**.

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

Step 9 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 10 Complete the "1.2.3 Perform an XC Loopback on the Source Optical Port" procedure on page 1-13.

1.2.3 Perform an XC Loopback on the Source Optical Port

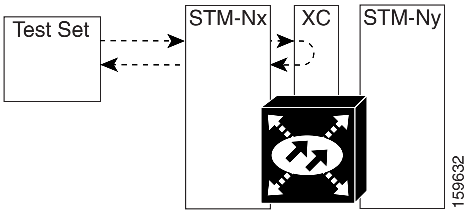
Note This procedure is performed from an STM-N card or ASAP card optical port to test the cross-connect circuit connection.

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

Note XC loopbacks do not require on-site personnel.

The XC loopback test is available for STM-16, STM-64, and ASAP cards and occurs on an optical circuit transiting the SSXC card in a network circuit. Completing a successful XC loopback from an optical port through the SSXC card eliminates the SSXC card as the source of trouble for a faulty circuit. Figure 1-8 shows an example of an XC loopback path on a source STM-N port.

Figure 1-8 XC Loopback on a Source STM-N Port



Complete the "Create the XC Loopback on the Source-Node Optical Port" procedure on page 1-13.

Create the XC Loopback on the Source-Node Optical Port

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

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

a. If you just completed the "1.2.2 Perform a Terminal Loopback on a Source-Node Optical Port" procedure on page 1-10, leave the optical test set hooked up to the source-node port.

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

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

Step 3 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 Admin 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 STM-N card to display the card view.

b. Click the **Maintenance > Loopback > VC3** or **VC4** tabs (or **Maintenance > Optical > Loopback > VC3** or **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 1-14.

Test and Clear the XC 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 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 > VC3** or **VC4** tabs (or **Maintenance > Optical > Loopback > VC3** or **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 Alternate SSXC Card" procedure on page 1-14.

Test the Alternate SSXC Card

Step 1 Do a manual data copy switch of the SSXC cards before retesting the XC loopback circuit:

a. In node view, select the **Maintenance > Preferred Copy** tabs.

b. In the **Set Preferred** drop-down list, select the alternate copy. (For example, if Copy B is preferred and in use, select Copy A.)

Note CTC Copy A refers to the SSXC card in Slot 6. Copy B refers to the SSXC card in Slot 8. Either copy might be chosen as the preferred copy SSXC. The other SSXC is called the alternate SSXC in this chapter.

c. Click **Apply**.

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

Note If you attempt a preferred copy switch and the switch is unsuccessful, a problem is present with the alternate SSXC.

e. Click **Refresh** until the tab shows that the alternate copy you selected is now the preferred copy. The Currently Used field will show the newly-selected preferred copy.

Step 2 Resend test traffic on the XC loopback circuit.

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

Step 3 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 from the Circuits tab list. If the test set indicates a good circuit, the problem might be a defective cross-connect card.

Step 4 To confirm a defective preferred cross-connect card, complete the "Retest the Preferred SSXC Card" procedure on page 1-15.

Retest the Preferred SSXC Card

Step 1 Do a manual data copy switch of the SSXC cards before retesting the loopback circuit:

a. In node view, select the **Maintenance > Preferred Copy** tabs.

b. In the **Set Preferred** drop-down menu, select the alternate copy. (For example, if Copy B is preferred and in use, select Copy A.)

c. Click **Apply**.

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

Note If you attempt a preferred copy switch and the switch is unsuccessful, a problem is present with the alternate SSXC.

e. Click **Refresh** until the tab shows that the alternate copy you selected is now the preferred copy. The Currently Used field will show the newly selected preferred copy.

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. Contact Cisco Technical Support (1 800 553-2447) and proceed to 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 4 Complete the "Replace an SSXC Card" procedure on page 2-132 for the defective card. Perform Step 5.

Step 5 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**.

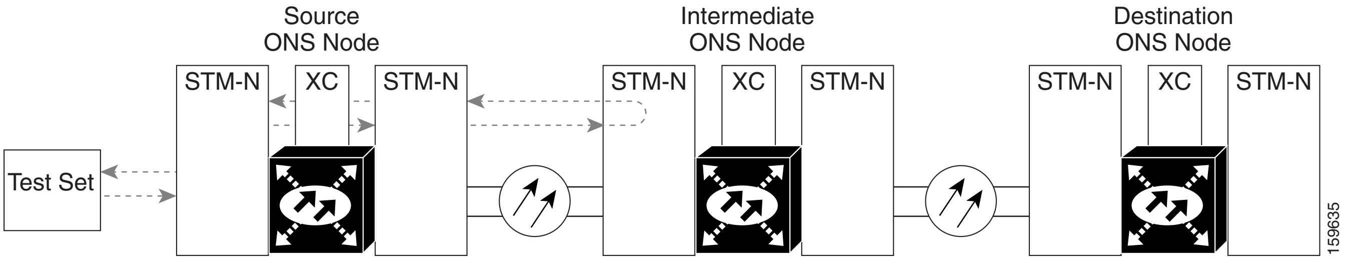
d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

Step 6 Complete the "1.2.4 Perform a Facility Loopback or Payload Loopback on an Intermediate-Node Optical Port" procedure on page 1-16.

1.2.4 Perform a Facility Loopback or Payload Loopback on an Intermediate-Node Optical Port

Performing an STM-16 or ASAP card optical facility loopback (or STM-64 payload loopback) on an intermediate port isolates whether this node is causing circuit failure. In the situation shown in Figure 1-9, the test is being performed on an intermediate STM-N port.

Figure 1-9 Facility Loopback Path to an Intermediate-Node STM-N Port



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

Note Facility and payload loopbacks require on-site personnel.

Complete the "Create a Facility Loopback or Payload Loopback on an Intermediate-Node Optical Port" procedure on page 1-17.

Create a Facility Loopback or Payload Loopback on an Intermediate-Node Optical Port

Step 1 Connect an optical test set to the port you are testing. If you are starting the current procedure without the optical test set hooked up to the source port port, use appropriate cabling to attach the Tx and Rx terminals of the optical test set to the port you are testing. Both Tx and Rx connect to the same port.

For specific procedures to use the test set equipment, consult the manufacturer.

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

Step 3 Use CTC to set up the facility 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_PATH_CIRCUIT, and circuit number, such as 1.

c. Click **Next**.

d. In the next Circuit Creation dialog box, give the circuit an easily identifiable name such as Opt1toOpt3.

e. Leave the Bidirectional check box checked.

f. Click **Next**.

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

h. Click **Next**.

i. In the Circuit Creation destination dialog box, use the same Node, card Slot, Port, and VC 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 (STMN)" condition on page 2-87 to appear during a loopback setup. The condition clears when you remove the loopback.

Step 5 Create the facility loopback on the intermediate 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 > Port** tabs (or **Maintenance > Optical > Loopback > Port** tabs).

d. Select **locked,maintenance** from the Admin State column. If multiple ports are available, select the row appropriate for the desired port.

e. For an STM-16 card or ASAP card optical port, select **Facility** from the Loopback Type column. For an STM-64 card, select **Payload**. If multiple ports are available, 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 Loopback or Payload Loopback Circuit" procedure on page 1-18.

Test and Clear the Facility Loopback or Payload 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 from the port:

a. Click the **Maintenance > Loopback > Port** tabs (or **Maintenance > Optical > Loopback > Port** tabs).

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

c. Choose the appropriate state (**Unlocked**; **Locked,disabled**; **Locked,maintenance**; **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 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 1-18.

Test the Optical Card

Step 1 Complete the "Replace an I/O Card" procedure on page 2-133 for the suspected bad STM-N or ASAP card and replace it with a known-good one.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the procedures in the "2.8.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-121. For more information, refer to the "Maintain the Node" chapter of the *Cisco ONS 15600 SDH Procedure Guide*.

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. Contact Cisco Technical Support (1 800 553-2447).

Step 4 Complete the "Replace an I/O Card" procedure on page 2-133 for the faulty card.

Step 5 Clear the facility loopback from the port:

a. Click the **Maintenance > Loopback > Port** tabs (or **Maintenance > Optical > Loopback > Port** tabs).

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

c. Choose the appropriate state (**Unlocked**; **Locked,disabled**; **Locked,maintenance**; **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 loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

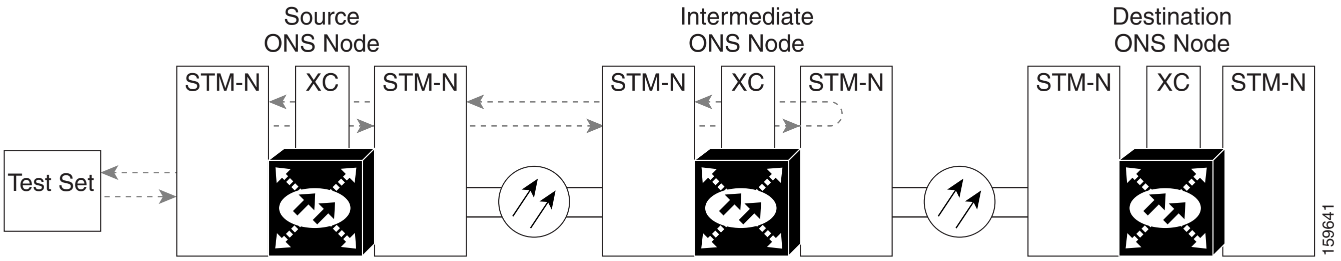
d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

Step 7 Complete the "1.2.6 Perform a Facility Loopback or Payload Loopback on a Destination-Node Optical Port" procedure on page 1-22.

1.2.5 Perform a Terminal Loopback on an Intermediate-Node Optical Port

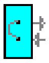
In the next troubleshooting test, you perform a terminal loopback on the intermediate-node port to isolate whether the destination port is causing circuit trouble. In the example situation in Figure 1-10, the terminal loopback is performed on an intermediate optical port in the circuit. You first create a bidirectional circuit that originates on the source-node optical port and loops back on the 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 1-10 Terminal Loopback on an Intermediate-Node STM-N Port



STM-N cards placed in facility loopback state display an icon, shown in Figure 1-11.

Figure 1-11 Facility Loopback Indicator



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

Note Terminal loopbacks require on-site personnel.

Complete the "Create a Terminal Loopback on Intermediate-Node Optical Ports" procedure on page 1-20.

Create a 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 "1.2.4 Perform a Facility Loopback or Payload Loopback on an Intermediate-Node Optical Port" section on page 1-16, leave the optical test set hooked up to the source-node port.
- **b.** If you are starting the current procedure without the optical test set hooked up to the source port, use appropriate cabling to attach the Tx and Rx terminals of the optical test set to the port you are testing. Both Tx and Rx connect to the same port.

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

Step 3 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_PATH_CIRCUIT, and circuit number, such as 1.
- **c.** Click **Next**.
- **d.** In the next Circuit Creation dialog box, give the circuit an easily identifiable name such as STMN1toSTMN4.
- **e.** Leave the **Bidirectional** check box checked.
- **f.** Click **Next**.
- **g.** In the Circuit Creation source dialog box, select the same Node, card Slot, Port, and VC where the test set is connected.
- **h.** Click **Next**.
- **i.** In the Circuit Creation destination dialog box, use the same Node, card Slot, Port, and VC 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 (STMN)" condition on page 2-88 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** > **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** 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 1-21.

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 from the port:

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

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**; **Locked,maintenance**; **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 1-22.

Test the Optical Card

Step 1 Complete the "Replace an I/O Card" procedure on page 2-133 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. Contact Cisco Technical Support at (1 800 553-2447).

Step 4 Complete the "Replace an I/O Card" procedure on page 2-133 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**; **Locked,maintenance**; **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**.

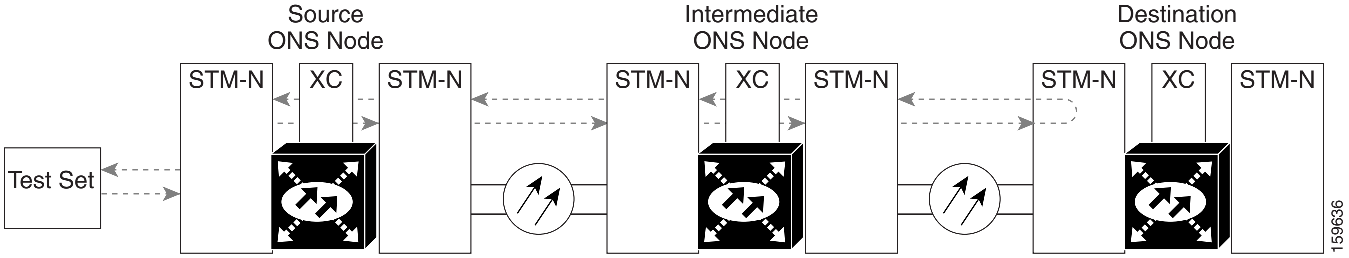
d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

Step 7 Complete the "1.2.6 Perform a Facility Loopback or Payload Loopback on a Destination-Node Optical Port" procedure on page 1-22.

1.2.6 Perform a Facility Loopback or Payload Loopback on a Destination-Node Optical Port

You perform a facility loopback test at the destination port to determine whether this local port is the source of circuit trouble. The example in Figure 1-12 shows a facility loopback being performed on a destination-node STM-N port.

Figure 1-12 Facility Loopback Path to a Destination-Node STM-N Port



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

Note Facility loopbacks require on-site personnel.

Complete the "Create the Facility Loopback or Payload Loopback on a Destination-Node Optical Port" procedure on page 1-23.

Create the Facility Loopback or Payload Loopback on a Destination-Node Optical Port

Step 1 Connect an optical test set to the STM-N or ASAP optical port you are testing. If you are starting the current procedure without the optical test set hooked up to the source port, use appropriate cabling to attach the Tx and Rx terminals of the optical test set to the port you are testing. Both Tx and Rx connect to the same port.

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

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

Step 3 Use CTC to set up the facility 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_PATH_CIRCUIT, and circuit number, such as 1.

c. Click **Next**.

d. In the next Circuit Creation dialog box, give the circuit an easily identifiable name such as Opt1toOpt5.

e. Leave the Bidirectional check box checked.

f. Click **Next**.

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

h. Click **Next**.

i. In the Circuit Creation destination dialog box, use the same Node, card Slot, Port, and VC 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 (STMN)" condition on page 2-87 to appear during a loopback setup. The condition clears when you remove the loopback.

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

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

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

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

c. Click the **Maintenance > Loopback > Port** tabs (or **Maintenance > Optical > Loopback > Port** tabs).

d. Select **Locked,maintenance** from the Admin State column. If multiple ports are available, select the row appropriate for the desired port.

e. For an ASAP card or STM-16 card, select **Facility** from the Loopback Type column. For an STM-64 card, select **Payload**. If multiple ports are available, 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 Facility Loopback or Payload Loopback Circuit" procedure on page 1-24.

Test and Clear the Optical Facility Loopback or Payload 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 from the port:

a. Click the **Maintenance > Loopback > Port** tabs (or **Maintenance > Optical > Loopback > Port** tabs).

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

c. Choose the appropriate state (**Unlocked**; **Locked,disabled**; **Locked,maintenance**; **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 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 1-25.

Test the Optical Card

Step 1 Complete the "Replace an I/O Card" procedure on page 2-133 for the suspected bad STM-N or ASAP card and replace it with a known-good one.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the procedures in the "2.8.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-121. For more information, refer to the "Maintain the Node" chapter of the *Cisco ONS 15600 SDH Procedure Guide*.

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. Contact Cisco Technical Support (1 800 553-2447).

Step 4 Complete the "Replace an I/O Card" procedure on page 2-133 for the faulty card.

Step 5 Clear the loopback on the port:

a. Click the **Maintenance > Loopback > Port** tabs (or **Maintenance > Optical > Loopback > Port** tabs).

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

c. Choose the appropriate state (**Unlocked**; **Locked,disabled**; **Locked,maintenance**; **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 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 "1.2.7 Perform a Terminal Loopback on a Destination-Node Optical Port" procedure on page 1-25.

1.2.7 Perform a Terminal Loopback on a Destination-Node Optical Port

The terminal loopback at the destination-node ASAP card optical 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.

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

Note STM-16 and STM-64 cards are not capable of terminal loopbacks.

Note Terminal loopbacks require on-site personnel.

Complete the "Create the Terminal Loopback on a Destination-Node Optical Port" procedure on page 1-26.

Create the Terminal Loopback on a Destination-Node Optical Port

Step 1 Connect an optical test set to the ASAP card optical port you are testing: If you are starting the current procedure without the optical test set hooked up to the source port, use appropriate cabling to attach the Tx and Rx terminals of the optical test set to the port you are testing. Both Tx and Rx connect to the same port.

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

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

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_PATH_CIRCUIT, and circuit number, such as 1.

c. Click **Next**.

d. In the next Circuit Creation dialog box, give the circuit an easily identifiable name such as Opt1toOpt6.

e. Leave the Bidirectional check box checked.

f. Click **Next**.

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

h. Click **Next**.

i. In the Circuit Creation destination dialog box, use the same Node, card Slot, Port, and VC 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 (STMN)" condition on page 2-88 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 > Optical > Loopback > Port** tab.

d. Select **Locked,maintenance** from the Admin State column. If multiple ports are available, select the row appropriate for the desired port.

e. Select **Terminal** from the Loopback Type column. If multiple ports are available, 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 1-27.

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 from the port:

a. Double-click the destination-node ASAP card with the terminal loopback.

b. Click the **Maintenance > Optical > Loopback > Port** tab.

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

d. Select the appropriate state (**Unlocked**; **Locked,disabled**; **Locked,maintenance**; **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 ASAP Card" procedure on page 1-28.

Test the ASAP Card

Step 1 Determine whether you are experiencing trouble on a single SFP (PPM), on all PPMs within a 4PIO (PIM), or on all 4PIO used in that ASAP card. If there is only partial failure, you might be able to replace this part rather than the entire card.

Step 2 If the errors are being observed on one port but not all ports of the ASAP, you might only need to replace that SFP (PPM). Remove the errored SFP (PPM) and replace it with a known-good SFP (PPM) by completing the procedures for this in the "Install Cards and Fiber-Optic Cable" chapter of the *Cisco ONS 15600 SDH Procedure Guide*.

Step 3 If all SFPs (PPMs) on a particular 4PIO (PIM) are experiencing problems, the 4PIO (PIM) is indicated. Remove this 4PIO (PIM) and replace it with a known-good one using the procedures for this in the "Install Cards and Fiber-Optic Cable" chapter of the *Cisco ONS 15600 SDH Procedure Guide*.

Step 4 If the trouble still is not located, complete the "Replace an I/O Card" procedure on page 2-133 for the suspected bad ASAP card and replace it with a known-good one.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the procedures in the "2.8.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-121. For more information, refer to the "Maintain the Node" chapter of the *Cisco ONS 15600 SDH Procedure Guide*.

Step 5 Resend test traffic on the loopback circuit with a known-good card.

Step 6 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. Contact Cisco Technical Support (1 800 553-2447).

Step 7 Complete the "Replace an I/O Card" procedure on page 2-133 for the defective card.

Step 8 Clear the terminal loopback on the port:

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

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

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

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

e. Click **Apply**.

f. 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.

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

1.3 Troubleshooting an Ethernet Circuit Path With Loopbacks

Facility loopbacks and terminal loopbacks are often used together to test the circuit path through the network or to logically isolate a fault. Performing a loopback test at each point along the circuit path systematically isolates possible points of failure.

You can use these procedures only on the ASAP card Ethernet ports in the ONS 15600 SDH system. The example in this section tests an Ethernet circuit on a three-node MS-SP Ring. Using a series of facility loopbacks and terminal loopbacks, the example scenario traces the circuit path, tests the possible failure points, and eliminates them. The logical progression contains six network test procedures:

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

1. A facility loopback on the source-node Ethernet port
2. A terminal loopback on the source-node Ethernet port
3. A facility loopback on the intermediate-node Ethernet port
4. A terminal loopback on the intermediate-node Ethernet port
5. A facility loopback on the destination-node Ethernet port
6. A terminal loopback on the destination-node Ethernet port

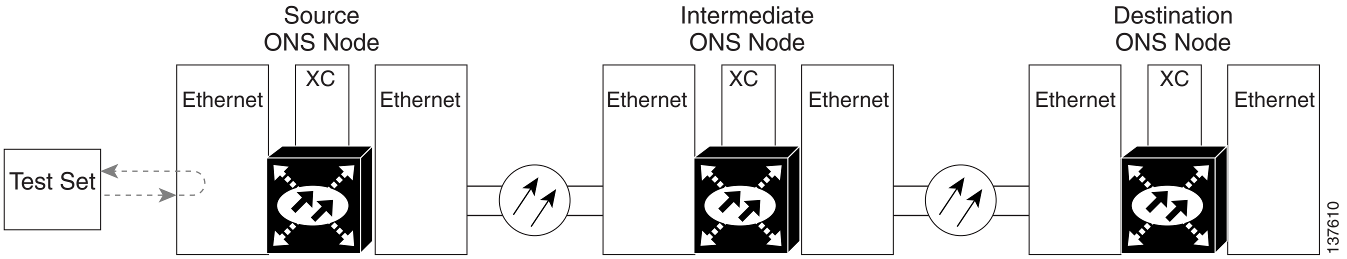
Note Facility and terminal loopback tests require on-site personnel.

1.3.1 Perform a Facility Loopback on a Source-Node Ethernet Port

The facility loopback test is performed on the node source port in the network circuit. In the testing situation used in this example, the source is an ASAP Ethernet port in the source node. Completing a successful facility loopback on this port isolates the port as a possible failure point. Figure 1-13 shows an example of a facility loopback on a circuit source Ethernet port.

Note Facility loopbacks require on-site personnel.

Figure 1-13 Facility Loopback on a Circuit Source Ethernet Port



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

Complete the "Create the Facility Loopback on the Source-Node Ethernet Port" procedure on page 1-30.

Create the Facility Loopback on the Source-Node Ethernet Port

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

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

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

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

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

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

Step 5 Choose **Locked,maintenance** from the Admin State column for the port being tested. If multiple ports are available, select the appropriate row for the desired port.

Step 6 Choose **Facility** from the Loopback Type column for the port being tested. If multiple ports are available, select the appropriate row for the desired port.

Step 7 Click **Apply**.

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

Note It is normal for the "LPBKFACILITY (GIGE)" condition on page 2-86 to appear during loopback setup. The condition clears when you remove the loopback.

Step 9 Complete the "Test and Clear the Facility Loopback Circuit" procedure on page 1-30.

Test and Clear the 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. Clear the facility loopback:

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

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

c. Choose the appropriate state (**Unlocked**; **Locked,disabled**; **Locked,maintenance**) 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 ASAP Card" procedure on page 1-31.

Test the ASAP Card

Step 1 Determine whether you are experiencing trouble on a single SFP (PPM), on all PPMs within a 4PIO (PIM), or on all 4PIO used in that ASAP card. If there is only partial failure, you might be able to replace this part rather than the entire card.

Step 2 If the errors are being observed on one port but not all ports of the ASAP, you might only need to replace that SFP (PPM). Remove the errored SFP (PPM) and replace it with a known-good SFP (PPM) by completing the procedures for this in the "Install Cards and Fiber-Optic Cable" chapter of the *Cisco ONS 15600 SDH Procedure Guide*.

Step 3 If all SFPs (PPMs) on a particular 4PIO (PIM) are experiencing problems, the 4PIO (PIM) is indicated. Remove this 4PIO (PIM) and replace it with a known-good one using the procedures for this in the "Install Cards and Fiber-Optic Cable" chapter of the *Cisco ONS 15600 SDH Procedure Guide*.

Step 4 If the trouble still is not located, complete the "Replace an I/O Card" procedure on page 2-133 for the suspected bad ASAP card and replace it with a known-good one.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the procedures in the "2.8.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-121. For more information, refer to the "Maintain the Node" chapter of the *Cisco ONS 15600 SDH Procedure Guide*.

Step 5 Resend test traffic on the loopback circuit with a known-good card installed.

Step 6 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. Contact Cisco Technical Support (1 800 553-2447).

Step 7 Complete the "Replace an I/O Card" procedure on page 2-133 for the faulty card.

Step 8 Clear the facility loopback:

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

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

c. Choose the appropriate state (**Unlocked**; **Locked,disabled**; **Locked,maintenance**) 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 "1.3.2 Perform a Terminal Loopback on a Source-Node Ethernet Port" procedure on page 1-32.

1.3.2 Perform a Terminal Loopback on a Source-Node Ethernet Port

The terminal loopback test is performed on the node source Ethernet port. For the circuit in this example, it is the source Ethernet port in the source node. You first create a bidirectional circuit that starts on the node destination Ethernet port and loops back on the node source Ethernet 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.

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

Note Terminal loopbacks require on-site personnel.

Complete the "Create the Terminal Loopback on a Source-Node Ethernet Port" procedure on page 1-32.

Create the Terminal Loopback on a Source-Node Ethernet Port

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

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

a. If you just completed the "1.3.1 Perform a Facility Loopback on a Source-Node Ethernet Port" procedure on page 1-29, 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 Ethernet port, use appropriate cabling to attach the Tx and Rx terminals of the optical test set to the port you are testing. Both Tx and Rx connect to the same port.

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

Step 3 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_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 Eth1toEth2.

e. Leave the Bidirectional check box checked.

f. Click **Next**.

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

h. Click **Next**.

i. In the Circuit Creation destination dialog box, use the same Node, card Slot, Port, and VC 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 (GIGE)" condition on page 2-88 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. In node view, double-click the card that requires the loopback, such as the ASAP card in the source node.

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

c. Select **Locked,maintenance** from the Admin State column. If multiple ports are available, select the row appropriate for the desired port.

d. Select **Terminal** from the Loopback Type column. If multiple ports are available, 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 1-33.

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 ASAP card in the source node with the terminal loopback.

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

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

d. Select the appropriate state (**Unlocked**; **Locked,disabled**; **Locked,maintenance**) 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 ASAP Card" procedure on page 1-34.

Test the ASAP Card

Step 1 Determine whether you are experiencing trouble on a single SFP (PPM), on all PPMs within a 4PIO (PIM), or on all 4PIO used in that ASAP card. If there is only partial failure, you might be able to replace this part rather than the entire card.

Step 2 If the errors are being observed on one port but not all ports of the ASAP, you might only need to replace that SFP (PPM). Remove the errored SFP (PPM) and replace it with a known-good SFP (PPM) by completing the procedures for this in the "Install Cards and Fiber-Optic Cable" chapter of the *Cisco ONS 15600 SDH Procedure Guide*.

Step 3 If all SFPs (PPMs) on a particular 4PIO (PIM) are experiencing problems, the 4PIO (PIM) is indicated. Remove this 4PIO (PIM) and replace it with a known-good one using the procedures for this in the "Install Cards and Fiber-Optic Cable" chapter of the *Cisco ONS 15600 SDH Procedure Guide*.

Step 4 If the trouble still is not located, complete the "Replace an I/O Card" procedure on page 2-133 for the suspected bad ASAP card and replace it with a known-good one.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the procedures in the "2.8.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-121. For more information, refer to the "Maintain the Node" chapter of the *Cisco ONS 15600 SDH Procedure Guide*.

Step 5 Resend test traffic on the loopback circuit with a known-good card.

Step 6 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. Contact Cisco Technical Support (1 800 553-2447).

Step 7 Complete the "Replace an I/O Card" procedure on page 2-133 for the defective card.

Step 8 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 > Ethernet > Loopback > Port** tabs.

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

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

e. Click **Apply**.

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

Step 9 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**.

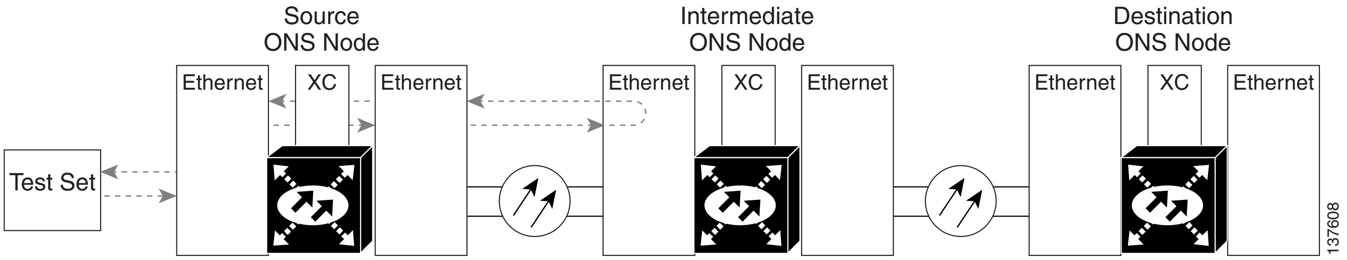
d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

Step 10 Complete the "1.3.3 Create a Facility Loopback on an Intermediate-Node Ethernet Port" procedure on page 1-35.

1.3.3 Create a Facility Loopback on an Intermediate-Node Ethernet Port

Performing the facility loopback test on an intermediate port isolates whether this node is causing circuit failure. It is shown in Figure 1-14.

Figure 1-14 Facility Loopback on an Intermediate-Node Ethernet Port



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

Note Facility loopbacks require on-site personnel.

Complete the "Create a Facility Loopback on an Intermediate-Node Ethernet Port" procedure on page 1-35.

Create a Facility Loopback on an Intermediate-Node Ethernet Port

Step 1 Connect an optical test set to the ASAP card Ethernet port you are testing: If you are starting the current procedure without the optical test set hooked up to the source ASAP card Ethernet port, use appropriate cabling to attach the Tx and Rx terminals of the optical test set to the port you are testing. Both Tx and Rx connect to the same port.

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

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

Step 3 Use CTC to set up the facility 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_PATH_CIRCUIT, and circuit number, such as 1.

c. Click **Next**.

d. In the next Circuit Creation dialog box, give the circuit an easily identifiable name such as Eth1toEth3.

e. Leave the Bidirectional check box checked.

f. Click **Next**.

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

h. Click **Next**.

i. In the Circuit Creation destination dialog box, use the same Node, card Slot, Port, and VC 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 (GIGE)" condition on page 2-86 to appear during a loopback setup. The condition clears when you remove the loopback.

Step 5 Create the facility 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 or **Maintenance > Ethernet > Loopback > Port** tabs.

d. Select **Locked,maintenance** from the Admin State column. If multiple ports are available, select the row appropriate for the desired port.

e. Select **Facility** from the Loopback Type column. If multiple ports are available, 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 Loopback Circuit" procedure on page 1-36.

Test and Clear the Ethernet 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. Clear the facility loopback from the port:

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

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

c. Choose the appropriate state (**Unlocked**; **Locked,disabled**; **Locked,maintenance**) 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 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 ASAP Card" procedure on page 1-37.

Test the ASAP Card

Step 1 Determine whether you are experiencing trouble on a single SFP (PPM), on all PPMs within a 4PIO (PIM), or on all 4PIO used in that ASAP card. If there is only partial failure, you might be able to replace this part rather than the entire card.

Step 2 If the errors are being observed on one port but not all ports of the ASAP, you might only need to replace that SFP (PPM). Remove the errored SFP (PPM) and replace it with a known-good SFP (PPM) by completing the procedures for this in the "Install Cards and Fiber-Optic Cable" chapter of the *Cisco ONS 15600 SDH Procedure Guide*.

Step 3 If all SFPs (PPMs) on a particular 4PIO (PIM) are experiencing problems, the 4PIO (PIM) is indicated. Remove this 4PIO (PIM) and replace it with a known-good one using the procedures for this in the "Install Cards and Fiber-Optic Cable" chapter of the *Cisco ONS 15600 SDH Procedure Guide*.

Step 4 If the trouble still is not located, complete the "Replace an I/O Card" procedure on page 2-133 for the suspected bad ASAP card and replace it with a known-good one.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the procedures in the "2.8.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-121. For more information, refer to the "Maintain the Node" chapter of the *Cisco ONS 15600 SDH Procedure Guide*.

Step 5 Resend test traffic on the loopback circuit with a known-good ASAP card installed.

Step 6 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. Contact Cisco Technical Support (1 800 553-2447).

Step 7 Complete the "Replace an I/O Card" procedure on page 2-133 for the faulty card.

Step 8 Clear the facility loopback from the port:

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

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

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

d. Click **Apply**.

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

Step 9 Clear the loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

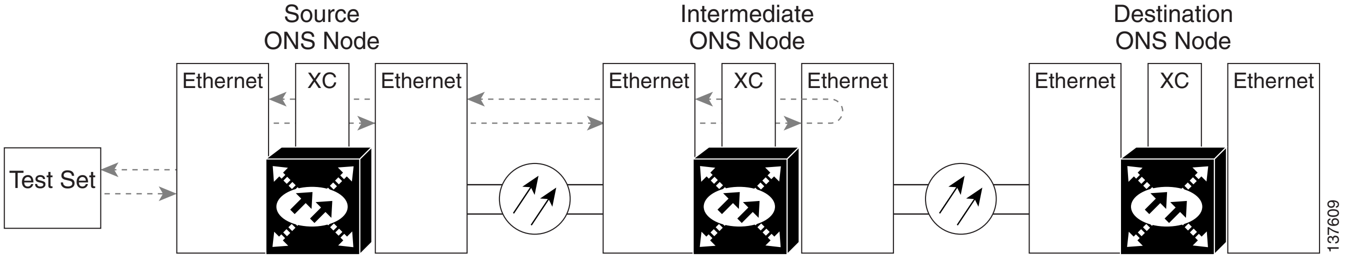
d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

Step 10 Complete the "1.3.4 Create a Terminal Loopback on an Intermediate-Node Ethernet Port" procedure on page 1-38.

1.3.4 Create a Terminal Loopback on an Intermediate-Node Ethernet Port

In the next troubleshooting test, you perform a terminal loopback on the intermediate-node ASAP Ethernet port to isolate whether the destination port is causing circuit trouble. In the example situation in Figure 1-15, 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 1-15 Terminal Loopback on an Intermediate-Node Ethernet Port



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

Note Terminal loopbacks require on-site personnel.

Complete the "Create a Terminal Loopback on an Intermediate-Node Ethernet Port" procedure on page 1-38.

Create a Terminal Loopback on an Intermediate-Node Ethernet Port

Step 1 Connect an optical test set to the intermediate node ASAP card Ethernet port you are testing:

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

a. If you just completed the "1.3.3 Create a Facility Loopback on an Intermediate-Node Ethernet Port" procedure on page 1-35 for an ASAP card Ethernet port, leave the optical test set hooked up to the intermediate-node port.

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

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

Step 3 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_PATH_CIRCUIT, and circuit number, such as 1.

c. Click **Next**.

d. In the next Circuit Creation dialog box, give the circuit an easily identifiable name such as Eth1toEth4.

e. Leave the Bidirectional check box checked.

f. Click **Next**.

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

h. Click **Next**.

i. In the Circuit Creation destination dialog box, use the same Node, card Slot, Port, and VC 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 (GIGE)" condition on page 2-88 to appear during a loopback setup. The condition clears when you remove the loopback.

Step 5 Create the terminal loopback on the intermediate 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 > Ethernet > Loopback > Port** tabs.

d. Select **Locked,maintenance** from the Admin State column. If multiple ports are available, select the row appropriate for the desired port.

e. Select **Terminal** from the Loopback Type column. If multiple ports are available, 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 1-40.

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 > Ethernet > Loopback > Port** tabs.

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

d. Select the appropriate state (**Unlocked**; **Locked,disabled**; **Locked,maintenance**) 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 ASAP Card" procedure on page 1-40.

Test the ASAP Card

Step 1 Determine whether you are experiencing trouble on a single SFP (PPM), on all PPMs within a 4PIO (PIM), or on all 4PIO used in that ASAP card. If there is only partial failure, you might be able to replace this part rather than the entire card.

Step 2 If the errors are being observed on one port but not all ports of the ASAP, you might only need to replace that SFP (PPM). Remove the errored SFP (PPM) and replace it with a known-good SFP (PPM) by completing the procedures for this in the "Install Cards and Fiber-Optic Cable" chapter of the *Cisco ONS 15600 SDH Procedure Guide*.

Step 3 If all SFPs (PPMs) on a particular 4PIO (PIM) are experiencing problems, the 4PIO (PIM) is indicated. Remove this 4PIO (PIM) and replace it with a known-good one using the procedures for this in the "Install Cards and Fiber-Optic Cable" chapter of the *Cisco ONS 15600 SDH Procedure Guide*.

Step 4 If the trouble still is not located, complete the "Replace an I/O Card" procedure on page 2-133 for the suspected bad ASAP card and replace it with a known-good one.

⚠ **Caution** Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the procedures in the "2.8.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-121. For more information, refer to the "Maintain the Node" chapter of the *Cisco ONS 15600 SDH Procedure Guide*.

Step 5 Resend test traffic on the loopback circuit with a known-good card.

Step 6 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. Contact Cisco Technical Support (1 800 553-2447).

Step 7 Complete the "Replace an I/O Card" procedure on page 2-133 for the defective card.

Step 8 Clear the terminal loopback on the port:

- **a.** Double-click the intermediate-node ASAP card with the terminal loopback.
- **b.** Click the **Maintenance > Ethernet > Loopback > Port** tabs.
- **c.** Select **None** from the Loopback Type column for the port being tested.
- **d.** Select the appropriate state (**Unlocked**; **Locked,disabled**; **Locked,maintenance**) in the Admin State column for the port being tested.
- **e.** Click **Apply**.
- **f.** Click **Yes** in the confirmation dialog box.

Step 9 Clear the terminal loopback circuit:

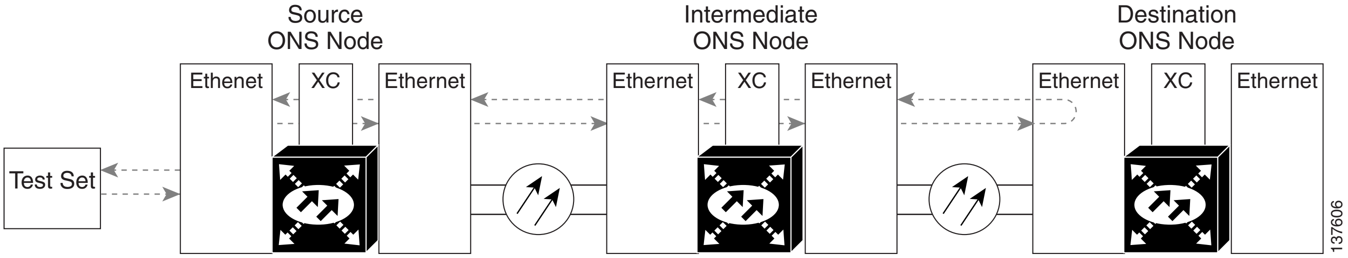
- **a.** Click the **Circuits** tab.
- **b.** Choose the loopback circuit being tested.
- **c.** Click **Delete**.
- **d.** Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

Step 10 Complete the "1.3.5 Perform a Facility Loopback on a Destination-Node Ethernet Port" procedure on page 1-41.

1.3.5 Perform a Facility Loopback on a Destination-Node Ethernet Port

You perform a facility loopback test for ASAP card Ethernet port at the destination port to determine whether this local port is the source of circuit trouble. The example in Figure 1-16 shows a facility loopback being performed on an Ethernet port.

Figure 1-16 Facility Loopback on a Destination-Node Ethernet Port



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

Note Facility loopbacks require on-site personnel.

Complete the "Create the Facility Loopback on a Destination-Node Ethernet Port" procedure on page 1-42.

Create the Facility Loopback on a Destination-Node Ethernet Port

Step 1 Connect an optical test set to the destination ASAP card optical port you are testing. If you are starting the current procedure without the optical test set hooked up to the source optical port, use appropriate cabling to attach the Tx and Rx terminals of the optical test set to the port you are testing. Both Tx and Rx connect to the same port.

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

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

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_PATH_CIRCUIT, and circuit number, such as 1.
- **c.** Click **Next**.
- **d.** In the next Circuit Creation dialog box, give the circuit an easily identifiable name such as Eth1toEth5.
- **e.** Leave the Bidirectional check box checked.
- **f.** Click **Next**.
- **g.** In the Circuit Creation source dialog box, select the same Node, card Slot, Port, and VC where the test set is connected.
- **h.** Click **Next**.
- **i.** In the Circuit Creation destination dialog box, use the same Node, card Slot, Port, and VC 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 (GIGE)" condition on page 2-86 to appear during a loopback setup. The condition clears when you remove the loopback.

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

- **a.** Go to the node view of the destination node:
  - Choose **View > Go To Other Node** from the menu bar.
  - Choose the node from the drop-down list in the Select Node dialog box and click **OK**.
- **b.** In node view, double-click the card that requires the loopback.
- **c.** Click the **Maintenance > Ethernet > Loopback > Port** tabs.
- **d.** Select **Locked,maintenance** from the Admin State column. If multiple ports are available, select the row appropriate for the desired port.

e. Select **Facility** from the Loopback Type column. If multiple ports are available, 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 Loopback Circuit" procedure on page 1-43.

Test and Clear the Ethernet 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. Clear the facility loopback from the port:

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

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

c. Choose the appropriate state (**Unlocked**; **Locked,disabled**; **Locked,maintenance**) 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 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 ASAP Card" procedure on page 1-43.

Test the ASAP Card

Step 1 Determine whether you are experiencing trouble on a single SFP (PPM), on all PPMs within a 4PIO (PIM), or on all 4PIO used in that ASAP card. If there is only partial failure, you might be able to replace this part rather than the entire card.

Step 2 If the errors are being observed on one port but not all ports of the ASAP, you might only need to replace that SFP (PPM). Remove the errored SFP (PPM) and replace it with a known-good SFP (PPM) by completing the procedures for this in the "Install Cards and Fiber-Optic Cable" chapter of the *Cisco ONS 15600 SDH Procedure Guide*.

Step 3 If all SFPs (PPMs) on a particular 4PIO (PIM) are experiencing problems, the 4PIO (PIM) is indicated. Remove this 4PIO (PIM) and replace it with a known-good one using the procedures for this in the "Install Cards and Fiber-Optic Cable" chapter of the *Cisco ONS 15600 SDH Procedure Guide*.

Step 4 If the trouble still is not located, complete the "Replace an I/O Card" procedure on page 2-133 for the suspected bad ASAP card and replace it with a known-good one.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the procedures in the "2.8.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-121. For more information, refer to the "Maintain the Node" chapter of the *Cisco ONS 15600 SDH Procedure Guide*.

Step 5 Resend test traffic on the loopback circuit with a known-good card installed.

Step 6 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. Contact Cisco Technical Support (1 800 553-2447).

Step 7 Complete the "Replace an I/O Card" procedure on page 2-133 for the faulty card.

Step 8 Clear the facility loopback on the port:

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

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

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

d. Click **Apply**.

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

Step 9 Clear the loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

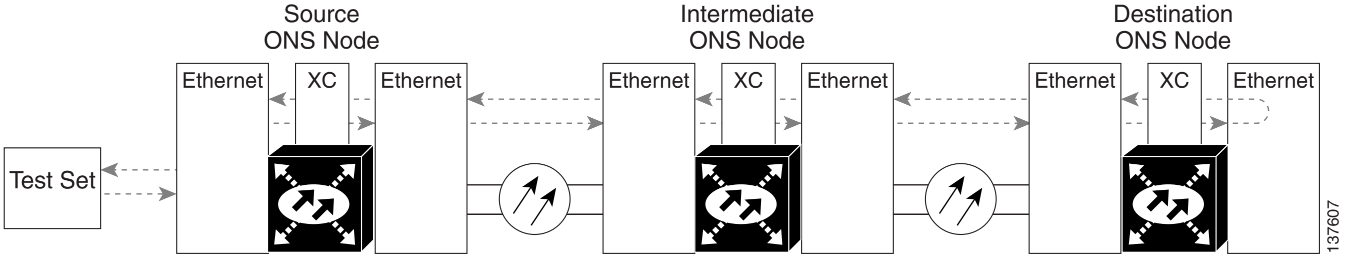
d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

Step 10 Complete the "1.3.6 Perform a Terminal Loopback on a Destination-Node Ethernet Port" procedure on page 1-44.

1.3.6 Perform a Terminal Loopback on a Destination-Node Ethernet Port

The terminal loopback at the destination-node ASAP card Ethernet port is the final local hardware error elimination in the circuit troubleshooting process, and is performed on the destination-node ASAP card Ethernet port. If this test is completed successfully, you have verified that the circuit is good up to the destination port. The example in Figure 1-17 shows a terminal loopback on a destination-node Ethernet port.

Figure 1-17 Terminal Loopback on a Destination-Node Ethernet Port



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

Note Terminal loopbacks require on-site personnel.

Complete the "Create the Terminal Loopback on a Destination-Node Ethernet Port" procedure on page 1-45.

Create the Terminal Loopback on a Destination-Node Ethernet Port

Step 1 Connect an optical test set to the destination node ASAP card Ethernet port you are testing:

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

a. If you just completed the "1.3.5 Perform a Facility Loopback on a Destination-Node Ethernet Port" procedure on page 1-41 for an ASAP card Ethernet port, leave the optical test set hooked up to the source port.

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

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

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_PATH_CIRCUIT, and circuit number, such as 1.

c. Click **Next**.

d. In the next Circuit Creation dialog box, give the circuit an easily identifiable name such as Eth1toEth6.

e. Leave the Bidirectional check box checked.

f. Click **Next**.

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

h. Click **Next**.

i. In the Circuit Creation destination dialog box, use the same Node, card Slot, Port, and VC 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 (GIGE)" condition on page 2-88 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 > Ethernet > Loopback > Port** tabs.

d. Select **Locked,maintenance** from the Admin State column. If multiple ports are available, select the row appropriate for the desired port.

e. Select **Terminal** from the Loopback Type column. If multiple ports are available, 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 1-46.

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 destination-node ASAP card.

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

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

d. Select the appropriate state (**Unlocked**; **Locked,disabled**; **Locked,maintenance**) 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 ASAP Card" procedure on page 1-47.

Test the ASAP Card

Step 1 Determine whether you are experiencing trouble on a single SFP (PPM), on all PPMs within a 4PIO (PIM), or on all 4PIO used in that ASAP card. If there is only partial failure, you might be able to replace this part rather than the entire card.

Step 2 If the errors are being observed on one port but not all ports of the ASAP, you might only need to replace that SFP (PPM). Remove the errored SFP (PPM) and replace it with a known-good SFP (PPM) by completing the procedures for this in the "Install Cards and Fiber-Optic Cable" chapter of the *Cisco ONS 15600 SDH Procedure Guide*.

Step 3 If all SFPs (PPMs) on a particular 4PIO (PIM) are experiencing problems, the 4PIO (PIM) is indicated. Remove this 4PIO (PIM) and replace it with a known-good one using the procedures for this in the "Install Cards and Fiber-Optic Cable" chapter of the *Cisco ONS 15600 SDH Procedure Guide*.

Step 4 If the trouble still is not located, complete the "Replace an I/O Card" procedure on page 2-133 for the suspected bad ASAP card and replace it with a known-good one.

⚠ **Caution** Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the procedures in the "2.8.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-121. For more information, refer to the "Maintain the Node" chapter of the *Cisco ONS 15600 SDH Procedure Guide*.

Step 5 Resend test traffic on the loopback circuit with a known-good card.

Step 6 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. Contact Cisco Technical Support (1 800 553-2447).

Step 7 Complete the "Replace an I/O Card" procedure on page 2-133 for the defective card.

Step 8 Clear the terminal loopback on the port:

a. Double-click the destination-node ASAP card.

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

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

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

e. Click **Apply**.

f. 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.

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

1.4 Using CTC Diagnostics

CTC provides diagnostics for the following functions:

- Verification of proper card application-specific integrated circuit (ASIC) function
- Verification of standby card operation
- Verification of proper card LED operation
- Notification of problems detected through alarms
- Provision of a downloaded, machine-readable diagnostic log file to be used by Cisco Technical Support

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

1.4.1 Card LED Lamp Tests

A card LED lamp test determines whether card-level indication LEDs are operational. This diagnostic test is run as part of the initial ONS 15600 SDH turn-up, during maintenance routines, or any time you question whether an LED is in working order. Maintenance or higher-level users can complete the following tasks to verify LED operation.

Verify Card LED Operation

Note The LED test must be performed on the physical card. This test is not available in the CTC interface. For typical STM-N, SSXC, and TSC card LED behavior, see the "2.7 LED Behavior" section on page 2-118.

Step 1 Determine the active TSC card using the green ACT /STBY LED on the face of the card.

Step 2 Press the LAMP button on the face of the active TSC card.

Step 3 Ensure that all the LEDs on the cards in the shelf illuminate for several seconds.

Step 4 If an LED does not illuminate, the LED might be faulty.

Return the defective card to Cisco through the returned materials authorization (RMA) process. See the "Obtaining Documentation and Submitting a Service Request" section on page xxxi to contact Cisco Technical Assistance Center (TAC).

1.4.2 Retrieve Tech Support Logs Button

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

Note In addition to the machine-readable diagnostics file, the ONS 15600 SDH stores an audit trail of all system events such as user log-ins, remote log-ins, configuration, and changes. This audit trail is considered a record-keeping feature rather than a troubleshooting feature. Information about the feature is located in the "Maintain the Node" chapter of the *Cisco ONS 15600 SDH Procedure Guide*.

Off-Load the Diagnostics File

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

The diagnostic files retrieved by CTC depends on the user privilege levels. Table 1-1 lists the user privilege levels and the diagnostic retrieval operations they can perform.

Table 1-1 Diagnostic Files Retrieved Based on User Privilege

User Privilege Level	Diagnostic File Retrieval Operation
Retrieve	• Export the unfiltered alarm table contents • Export the unfiltered conditions table contents • Export the unfiltered history table contents • Export the inventory table contents • CTC Dump Diagnostics log
Maintenance	• All Retrieve level access operations • Save the node database
Provisioning	• All Maintenance level access operations • Retrieve and save the node-level diagnostics report[1] • Export the audit table contents[2]
Superuser	• All Provisioning level access operations • Retrieve and save the node-level diagnostics report • Export the audit table contents

1. If secure mode is not set on the node.
2. If the NODE.security.grantPermission.RetrieveAuditLog NE Default is set to "Provisioning."

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

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

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

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

Step 4 Click **Save**.

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

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

Table 1-2 lists the diagnostic files retrieved by CTC.

Table 1-2 List of Diagnostic Files

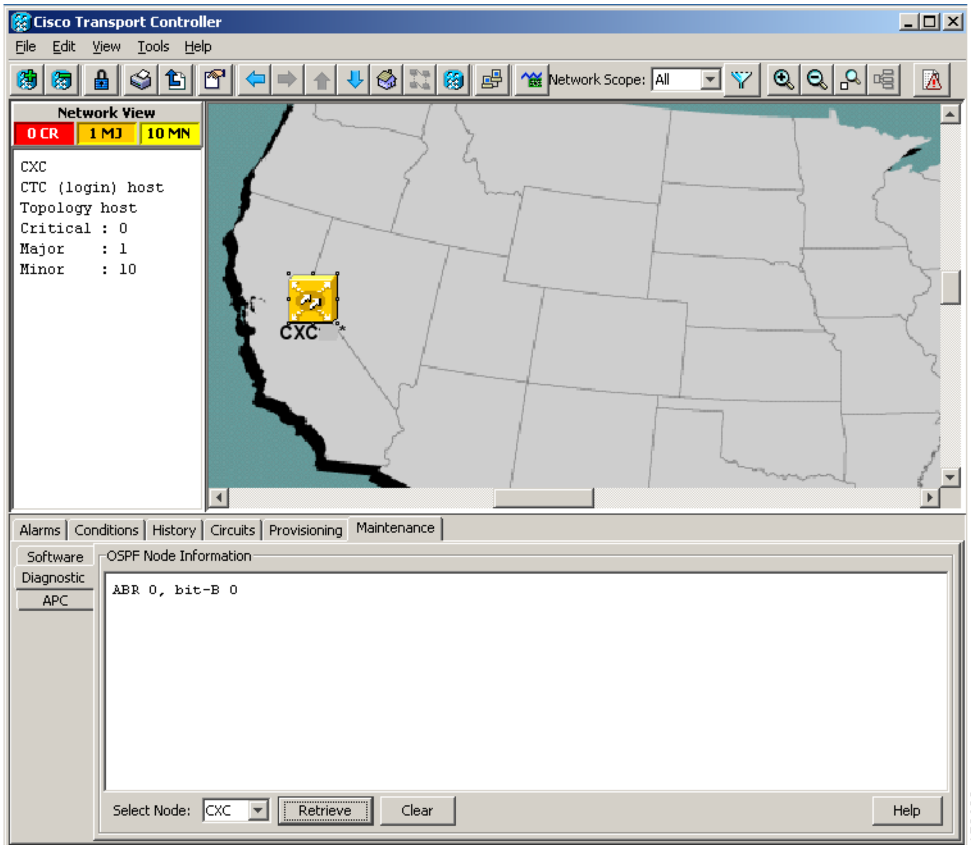
Diagnostic File	Diagnostic File Content
AlarmTableLog.html	Alarm Table export
HistoryTableLog.html	Alarm Table export
ConditionsTableLog.html	Conditions Table export
InventoryTableLog.html	Inventory Table export
AuditTableLog.html	Audit Table export
CTCDumpDiagLog.txt	Audit Table export
NodeDiagnostics.bin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

Step 5 Click **OK**.

1.4.3 Data Communications Network (DCN) Tool

In Software R8.0, CTC contains a DCN tool that assists with network troubleshooting for Open Shortest Path First (OSPF) networks. This tool, located in network view, is shown in Figure 1-18. It executes an internal dump command to retrieve information about all nodes accessible from the entry point.

Figure 1-18 DCN Tools OSPF Dump



Network View: 0 CR | 1 MJ | 10 MN

```
CXC
CTC (login) host
Topology host
Critical : 0
Major    : 1
Minor    : 10
```

Network Scope: All

OSPF Node Information

```
ABR 0, bit-B 0
```

Select Node: CXC

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

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

1.5 Restoring the Database to a Previous or Original Configuration

This section contains troubleshooting for node operation errors that might require restoring software data or restoring the node to the default setup.

1.5.1 Node is Functioning Improperly or Has Incorrect Data

Symptom One or more nodes are not functioning properly or have incorrect data.

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

Table 1-3 Node is Functioning Improperly or Has Incorrect Data

Possible Problem	Solution
The node has an incorrect or corrupted database.	Complete the procedures in the "Maintain the Node" chapter of the *Cisco ONS 15600 SDH Procedure Guide*.

1.6 PC Connectivity Troubleshooting

This section contains information about system minimum requirements, supported platforms, browsers, and Java Runtime Environments (JREs) for Software Releases 9.1 and 9.2, and troubleshooting procedures for PC and network connectivity to the ONS 15600 SDH.

1.6.1 PC System Minimum Requirements

Table 1-4 provides the minimum requirements for PCs and UNIX workstations.

Table 1-4 Minimum Computer Requirements for CTC

Area	Requirements	Notes
Processor (PC only)	Pentium 4 processor or equivalent	A faster CPU is recommended if your workstation runs multiple applications or if CTC manages a network with a large number of nodes and circuits.
RAM	512 MB RAM or more	A minimum of 1 GB is recommended if your workstation runs multiple applications or if CTC manages a network with a large number of nodes and circuits.
Hard drive	20 GB hard drive with 100MB of free space required	CTC application files are downloaded from the TCC2/TCC2P to your computer. These files occupy around 100MB (250MB to be safer) or more space depending on the number of versions in the network.

Table 1-4 Minimum Computer Requirements for CTC (continued)

Area	Requirements	Notes
Operating System	• Release 9.1 – PC: Windows 2000 with SP4, Windows XP with SP2, Windows Vista SP1, Windows Server 2003 SP2 – Workstation: Solaris versions 9 or 10 • Release 9.2.1 – PC: Windows 2000, Windows XP, Windows Vista, Windows 7, Windows Server 2003, Windows Server 2008 – Workstation: Solaris Version 9 or 10 on an UltraSPARC-III or faster processor, with a minimum of 1 GB RAM and 250 MB of available hard drive space – Apple Mac OS X. CTC needs to be installed using the CacheInstaller available on the CCO or the ONS CD	Check with the vendor for the latest patch/Service Pack level
Java Runtime Environment	JRE 5.0 (Release 9.1) JRE 1.6 (Release 9.2.1)	The appropriate JRE version is installed by the CTC Installation Wizard included in the Cisco ONS 15454 software CD. JRE installation provides enhancements to CTC performance, especially for large networks with numerous circuits. Cisco recommends that you use JRE 5.0 for networks with Software R8.5 nodes. If CTC must be launched directly from nodes running software R7.0 or R7.2, Cisco recommends JRE 1.4.2 or JRE 5.0. If CTC must be launched directly from nodes running software R5.0 or R6.0, Cisco recommends JRE 1.4.2. If CTC must be launched directly from nodes running software earlier than R5.0, Cisco recommends JRE 1.3.1_02.

Table 1-4 Minimum Computer Requirements for CTC (continued)

Area	Requirements	Notes
Web browser	• Release 9.1 – PC: Internet Explorer 6.x or Netscape 7.x – UNIX Workstation: Mozilla 1.7, Netscape 4.76, Netscape 7.x • Release 9.2.1 – PC: Internet Explorer 6.x, 7.x, 8.x – UNIX Workstation: Mozilla 1.7 – Mac OS X PC: Safari	For the PC, use JRE 5.0 or JRE 1.6 with any supported web browser. For UNIX, use JRE 5.0 with Netscape 7.x or JRE 1.3.1_02 with Netscape 4.76. Netscape is available at this site: http://channels.netscape.com/ns/browsers/default.jsp Internet Explorer is available at this site: http://www.microsoft.com Mozilla is available at this site: http://www.mozilla.com Safari is available at this site: http://www.apple.com
Cable	Use a crossover or straight-through LAN (CAT-5) cable to connect: • The ONS 15600 to a hub using the backplane RJ-45 ports, or to connect through a LAN. • The ONS 15600 to a PC using the backplane RJ-45 ports. • The active TSC RJ-45 port to a laptop or hub.	A direct PC-to-ONS 15600 connection means your computer is physically connected to the ONS 15600. This is most commonly done by connecting a LAN (CAT-5) straight-through cable from your PC to the RJ-45 port on the TSC. However, direct connections include connections to switches or hubs where the ONS 15600 is physically connected. **Note** Use only the active TSC connector for connectivity. If you connect to the standby or switch TSCs, you will lose connectivity. Cisco recommends that you use the RJ-45 connector on the Customer Access Panel (CAP/CAP2) so that connection to the ONS 15600 will not be lost during a TSC switch.

1.6.2 Retrieve the Node Information

If you do not know the IP address of your ONS 15600 SDH network element (NE), you can obtain and view the NE information using a TL1 session.

Step 1 Connect a 3-pair swapping null modem adapter to the EIA/TIA-232 (RS-232) port on the customer access panel (CAP).

Step 2 Connect a serial cable to the null modem adapter and to the serial port on your PC.

Step 3 Configure the terminal emulation software (HyperTerminal):

a. Terminal emulation = vt100

b. Bits per second = 9600

c. Parity = None

d. Stop BITS = 1

e. Flow control = None

Step 4 Press **Enter**. A > prompt appears.

Step 5 At the prompt, type the Activate User command to open a TL1 session:

```
ACT-USER::CISCO15:<CTAG>::<PID>;
```

Note When the semicolon is typed, the TL1 command is executed immediately.

Step 6 At the prompt, type the Retrieve Network Element General command to retrieve the NE information:

```
RTRV-NE-GEN:::<CTAG>;
```

Step 7 The response message will provide the following NE information.

- <IPADDR> indicates the node IP address; <IPADDR> is a string.
- <IPMASK> indicates the node IP mask; <IPMASK> is a string.
- <DEFRTR> indicates the node default router; <DEFRTR> is a string.
- <NAME> is the node name. The maximum name size is 20 characters; <name> is a string.
- <SWVER> is the software version; <SWVER> is a string.
- <LOAD> is the load version; <LOAD> is a string.
- <SELCLK> is the system-wide selected clock/sync copy; <SELCLK> is of type DATA_CLK_COPY.
- <PREFCLK> is the preferred clock/sync copy; <PREFCLK> is of type DATA_CLK_COPY.
- <SELDATA> is the system-wide selected data copy; <SELDATA> is of type DATA_CLK_COPY.
- <PREFDATA> is the preferred data copy; <SELDATA> is of type DATA_CLK_COPY.

Step 8 At the prompt, type the Cancel User command to close the TL1 session:

```
CANC-USER::CISCO15:<CTAG>;
```

Step 9 Remove the serial cable from the null modem adapter on the CAP and the serial port on your PC.

Step 10 Remove the null modem adapter from the EIA/TIA-232 port on the CAP.

1.6.3 Unable to Ping Your PC

Symptom When connecting your PC to the ONS 15600 SDH, you are unable to ping the IP address of your PC to verify the IP configuration.

Table 1-5 describes the potential causes of the symptom and the solutions.

Table 1-5 Unable to Ping Your PC

Possible Problem	Solution
The IP address was typed incorrectly.	Verify that the IP address used to ping the PC matches the IP address displayed in the Windows IP Configuration information retrieved from the system. See the "Verify the IP Configuration of Your PC" procedure on page 1-56.
The IP configuration of your PC is not properly set.	To verify the IP configuration of your PC, see the "Verify the IP Configuration of Your PC" procedure on page 1-56. 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 on your PC.

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

Step 3 At the prompt in the DOS window for Windows 98, Windows NT, Windows 2000, or Windows XP, type **ipconfig** and press the **Enter** key.

The Windows IP configuration information appears, including the IP address, Subnet Mask, and the Default Gateway.

Step 4 At the prompt in the DOS window, type **ping** followed by the IP address you verified in Step 3.

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

- If the DOS window displays multiple (usually four) replies, the IP configuration is working properly.
- If you do not receive a reply, your IP configuration might not be properly set. Contact your network administrator for instructions to correct the IP configuration of your PC.

1.6.4 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.

Table 1-6 describes the potential cause of the symptom and the solutions.

Table 1-6 Browser Login Does Not Launch Java

Possible Problem	Solution
The PC operating system and browser are not properly configured.	Reconfigure the PC operating system and the browser. See the "Reconfigure the PC Operating System and the Browser" procedure on page 1-57.

Reconfigure the PC Operating System and the Browser

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.

a. Run the Cisco ONS 15600 SDH software CD.

b. Open the *CD drive*:\Windows\JRE folder.

c. Double-click the **jre-5_0-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 Double-click the **Java Plug-in 5.0** icon.

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

Step 6 From the Java Run Time Environment drop-down list, choose **JRE 5.0 in C:\ProgramFiles\JavaSoft\JRE\5.0**.

Step 7 Click **Apply**.

Step 8 In Communicator, click **Edit > Preferences**.

Step 9 Click **Advanced > Proxies > Direct connection to the Internet > OK**.

Step 10 Again in Communicator, click **Edit > Preferences**.

Step 11 Click **Advanced > Cache**.

Step 12 Confirm that the Disk Cache Folder field shows the following:

C:\ProgramFiles\Netscape\<username>\Communicator\cache for *platform/platform*.

Step 13 If the Disk Cache Folder field is not correct, click **Choose Folder**.

Step 14 Navigate to the file listed in Step 12 and click **OK**.

Step 15 Click **OK** in the Preferences window and exit the browser.

Step 16 Temporarily disable any virus-scanning software on the computer. See the "1.7.2 Browser Stalls When Downloading JAR Files From TSC Card" procedure on page 1-60.

Step 17 Verify that the computer does not have two network interface cards (NICs) installed. If the computer does have two NICs, remove one.

Step 18 Restart the browser and log into the ONS 15600 SDH.

1.6.5 Unable to Verify the NIC Connection on your PC

Symptom When connecting your PC to the ONS 15600 SDH, you are unable to verify that the NIC connection is working properly because the link LED is not illuminated or flashing.

Table 1-7 describes the potential causes of the symptom and the solutions.

Table 1-7 Unable to Verify the NIC Connection on Your PC

Possible Problem	Solution
The CAT-5 cable is not plugged in properly.	Confirm that both ends of the cable are properly inserted. If the cable is not fully inserted because of a broken locking clip, replace the cable.
The CAT-5 cable is damaged.	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.
Incorrect type of CAT-5 cable is being used.	• CAP connection: To connect an ONS 15600 SDH directly to your laptop/PC or a router, use a cross-over CAT-5 cable. To connect the ONS 15600 SDH to a hub or a LAN switch, use a straight-through CAT-5 cable. • TSC card connection: To connect an ONS 15600 SDH active TSC card directly to your laptop/PC, you might use either a straight-through or cross-over CAT-5 cable because the RJ-45 port on the faceplate is auto sensing. For details on the types of CAT-5 cables, see the "Crimp Replacement CAT-5 Cables" procedure on page 1-74.
The NIC is improperly inserted or installed.	• If you are using a PCMCIA-based NIC, remove and reinsert the 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.
The NIC is faulty.	Confirm that the NIC is working properly. If you have no issues connecting to the network (or any other node), the NIC should be working correctly. If you have difficulty connecting to the network (or any other node), the NIC might be faulty and needs to be replaced.

1.6.6 TCP/IP Connection is Lost

Symptom The TCP/IP connection was established and then lost, and a DISCONNECTED alarm appears on CTC.

Table 1-8 describes the potential cause of the symptom and the solution.

Table 1-8 TCP/IP Connection is Lost

Possible Problem	Solution
Your PC lost TCP/IP connection with the ONS 15600 SDH.	Use a standard ping command to verify the TCP/IP connection between the PC and the ONS 15600 SDH TSC card. A ping command will work if the PC connects directly to the TSC card or uses a LAN to access the TSC card. A ping command will also work if the CTC is connected through a gateway network element (GNE) and DCC if the node and CTC are in the same subnet or the required static routes are configured. See the "Ping the ONS 15600" procedure on page 1-59.

Ping the ONS 15600

Step 1 Display the command prompt:

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

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

Step 2 For both the Microsoft and Sun operating systems, type the following at the prompt:

ping *ONS 15600 SDH IP address*

For example

ping 192.1.0.2

If the workstation has connectivity to the ONS 15600 SDH, the ping is successful and displays a reply from the IP address. If the workstation does not have connectivity, a "Request timed out" message appears.

Step 3 If the ping is successful, it demonstrates that an active TCP/IP connection exists. Restart CTC.

Step 4 If the ping is not successful, and the workstation connects to the ONS 15600 SDH through a LAN, verify that the workstation's IP address is on the same subnet as the ONS node.

If the ping is not successful and the workstation connects directly to the ONS 15600 SDH, verify that the link light on the workstation NIC is illuminated.

1.7 CTC Operation Troubleshooting

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

1.7.1 Cisco Transport Controller Installation Wizard Hangs

Symptom The CTC Installation Wizard hangs or stalls during Netscape Communicator installation when installing the RealPlayer G2 plug-in application from the Cisco ONS 15600 SDH software or documentation CD-ROM.

Table 1-9 describes the potential cause of the symptom and the solutions.

Table 1-9 Cisco Transport Controller Installation Wizard Hangs

Possible Problem	Solution
RealPlayer G2 is incompatible with the CTC Installation Wizard when it is installed with the Netscape Communicator software.	Abort the installation. See the "Abort the Stalled Installation Wizard" procedure on page 1-60. Restart the CTC Installation Wizard and perform a custom Netscape Communicator installation that excludes RealPlayer G2 from the items being installed. Refer to the *Cisco ONS 15600 SDH Procedure Guide* to perform a custom installation that excludes RealPlayer G2. **Note** The RealPlayer G2 software can be installed separately at a later time without affecting the other Cisco Transport Controller software.

Abort the Stalled Installation Wizard

Step 1 Abort the stalled CTC Installation Wizard by pressing **Ctrl+Alt+Del**. The Windows Security dialog box appears.

Step 2 In the Windows Security dialog, click **Task Manager**.

Step 3 In the Windows Task Manager dialog box, highlight the Cisco Transport Controller Installation Wizard and click the **End Task** button.

Step 4 Click **Yes** in the confirmation dialog box.

Step 5 Navigate to the drive containing the CTC CD-ROM and double-click **setup.exe** to restart the CTC Installation Wizard.

Step 6 Refer to the *Cisco ONS 15600 SDH Procedure Guide* to perform a custom Netscape Communicator installation that excludes RealPlayer G2 from the items to be installed.

1.7.2 Browser Stalls When Downloading JAR Files From TSC Card

Symptom The browser stalls or hangs when downloading Cisco Transport Controller JAR files from the TSC card.

Table 1-10 describes the potential cause of the symptom and the solution.

Table 1-10 Browser Stalls When Downloading JAR Files From TSC Card

Possible Problem	Solution
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.	Run the CTC installation wizard to preinstall the CTC JAR files. Disable the VirusScan Download Scan feature. See the "Disable the VirusScan Download Scanning" procedure on page 1-61.

Disable the VirusScan Download Scanning

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 the **Configure** button on the lower part of the Task Properties window.

Step 4 Click the **Download Scan** icon next to the System Scan Properties dialog box.

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

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

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

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

Step 9 Close the McAfee VirusScan window.

1.7.3 Cisco Transport Controller Does Not Launch

Symptom CTC does not launch and usually an error message appears before the login screen appears.

Table 1-11 describes the potential causes of the symptom and the solutions.

Table 1-11 Cisco Transport Controller Does Not Launch

Possible Problem	Solution
The Communicator browser cache points to an invalid directory.	Redirect the Communicator cache to a valid directory. See the "Redirect the Communicator Cache to a Valid Directory" procedure on page 1-61.
The user is connected to the standby TSC card.	Connect the login PC to the port on the front of the active TSC card; the active TSC card has a green ACT/STBY LED illuminated. **Note** For typical TSC card LED behavior, see the "2.7 LED Behavior" section on page 2-118.

Redirect the Communicator Cache to a Valid Directory

Step 1 Launch Netscape Communicator.

Step 2 Display the **Edit** menu.

Step 3 Choose **Preferences**.

Step 4 In the Category column on the left-hand side, go to **Advanced** and choose the **Cache** tab.

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

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

1.7.4 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 15600 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 15600 SDH software CD and on the Cisco ONS 15600 SDH documentation CD. 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 1-12 shows JRE compatibility with ONS 15600 SDH software releases.

Table 1-12 JRE Compatibility

ONS Software Release	JRE 1.3 Compatible	JRE 1.4.2 Compatible[1]	JRE 5.0 Compatible	JRE 1.6 Compatible
ONS 15600 SDH R1.4	Yes	No	No	No
ONS 15600 SDH R8.0	No	No	Yes	No
ONS 15600 SDH R8.5	No	No	Yes	No
ONS 15600 SDH R9.0	No	No	Yes	No
ONS 15600 SDH R9.1	No	No	Yes	No
ONS 15600 SDH R9.2.1	No	No	No	Yes

[1] JRE 5.0 is the recommended version and is provided on the software CD.

1.7.5 Sluggish Cisco Transport Controller Operation or Login Problems

Symptom You experience sluggish CTC operation or have problems logging into CTC.

Table 1-13 describes the potential cause of the symptom and the solution.

Table 1-13 Sluggish Cisco Transport Controller Operation or Login Problems

Possible Problem	Solution
The CTC cache file is corrupted.	Delete the CTC cache file. This operation forces the ONS 15600 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 1-63 or the "Delete the CTC Cache File Manually" procedure on page 1-64.
Insufficient heap memory allocation.	Increase the heap size if you are using CTC to manage more than 50 nodes concurrently. See the "1.7.5.1 Set the CTC_HEAP and CTC_MAX_PERM_SIZE_HEAP Environment Variables for Windows" procedure on page 1-64 and the "Set the CTC_HEAP and CTC_MAX_PERM_SIZE_HEAP Environment Variables for Solaris" procedure on page 1-64. **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.

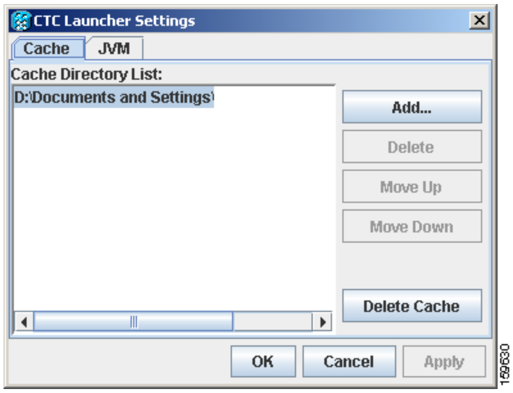
Delete the CTC Cache File Automatically

Step 1 Enter an ONS 15600 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 will not allow you to delete files that are in use.

Step 3 Click the **Settings** button on the initial browser window, then click **Delete CTC Cache** to clear the CTC cache. Figure 1-19 shows the Delete CTC Cache window.

Figure 1-19 The Delete the CTC Cache Window



Delete the CTC Cache File Manually

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 TSC card.

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

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

1.7.5.1 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 browser applications.

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

Example

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

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

1.7.6 Node Icon is Gray on Cisco Transport Controller Network View

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

Table 1-14 describes the potential causes of the symptom and the solutions.

Table 1-14 Node Icon is Gray on Cisco Transport Controller Network View

Possible Problem	Solution
Different CTC releases do not recognize each other.	Usually accompanied by an INCOMPATIBLE-SW alarm. Incompatibility occurs on login nodes with compatible software that encounter other nodes in the network that have a newer software version. **Note** In mixed-platform networks (ONS 15600 SDH and ONS 15454 SDH), you do not necessarily need to log into CTC on an ONS 15600 SDH node to enable operation, administration, maintenance, and provisioning (OAM&P) for all nodes. For example, ONS 15454 SDH also recognizes ONS 15600 SDH nodes.
A username/password mismatch.	Usually accompanied by a NOT-AUTHENTICATED alarm. Correct the username and password as described in the "1.7.8 Username or Password Mismatch" procedure on page 1-66.
No IP connectivity between nodes.	Usually accompanied by Ethernet-specific alarms. Verify the Ethernet connections between nodes.
A lost DCC connection.	Usually accompanied by an EOC alarm. Clear the EOC alarm and verify the DCC connection as described in the "EOC" alarm on page 2-41.
OSPF not properly configured.	Usually accompanied by a HELLO failure. Reconfigure the OSPF on the system to proper settings.
CTC launched from ONS 15454 SDH node.	You can manage an ONS 15600 SDH from CTC launched on the same release or higher CTC session from an ONS 1545 SDH node. Restart CTC and log into an ONS 15600 SDH node to enable node management.

1.7.7 Cisco Transport Controller Does Not Recognize the Node

Symptom This situation is often accompanied by the INCOMPATIBLE-SW alarm.

Table 1-15 describes the potential cause of the symptom and the solutions.

Table 1-15 Cisco Transport Controller Does Not Recognize the Node

Possible Problem	Solution
The software loaded on the connecting workstation and the software on the TSC card are incompatible.	Incompatibility occurs when the TSC card software is upgraded but the PC has not yet upgraded to 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. In mixed platform networks (ONS 15600 SDH and ONS 15454 SDH), you must log into the same or higher CTC software release as the one loaded on the ONS 15600 SDH node to enable OAM&P of all nodes. **Note** You cannot access other nodes over DCC (the gray nodes) when the PC is connected to the active TSC card unless that ONS 15600 SDH is configured as a gateway NE.

1.7.8 Username or Password Mismatch

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

Table 1-16 describes the potential cause of the symptom and the solution.

Table 1-16 Username or Password Mismatch

Possible Problem	Solution
The username or password entered does not match the information stored in the TSC card.	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 15600 SDH, type the **CISCO15** user name in capital letters, type the **otbu+1** password, and click **Login**. See the "Verify Correct Username and Password" procedure on page 1-66.
The username or password does not match the information stored in the RADIUS server database.	If the node has been configured for RADIUS authentication, the username and password are verified against the RADIUS server database rather than the security information in the local node database. For more information about RADIUS security, refer to the "Security" chapter in the *Cisco ONS 15600 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 user name and password.

Step 2 Contact your system administrator to verify the user name and password.

Step 3 Contact the Cisco TAC to create a new user name and password. See the "Obtaining Documentation and Submitting a Service Request" section on page xxxi.

1.7.9 Superuser Password Needs to Be Reset

Symptom The Superuser password has been lost or compromised.

Table 1-17 describes the potential cause of the symptom and the solution.

Table 1-17 No IP Connectivity Exists Between Nodes

Possible Problem	Solution
A security breach or record-keeping error has occurred.	Reset the ONS 15600 SDH to the default Superuser UID and password combination using the lamp test button using the "Reset the ONS 15600 SDH Password" procedure on page 1-67.

Reset the ONS 15600 SDH Password

Note To complete this procedure, you must be on site and have IP connectivity to the node.

Step 1 Locate the recessed button labeled LAMP TEST on the front of the active TSC card.

Step 2 Press in and hold down the recessed button labelled LAMP TEST for five seconds.

Step 3 Release the LAMP TEST button for approximately two seconds.

Step 4 Again press in and hold down the button labelled LAMP TEST for five seconds.

Step 5 Again release the LAMP TEST button.

Step 6 Start a normal CTC session. At the login screen, CTC accepts the default username and password set when the ONS 15600 SDH node shipped. The default username is **CISCO15** and the password is **otbu+1**. CISCO15 has Superuser rights and privileges, which allow you to create a user name and assign a password.

Note Other existing usernames and passwords are not affected by the reset. The Superuser reset applies only to the local node where the procedure is performed.

Step 7 If you need to create another user name and password, complete the following steps:

a. Click the **Provisioning** > **Security** tabs and click **create**.

b. Fill in the fields with a new user name and password and assign a security level.

c. Click **OK**.

Note After new user names and passwords are set up, including at least one Superuser, log in as a newly created Superuser and delete the default CISCO15 username and otbu+1 password to ensure that security is not compromised.

1.7.10 No IP Connectivity Exists Between Nodes

Symptom The nodes have a gray icon which is usually accompanied by alarms.

Table 1-18 describes the potential causes of the symptom and the solutions.

Table 1-18 No IP Connectivity Exists Between Nodes

Possible Problem	Solution
The node has lost DCC connection.	Usually is accompanied by DCC termination alarms, such as EOC or EOC-L. Clear the EOC (or EOC-L) alarm and verify the DCC connection as described in the "EOC" alarm on page 2-41.
The nodes are in different subnetworks and required static routes that are not provisioned.	Usually is accompanied by DCC termination alarms. Properly provision required static routes and nodes in the same subnets. Refer to the procedure for setting up CTC access in the *Cisco ONS 15600 SDH Procedure Guide*.
OSPF is not properly configured.	Usually is accompanied by OSPF Hello Fail alarms. Configure the OSPF to the proper settings. See the "HELLO" alarm on page 2-65.

1.7.11 DCC Connection Lost

Symptom A span between nodes on the network view is gray or the node is reporting DCC termination alarms, such as EOC.

Table 1-19 describes the potential cause of the symptom and the solution.

Table 1-19 DCC Connection Lost

Possible Problem	Solution
The DCC connection is lost.	Clear the EOC alarm and verify the DCC connection as described in the "EOC" alarm on page 2-41.

1.7.12 Loss of IP Communication Between Nodes on an OSPF LAN

Symptom The CTC session on an ONS 15600 SDH connected to Router 1 loses communication with the ONS 15600 SDH connected to Router 2 on the same LAN in OSPF backbone Area 0.

Table 1-20 describes the potential causes of the symptom and the solutions.

Table 1-20 Loss of IP Communication in Segmented OSPF Area

Possible Problem	Solution
The OSPF backbone Area 0 has segmented into multiple gateway network elements (GNEs_.	If multiple ONS 15600 SDH nodes and routers are connected to the same LAN in OSPF backbone Area 0 and a link between two routers breaks, the backbone OSPF area 0 could divide into multiple GNEs. If this occurs, the CTC session on the ONS node connected to Router 1 will not be able to communicate with the ONS 15600 SDH connected to Router 2. This is standard behavior for an OSPF network. To resolve this problem, you must repair the link between the routers or provide another form of redundancy in the network. Refer to the *Cisco ONS 15600 SDH Procedure Guide* for procedures to repair the link between the routers.
A broken link between two routers on the LAN in OSPF backbone Area 0.	

1.8 Circuits and Timing

This section provides solutions to circuit creation and reporting errors, as well as common timing reference errors and alarms.

1.8.1 ONS 15600 SDH Switches Timing Reference

Symptom Timing references switch when one or more problems occur.

Table 1-21 describes the potential causes of the symptom and the solutions.

Table 1-21 ONS 15600 Switches Timing Reference

Possible Problem	Solution
The optical or building integrated timing supply (BITS) input is receiving loss of signal (LOS), loss of frame (LOF), or AIS from its timing source.	Clear the alarm and set up the timing source to a reliable source. To clear an LOS (BITS) alarm, see the "LOS (BITS)" alarm on page 2-84. To clear an LOF (BITS) alarm, see the "LOF (BITS)" alarm on page 2-80. To clear an AIS (BITS) alarm, see the "AIS" condition on page 2-15. Refer to the procedure for setting up timing in the *Cisco ONS 15600 SDH Procedure Guide*.
The optical or BITS input is not functioning.	
Synchronization status messaging (SSM) message is set to do not use (DUS).	The Synchronization Status Message (SSM) Changed to Do Not Use (DUS) condition occurs when the synchronization status message quality level is changed to DUS. The port that reports the condition is not at fault. The condition applies to the timing source. SSM-DUS prevents timing loops by providing a termination point for the signal usage. To clear the SSM-DUS alarm, see the "SSM-DUS" condition on page 2-110.
SSM indicates a Stratum 3 or lower clock quality.	

Table 1-21 ONS 15600 Switches Timing Reference (continued)

Possible Problem	Solution
The input frequency is off by more than 15 ppm.	Set up the timing input to a reliable timing source. Refer to the procedure for setting up timing in the *Cisco ONS 15600 SDH Procedure Guide*.
The input clock wanders and has more than three slips in 30 seconds.	

1.8.2 Holdover Synchronization Alarm

Symptom The clock is running at a different frequency than normal and the HLDOVRSYNC alarm appears. Holdover occurs when the node is provisioned for external or line timing and both of the provisioned references fail. The timing switches to the internal Stratum 3E clock on the TSC card.

Table 1-22 describes the potential cause of the symptom and the solution.

Table 1-22 Holdover Synchronization Alarm

Possible Problem	Solution
The primary and secondary reference inputs have failed.	This alarm is raised when the primary and secondary reference inputs fail. See the "HLDOVRSYNC" condition on page 2-66 for a detailed description. **Note** The ONS 15600 SDH supports holdover timing per Telcordia GR-436-CORE when provisioned for external timing.

1.8.3 Free-Running Synchronization Mode

Symptom The clock is running at a different frequency than normal and the FRNGSYNC alarm appears. Free Running is reported when the node is running on the internal clock after a failure of the primary and secondary clock references.

Table 1-23 describes the potential cause of the symptom and the solution.

Table 1-23 Free-Running Synchronization Mode

Possible Problem	Solution
No reliable reference input is available.	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 on page 2-64 for a detailed description.

1.8.4 Daisy-Chained BITS Not Functioning

Symptom You are unable to daisy-chain the BITS.

Table 1-24 describes the potential cause of the symptom and the solution.

Table 1-24 Daisy-Chained BITS Not Functioning

Possible Problem	Solution
Daisy-chaining BITS is not supported on the ONS 15600 SDH.	Daisy-chaining 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 15600 SDH. You cannot use BITS Out A and/or BITS Out B outputs when providing a clock source from BITS In A and/or BITS In B inputs. To provide BITS Out A and/or BITS Out B external outputs, the clock source must be derived from an optical input.

1.8.5 Circuits Remain in PARTIAL Status

Symptom Circuits remain in the PARTIAL status.

Table 1-27 describes the potential cause of the symptom and the solution.

Table 1-25 Circuits Remain in PARTIAL Status

Possible Problem	Solution
The MAC address changed.	Repair the circuits. See the "Repair Circuits" procedure on page 1-71.
The node is resetting.	Wait for the node to finish the reset.
The node has lost DCC connectivity.	See the "1.6.6 TCP/IP Connection is Lost" section on page 1-58.
There are user ID and.or password issues.	See the "1.7.8 Username or Password Mismatch" section on page 1-66.
Server Trail deleted.	—

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 CAP.

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 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 an RMA.

1.9 Fiber and Cabling

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

1.9.1 Bit Errors Appear for an Optical Traffic Card

Symptom An optical traffic card has multiple bit errors.

Table 1-26 describes the potential causes of the symptom and the solutions.

Table 1-26 Bit Errors Appear for a Traffic Card

Possible Problem	Solution
Faulty cabling Low optical-line power High optical-line power	Bit errors on line (traffic) ports usually originate from cabling problems or low or high optical-line power levels. The errors can be caused by synchronization problems, especially if PJ (pointer justification) errors are reported. Troubleshoot cabling problems using the "1.1 Network Troubleshooting Tests" section on page 1-2. Troubleshoot low or high optical-line power levels using the "1.9.2 Faulty Fiber-Optic Connections" section on page 1-72. Use a test set whenever possible to check for errors.

1.9.2 Faulty Fiber-Optic Connections

Symptom An optical (STM-N) card has multiple SDH alarms or signal errors.

Table 1-27 describes the potential cause of the symptom and the solution.

Table 1-27 Faulty Fiber-Optic Connections

Possible Problem	Solution
Faulty fiber-optic connections to the optical (STM-N) card	Faulty fiber-optic connections can be the source of SDH alarms and signal errors. See the "Verify Fiber-Optic Connections" procedure on page 1-73.

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

Warning **Invisible laser radiation may be emitted from the end of the unterminated fiber cable or connector. Do not view 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 may pose an eye hazard.** Statement 1056

Verify Fiber-Optic Connections

Step 1 Ensure that a single-mode fiber connects the ONS 15600 SDH optical (STM-N) port(s).

SM or SM Fiber should be printed on the fiber span cable. ONS 15600 SDH optical (STM-N) cards do not use multimode fiber.

Step 2 Ensure that the OGI fiber connector is properly aligned and locked.

Step 3 Verify that the single-mode fiber optical-line power level coming into the breakout panel is within the specified range:

a. Remove the Rx end of the suspect fiber.

b. Connect the Rx end of the suspect fiber to a fiber-optic power meter, such as a GN Nettest LP-5000.

c. Determine the power level of the fiber with the fiber-optic power meter.

d. Verify that the power meter is set to the appropriate wavelength for the optical (STM-N) card you are testing (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 "1.9.3 Optical Traffic Card Transmit and Receive Levels" section on page 1-76.

- If the power level is within tolerance, the problem is with the fan-out cables or the optical (STM-N) card.
- If the power level is too high, add the appropriate attenuation.

Step 4 If the power level falls below the specified range:

Note When this condition occurs, the far-end node is usually an ONS 15454 SDH.

a. Clean or replace the OGI fiber fan-out cables. If possible, do this for the optical (STM-N) card you are working on and the far-end card. Refer to the *Cisco ONS 15600 SDH Procedure Guide* for fiber cleaning procedures.

b. Clean the optical connectors on the card. If possible, do this for the optical (STM-N) card you are working on and the far-end card. Refer to the *Cisco ONS 15600 SDH Procedure Guide* for fiber cleaning procedures.

c. Replace the far-end transmitting optical (STM-N) card to eliminate the possibility of a degrading transmitter on the far-end optical (STM-N) card.

d. 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 STM-N port failed.

a. Check that the Tx and Rx fibers are not reversed. LOS and EOC alarms normally accompany reversed Tx and Rx fibers. Fixing reversed Tx and Rx fibers clears the alarms and restores the signal.

b. Clean or replace the OGI fiber fan-out cables. If possible, do this for both the STM-N port you are working on and the far-end STM-N port. Refer to the *Cisco ONS 15600 SDH Procedure Guide* for fiber cleaning procedures.

c. Retest the fiber power level.

d. If the replacement fiber still shows no power, replace the optical (STM-N) card.

Tip To prevent overloading the receiver, use an attenuator on the fiber between the STM-N port transmitter and the receiver. Place the attenuator on the receive transmitter of the STM-N ports. Refer to the attenuator documentation for specific instructions.

Crimp Replacement CAT-5 Cables

You can crimp your own CAT-5 cables for use with the ONS 15600 SDH. To connect the CAP of an ONS 15600 SDH directly to your laptop/PC or a router, use a straight-through CAT-5 cable. To connect the CAP of an ONS 15600 SDH to a hub or a LAN switch, use a cross-over CAT-5 cable. To connect an ONS 15600 SDH active TSC card directly to your laptop/PC, you might use either a straight-through or cross-over CAT-5 cable because the RJ-45 port on the faceplate is autosensing.

Use a straight-through or cross-over cable to connect to the backplane Ethernet connections of an ONS 15600 SDH. Use a straight-through cable to connect to the faceplate connector of the ONS 15600 SDH TSC card. Use CAT-5 cable RJ-45 T-568B, Color Code (100 Mbps), and a crimping tool. Figure 1-20 shows the layout of an RJ-45 connector.

Figure 1-20 ***RJ-45 Pin Numbers***

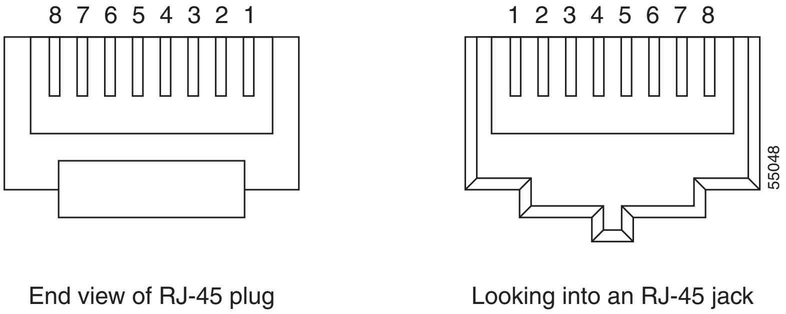


Figure 1-21 shows the layout of a straight-through cable.

Figure 1-21 ***Straight-Through Cable Layout***

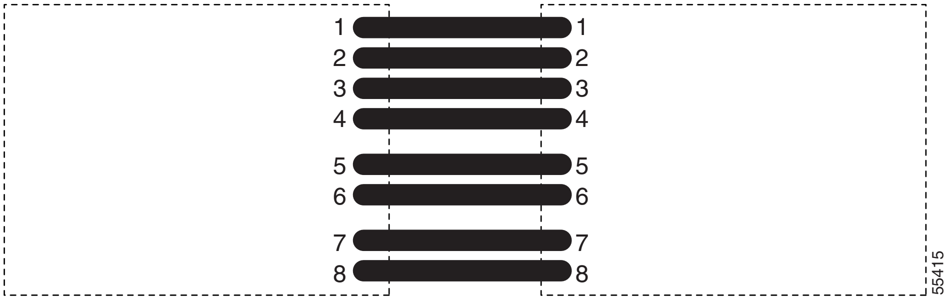


Table 1-28 shows the straight-through cable pinout.

Table 1-28 ***Straight-Through 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 1-22 shows the layout of a cross-over cable.

Figure 1-22 Crossover Cable Layout

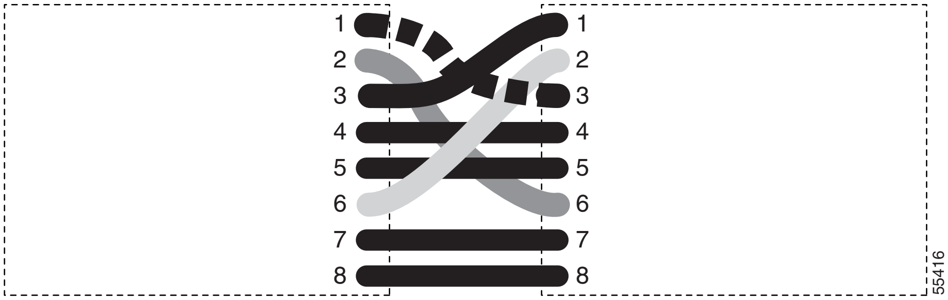


Table 1-29 shows the cross-over cable pinout.

Table 1-29 Crossover Cable Pinout

Pin	Color	Pair	Name	Pin
1	White/Orange	2	Transmit Data +	3
2	Orange	2	Transmit Data –	6
3	White/Green	3	Receive Data +	1
4	Blue	1	—	4
5	White/Blue	1	—	5
6	Green	3	Receive Data –	2
7	White/Brown	4	—	7
8	Brown	4	—	8

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

1.9.3 Optical Traffic Card Transmit and Receive Levels

Each optical traffic card has connectors on its faceplate that contain both transmit and receive ports. Table 1-30 shows the optical power levels for the transmit and receive ports of the optical traffic cards.

Table 1-30 Optical Transmit and Receive Levels

	Transmit		Receive	
Card	Minimum	Maximum	Minimum	Maximum
OC48/STM16 LR16 1550	–2 dBm	+3 dBm	–28 dBm	–9 dBm
OC192/STM64 LR4 1550	+4 dBm	+7 dBm	–22 dBm	–9 dBm
OC48/STM16 SR16 1310	–10 dBm	–3 dBm	–18 dBm	–3 dBm
OC192/STM64 SR4 1310	–6 dBm	–1 dBm	–11 dBm	–1 dBm
OC192/STM64 4 Port ITU C-Band				
ASAP SFPs				

Table 1-30 Optical Transmit and Receive Levels (continued)

	Transmit		Receive	
Card	**Minimum**	**Maximum**	**Minimum**	**Maximum**
ONS-SE-Z1 (Supports STM-1 SR-1, STM-4 SR-1, STM-16 IR-1, or GE LX)	–5.0 dBm	0 dBm	–23[1] –19[2] –18[3]	–3[1] –3[2] 0[3]
ONS-SI-155-L2 (Supports STM-1 LR-2)	–15	–8.0	–28	–8
ONS-SI-622-L2 (Supports STM-4 LR-2)	–5.0	0	–34	–10
ONS-SE-2G-L2 (Supports STM-16 LR-2)	–2.0	3.0	–28	–9
ONS-SI-2G-S1 (Supports STM-16, LR-2)	–2.0	3.0	–9	

[1] 155.52/622.08 Mbps

[2] 1250 Mbps

[3] 2488.32 Mbps

The CTC Maintenance > Transceiver tab shows the optical power transmitted (OPT) and optical power received (OPR) levels.

Note CTC might show OPT levels at 1 dBm more or less than the actual card OPT level.

1.10 Power Supply Problems

This section provides the a procedure for troubleshooting power supply difficulties.

Note For information about power consumption for nodes and cards, refer to the *Cisco ONS 15600 SDH Reference Manual*.

Symptom Loss of power or low voltage, resulting in a loss of traffic.

Table 1-31 describes the potential causes of the symptom and the solutions.

Table 1-31 Power Supply Problems

Possible Problem	Solution
A loss of power or low voltage reading.	The ONS 15600 SDH requires a constant source of DC power to properly function. Input voltage range is from –40.5 VDC to –72 VDC.
An improperly connected power supply.	A newly installed ONS 15600 SDH that is not properly connected to its power supply will not operate. Power problems can be confined to a specific ONS 15600 SDH or affect several pieces of equipment on the site. A loss of power or low voltage can result in a loss of traffic. See the "Isolate the Cause of Power Supply Problems" procedure on page 1-78.

Caution Operations that interrupt power supply or short the power connections to the ONS 15600 SDH are service-affecting.

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 equipment. This could cause the metal objects to heat up and cause serious burns or weld the metal object to the equipment.** Statement 207

Warning **Static electricity can damage electro-optical modules. While handling electro-optical module, wear a grounding wrist strap to discharge the static buildup. Wrist straps are designed to prevent static electricity damage to equipment.** Statement 312

Isolate the Cause of Power Supply Problems

Step 1 If a single ONS 15600 SDH show signs of fluctuating power or power loss:

a. Verify that the –48 VDC power terminals are properly connected to the power distribution unit (PDU).

b. Verify that the power cable is in good condition.

c. Verify that the power cable connections are properly crimped.

d. Verify that 50-A circuit breakers are used in the PDU.

e. Verify that the circuit breakers are not blown or tripped.

f. Verify that a rack-ground cable attaches to the frame-ground terminal (FGND) on the ONS 15600 SDH. 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 voltage is in the specified range from –40.5 VDC to –72 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.

CHAPTER 2

Alarm Troubleshooting

This chapter gives a description, severity, and troubleshooting procedure for each commonly encountered Cisco ONS 15600 SDH alarm and condition. Tables 2-1 through 2-5 provide lists of ONS 15600 SDH alarms organized by severity. Table 2-6 on page 2-4 provides a list of alarms organized alphabetically. Table 2-7 gives definitions of all ONS 15600 SDH alarm logical objects, which are the basis of the alarm profile list in Table 2-8 on page 2-8. For a comprehensive list of all conditions, refer to the *Cisco ONS SDH TL1 Command Guide*.

An alarm troubleshooting procedure applies to both the Cisco Transport Controller (CTC) and Transaction Language One (TL1) version of that alarm. If the troubleshooting procedure does not clear the alarm, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call the Cisco Technical Assistance Center (TAC) (1-800-553-2447).

2.1 Alarm Indexes by Default Severity

The following tables group alarms and conditions by their default severities in the ONS 15600 SDH system. These severities are the same whether they are reported in the CTC Alarms window severity (SEV) column or in TL1.

Note The CTC default alarm profile contains some alarms or conditions which are not currently implemented but are reserved for future use.

Note The CTC default alarm profile in some cases contains two severities for one alarm (for example, MJ/MN). The ONS 15600 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. This is in accordance with Telcordia GR-474-CORE.

2.1.1 Critical Alarms (CR)

Table 2-1 alphabetically lists ONS 15600 SDH Critical (CR) alarms.

Table 2-1 ONS 15600 SDH Critical Alarm List

AU-LOP (VCMON-HP)	HP-PLM (VCMON-HP)	MEA (EQPT)
BKUPMEMP (EQPT)	HP-UNEQ (VCMON-HP)	MEA (PIM)

Table 2-1 ONS 15600 SDH Critical Alarm List (continued)

CTNEQPT-PB-A (EQPT)	IMPROPRMVL (EQPT)	MEA (PPM)
CTNEQPT-PB-B (EQPT)	IMPROPRMVL (FAN)	MFGMEM (EQPT)
ENCAP-MISMATCH-P (POS)	IMPROPRMVL (PIM)	MFGMEM (FAN)
EQPT (EQPT)	IMPROPRMVL (PPM)	MFGMEM (PIM)
EQPT (PIM)	LASER-BIAS (EQPT)	MFGMEM (PPM)
EQPT (PPM)	LASER-BIAS (PPM)	RS-TIM (STMN)
EQPT-BOOT (EQPT)	LASER-OVER-TEMP (EQPT)	SYNCCLK (NE)
EQPT-CC-PIM (PIM)	LASER-OVER-TEMP (PPM)	XCMTX (NE)
EQPT-PIM-PPM (PPM)	LOF (STMN)	—
FAN-FAIL (FAN)	LOS (STMN)	—

2.1.2 Major Alarms (MJ)

Table 2-2 alphabetically lists ONS 15600 SDH Major (MJ) alarms.

Table 2-2 ONS 15600 SDH Major Alarm List

APSCM (STMN)	E-W-MISMATCH (STMN)	MEM-GONE (EQPT)
APSCNMIS (STMN)	EXTRA-TRAF-PREEMPT (STMN)	PRC-DUPID (STMN)
CARLOSS (GIGE)	FAN-FAIL-PARTIAL (FAN)	PWR (PWR)
CLKFAIL (EQPT)	GFP-LFD (POS)	RING-MISMATCH (STMN)
CXCHALT (EQPT)	GFP-UP-MISMATCH (POS)	SYNCPRI (NE-SREF)
DBOSYNC (NE)	HIBATVG (PWR)	SYSBOOT (NE)
EHIBATVG (PWR)	INVMACADR (BPlane)	TPTFAIL (POS)
ELWBATVG (PWR)	LWBATVG (PWR)	WVL-OUT-OF-LOCK (STMN)

2.1.3 Minor Alarms (MN)

Table 2-3 alphabetically lists ONS 15600 SDH Minor (MN) alarms.

Table 2-3 ONS 15600 SDH Minor Alarm List

APSB (STMN)	HELLO (STMN)	NON-CISCO-PPM (PPM)
APSCDFLTK (STMN)	HI-LASERBIAS (PPM)	OPEN-SLOT (EQPT)
APSC-IMP (STMN)	HI-LASERBIAS (STMN)	PROV-MISMATCH (PPM)
APSCINCON (STMN)	HI-RXPOWER (STMN)	PWR-FA (BPlane)
AUTORESET (EQPT)	HI-TXPOWER (PPM)	PWR-FAIL-A (CAP)
BPV (BITS)	HI-TXPOWER (STMN)	PWR-FAIL-A (EQPT)
CIDMISMATCH-A (EQPT)	HP-TIM (VCMON-HP)	PWR-FAIL-B (CAP)
CIDMISMATCH-B (EQPT)	IMPROPRMVL (CAP)	PWR-FAIL-B (EQPT)

Table 2-3 ONS 15600 SDH Minor Alarm List (continued)

CONTBUS-CLK-A (EQPT)	IMPR-XC (NE)	PWR-FAIL-RET-A (EQPT)
CONTBUS-CLK-B (EQPT)	ISIS-ADJ-FAIL (STMN)	PWR-FAIL-RET-B (EQPT)
CONTBUS-IO-A (EQPT)	KBYTE-APS-CHANNEL-FAILURE (STMN)	RS-EOC (STMN)
CONTBUS-IO-B (EQPT)	LOF (BITS)	SFTWDOWN (EQPT)
CONTCOM (EQPT)	LO-LASERBIAS (PPM)	SNTP-HOST (NE)
DATAFLT (NE)	LO-LASERBIAS (STMN)	SSM-FAIL (BITS)
DUP-IPADDR (NE)	LO-RXPOWER (STMN)	SSM-FAIL (STMN)
DUP-NODENAME (NE)	LOS (BITS)	SYNCPRI (EXT-SREF)
EQPT (CAP)	LO-TXPOWER (PPM)	SYNCSEC (EXT-SREF)
EQPT-HITEMP (EQPT)	LO-TXPOWER (STMN)	SYNCSEC (NE-SREF)
EXT (ENVALRM)	MATECLK (EQPT)	SYNCTHIRD (EXT-SREF)
FAN-DEGRADE (FAN)	MEM-LOW (EQPT)	UNPROT-SYNCCLK (NE)
FAN-PWR (FAN)	MFGMEM (CAP)	UNPROT-XCMTX (NE)
FEPRLF (STMN)	MS-EOC (STMN)	UNQUAL-PPM (PPM)
FREQ-MISMATCH (EQPT)	MSSP-SW-VER-MISM (STMN)	UNROUTEABLE-IP (NE)

2.1.4 Not Alarmed (NA) Conditions

Table 2-4 alphabetically lists ONS 15600 SDH Not Alarmed conditions.

Table 2-4 ONS 15600 SDH NA Conditions List

ALS (STMN)	HP-DEG (VCMON-HP)	SSM-DUS (STMN)
AUD-LOG-LOSS (NE)	HP-EXC (VCMON-HP)	SSM-LNC (BITS)
AUD-LOG-LOW (NE)	INTRUSION-PSWD (NE)	SSM-LNC (NE-SREF)
AUTOSW-LOP-SNCP (VCMON-HP)	KB-PASSTHR (STMN)	SSM-LNC (STMN)
AUTOSW-SDBER-SNCP (VCMON-HP)	LKOUTPR-S (STMN)	SSM-OFF (BITS)
AUTOSW-SFBER-SNCP (VCMON-HP)	LOCKOUT-REQ (STMN)	SSM-OFF (STMN)
AUTOSW-UNEQ-SNCP (VCMON-HP)	LOCKOUT-REQ (VCMON-HP)	SSM-PRC (BITS)
CHANLOSS (STMN)	LOCKOUT-REQ-RING (STMN)	SSM-PRC (NE-SREF)
EXERCISE-RING-FAIL (STMN)	LPBKCRS (VCMON-HP)	SSM-PRC (STMN)
FAILTOSW (STMN)	LPBKFACILITY (GIGE)	SSM-RES (BITS)
FAILTOSW-HO (VCMON-HP)	LPBKFACILITY (STMN)	SSM-SDH-TN (BITS)
FAILTOSWR (STMN)	LPBKPAYLOAD (STMN)	SSM-SDH-TN (NE-SREF)
FAILTOSWS (STMN)	LPBKTERMINAL (GIGE)	SSM-SDH-TN (STMN)
FE-FRCDWKSWBK-SPAN (STMN)	LPBKTERMINAL (STMN)	SSM-SETS (BITS)
FE-FRCDWKSWPR-RING (STMN)	MAN-REQ (VCMON-HP)	SSM-SETS (NE-SREF)
FE-FRCDWKSWPR-SPAN (STMN)	MANRESET (PIM)	SSM-SETS (STMN)

Table 2-4 ONS 15600 SDH NA Conditions List (continued)

FE-LOCKOUTOFPR-ALL (STMN)	MANRESET (PPM)	SSM-SMC (STMN)
FE-LOCKOUTOFPR-SPAN (STMN)	MANSWTOINT (NE-SREF)	SSM-STU (BITS)
FE-MANWKSWBK-SPAN (STMN)	MANSWTOPRI (EXT-SREF)	SSM-STU (NE-SREF)
FE-MANWKSWPR-RING (STMN)	MANSWTOPRI (NE-SREF)	SSM-STU (STMN)
FE-MANWKSWPR-SPAN (STMN)	MANSWTOSEC (EXT-SREF)	SWTOPRI (EXT-SREF)
FE-SF-SPAN (STMN)	MANSWTOSEC (NE-SREF)	SWTOPRI (NE-SREF)
FORCED-REQ (VCMON-HP)	MANSWTOTHIRD (EXT-SREF)	SWTOSEC (EXT-SREF)
FORCED-REQ-RING (STMN)	MANSWTOTHIRD (NE-SREF)	SWTOSEC (NE-SREF)
FORCED-REQ-SPAN (STMN)	MANUAL-REQ-RING (STMN)	SWTOTHIRD (EXT-SREF)
FRCDSWTOINT (NE-SREF)	MANUAL-REQ-SPAN (STMN)	SWTOTHIRD (NE-SREF)
FRCDSWTOPRI (EXT-SREF)	MS-DEG (STMN)	SW-VER (EQPT)
FRCDSWTOPRI (NE-SREF)	MS-EXC (STMN)	SYNC-FREQ (BITS)
FRCDSWTOSEC (EXT-SREF)	MS-SQUELCH-HP (STMN)	SYNC-FREQ (STMN)
FRCDSWTOSEC (NE-SREF)	PWRRESTART (EQPT)	UPGRADE (NE)
FRCDSWTOTHIRD (EXT-SREF)	RING-SW-EAST (STMN)	VOLT-MISM (PWR)
FRCDSWTOTHIRD (NE-SREF)	RING-SW-WEST (STMN)	WKSWPR (STMN)
FRNGSYNC (NE-SREF)	ROLL (VCMON-HP)	WKSWPR (VCMON-HP)
FSTSYNC (EQPT)	ROLL-PEND (VCMON-HP)	WTR (STMN)
FULLPASSTHR-BI (STMN)	SSM-DUS (BITS)	WTR (VCMON-HP)
HLDOVRSYNC (NE-SREF)	SSM-SMC (BITS)	—
MANRESET (EQPT)	SSM-SMC (NE-SREF)	—

2.1.5 Not Reported (NR) Conditions

Table 2-5 alphabetically lists ONS 15600 SDH Not Reported conditions.

Table 2-5 ONS 15600 SDH NR Conditions List

AIS (BITS)	AUTOSW-AIS-SNCP (VCMON-HP)	MS-AIS (STMN)
AU-AIS (VCMON-HP)	HP-RFI (VCMON-HP)	MS-RFI (STMN)

2.2 Alarms and Conditions Listed by Alphabetical Entry

Table 2-6 alphabetically lists all ONS 15600 SDH alarms and conditions.

Table 2-6 ONS 15600 SDH Alarm and Condition Alphabetical List

AIS (BITS)	FRNGSYNC (NE-SREF)	MS-EOC (STMN)
ALS (STMN)	FSTSYNC (EQPT)	MS-EXC (STMN)

Table 2-6 ONS 15600 SDH Alarm and Condition Alphabetical List (continued)

APSB (STMN)	FULLPASSTHR-BI (STMN)	MS-RFI (STMN)
APSCDFLTK (STMN)	GFP-LFD (POS)	MSSP-SW-VER-MISM (STMN)
APSC-IMP (STMN)	GFP-UP-MISMATCH (POS)	MS-SQUELCH-HP (STMN)
APSCINCON (STMN)	HELLO (STMN)	NON-CISCO-PPM (PPM)
APSCM (STMN)	HIBATVG (PWR)	OPEN-SLOT (EQPT)
APSCNMIS (STMN)	HI-LASERBIAS (PPM)	PRC-DUPID (STMN)
AU-AIS (VCMON-HP)	HI-LASERBIAS (STMN)	PROV-MISMATCH (PPM)
AUD-LOG-LOSS (NE)	HI-RXPOWER (STMN)	PWR (PWR)
AUD-LOG-LOW (NE)	HI-TXPOWER (PPM)	PWR-FA (BPlane)
AU-LOP (VCMON-HP)	HI-TXPOWER (STMN)	PWR-FAIL-A (CAP)
AUTORESET (EQPT)	HLDOVRSYNC (NE-SREF)	PWR-FAIL-A (EQPT)
AUTOSW-AIS-SNCP (VCMON-HP)	HP-DEG (VCMON-HP)	PWR-FAIL-B (CAP)
AUTOSW-LOP-SNCP (VCMON-HP)	HP-EXC (VCMON-HP)	PWR-FAIL-B (EQPT)
AUTOSW-SDBER-SNCP (VCMON-HP)	HP-PLM (VCMON-HP)	PWR-FAIL-RET-A (EQPT)
AUTOSW-SFBER-SNCP (VCMON-HP)	HP-RFI (VCMON-HP)	PWR-FAIL-RET-B (EQPT)
AUTOSW-UNEQ-SNCP (VCMON-HP)	HP-TIM (VCMON-HP)	PWRRESTART (EQPT)
BKUPMEMP (EQPT)	HP-UNEQ (VCMON-HP)	RING-MISMATCH (STMN)
BPV (BITS)	IMPROPRMVL (CAP)	RING-SW-EAST (STMN)
CARLOSS (GIGE)	IMPROPRMVL (EQPT)	RING-SW-WEST (STMN)
CHANLOSS (STMN)	IMPROPRMVL (FAN)	ROLL (VCMON-HP)
CIDMISMATCH-A (EQPT)	IMPROPRMVL (PIM)	ROLL-PEND (VCMON-HP)
CIDMISMATCH-B (EQPT)	IMPROPRMVL (PPM)	RS-EOC (STMN)
CLKFAIL (EQPT)	IMPR-XC (NE)	RS-TIM (STMN)
CONTBUS-CLK-A (EQPT)	INTRUSION-PSWD (NE)	SFTWDOWN (EQPT)
CONTBUS-CLK-B (EQPT)	INVMACADR (BPlane)	SNTP-HOST (NE)
CONTBUS-IO-A (EQPT)	ISIS-ADJ-FAIL (STMN)	SSM-DUS (BITS)
CONTBUS-IO-B (EQPT)	KB-PASSTHR (STMN)	SSM-DUS (STMN)
CONTCOM (EQPT)	KBYTE-APS-CHANNEL-FAILURE (STMN)	SSM-FAIL (BITS)
CTNEQPT-PB-A (EQPT)	LASER-BIAS (EQPT)	SSM-FAIL (STMN)
CTNEQPT-PB-B (EQPT)	LASER-BIAS (PPM)	SSM-LNC (BITS)
CXCHALT (EQPT)	LASER-OVER-TEMP (EQPT)	SSM-LNC (NE-SREF)
DATAFLT (NE)	LASER-OVER-TEMP (PPM)	SSM-LNC (STMN)
DBOSYNC (NE)	LKOUTPR-S (STMN)	SSM-OFF (BITS)
DUP-IPADDR (NE)	LOCKOUT-REQ (STMN)	SSM-PRC (BITS)
DUP-NODENAME (NE)	LOCKOUT-REQ (VCMON-HP)	SSM-PRC (NE-SREF)
EHIBATVG (PWR)	LOCKOUT-REQ-RING (STMN)	SSM-PRC (STMN)

Table 2-6 ONS 15600 SDH Alarm and Condition Alphabetical List (continued)

ELWBATVG (PWR)	LOF (BITS)	SSM-RES (BITS)
ENCAP-MISMATCH-P (POS)	LOF (STMN)	SSM-SDH-TN (BITS)
EQPT (CAP)	LO-LASERBIAS (PPM)	SSM-SDH-TN (NE-SREF)
EQPT (EQPT)	LO-LASERBIAS (STMN)	SSM-SDH-TN (STMN)
EQPT (PIM)	LO-RXPOWER (STMN)	SSM-SETS (BITS)
EQPT (PPM)	LOS (BITS)	SSM-SETS (NE-SREF)
EQPT-BOOT (EQPT)	LOS (STMN)	SSM-SETS (STMN)
EQPT-CC-PIM (PIM)	LO-TXPOWER (PPM)	SSM-SMC (BITS)
EQPT-HITEMP (EQPT)	LO-TXPOWER (STMN)	SSM-SMC (NE-SREF)
EQPT-PIM-PPM (PPM)	LPBKCRS (VCMON-HP)	SSM-SMC (STMN)
E-W-MISMATCH (STMN)	LPBKFACILITY (GIGE)	SSM-STU (BITS)
EXERCISE-RING-FAIL (STMN)	LPBKFACILITY (STMN)	SSM-STU (NE-SREF)
EXT (ENVALRM)	LPBKPAYLOAD (STMN)	SSM-STU (STMN)
EXTRA-TRAF-PREEMPT (STMN)	LPBKTERMINAL (GIGE)	SWTOPRI (EXT-SREF)
FAILTOSW (STMN)	LPBKTERMINAL (STMN)	SWTOPRI (NE-SREF)
FAILTOSW-HO (VCMON-HP)	LWBATVG (PWR)	SWTOSEC (EXT-SREF)
FAILTOSWR (STMN)	MAN-REQ (VCMON-HP)	SWTOSEC (NE-SREF)
FAILTOSWS (STMN)	MANRESET (EQPT)	SWTOTHIRD (EXT-SREF)
FAN-DEGRADE (FAN)	MANRESET (PIM)	SWTOTHIRD (NE-SREF)
FAN-FAIL (FAN)	MANRESET (PPM)	SW-VER (EQPT)
FAN-FAIL-PARTIAL (FAN)	MANSWTOINT (NE-SREF)	SYNCCLK (NE)
FAN-PWR (FAN)	MANSWTOPRI (EXT-SREF)	SYNC-FREQ (BITS)
FE-FRCDWKSWBK-SPAN (STMN)	MANSWTOPRI (NE-SREF)	SYNC-FREQ (STMN)
FE-FRCDWKSWPR-RING (STMN)	MANSWTOSEC (EXT-SREF)	SYNCPRI (EXT-SREF)
FE-FRCDWKSWPR-SPAN (STMN)	MANSWTOSEC (NE-SREF)	SYNCPRI (NE-SREF)
FE-LOCKOUTOFPR-ALL (STMN)	MANSWTOTHIRD (EXT-SREF)	SYNCSEC (EXT-SREF)
FE-LOCKOUTOFPR-SPAN (STMN)	MANSWTOTHIRD (NE-SREF)	SYNCSEC (NE-SREF)
FE-MANWKSWBK-SPAN (STMN)	MANUAL-REQ-RING (STMN)	SYNCTHIRD (EXT-SREF)
FE-MANWKSWPR-RING (STMN)	MANUAL-REQ-SPAN (STMN)	SYSBOOT (NE)
FE-MANWKSWPR-SPAN (STMN)	MATECLK (EQPT)	TPTFAIL (POS)
FEPRLF (STMN)	MEA (EQPT)	UNPROT-SYNCCLK (NE)
FE-SF-SPAN (STMN)	MEA (PIM)	UNPROT-XCMTX (NE)
FORCED-REQ (VCMON-HP)	MEA (PPM)	UNQUAL-PPM (PPM)
FORCED-REQ-RING (STMN)	MEM-GONE (EQPT)	UNROUTEABLE-IP (NE)
FORCED-REQ-SPAN (STMN)	MEM-LOW (EQPT)	UPGRADE (NE)
FRCDSWTOINT (NE-SREF)	MFGMEM (CAP)	VOLT-MISM (PWR)
FRCDSWTOPRI (EXT-SREF)	MFGMEM (EQPT)	WKSWPR (STMN)

Table 2-6 ONS 15600 SDH Alarm and Condition Alphabetical List (continued)

FRCDSWTOPRI (NE-SREF)	MFGMEM (FAN)	WKSWPR (VCMON-HP)
FRCDSWTOSEC (EXT-SREF)	MFGMEM (PIM)	WTR (STMN)
FRCDSWTOSEC (NE-SREF)	MFGMEM (PPM)	WTR (VCMON-HP)
FRCDSWTOTHIRD (EXT-SREF)	MS-AIS (STMN)	WVL-OUT-OF-LOCK (STMN)
FRCDSWTOTHIRD (NE-SREF)	MS-DEG (STMN)	XCMTX (NE)
FREQ-MISMATCH (EQPT)	SSM-OFF (STMN)	—

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 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 building integrated timing supply (BITS) clock as well as other objects. Therefore, both STMN: LOS and BITS: 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

Type	Description
BITS	Building integrated timing supply incoming references (BITS-1, BITS-2).
BPLANE	The backplane.
CAP	Customer access panel (CAP).
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, high-order paths (HOPs), and low-order paths (LOPs).
EXT-SREF	BITS outgoing references (SYNC-BITS1, SYNC-BITS2).
FAN	Fan-tray assembly.
GIGE	Gigabit Ethernet.
NE	The entire network element.
NE-SREF	The timing status of the NE.
PIM	Pluggable input-output module (or 4PIO) for the ASAP card.
POS	Packet over SDH (virtual entity).

Table 2-7 Alarm Logical Object Type Definitions (continued)

PPM	Pluggable port module (PPM), or Small Form-factor Pluggable (SFP), for the ASAP card.
PWR	The node's power supply.
STMN	An STM-N line on an STM-N card.
VCMON-HP	High-order path virtual concatenation monitoring. **Note** The network element reports alarms or conditions on ingress ports of the card. Alarms detected at the internal ports (TERM side) will be ingress mapped to the MON side. The alarm profile entities of VCMON-HP, if available, should be changed to the same severity as the customized severity for a specific VCMON-HP alarm.

2.4 Alarm List by Logical Object Type

Table 2-8 lists all ONS 15600 SDH Software Release 8.0 alarms and logical objects as they are given in the system alarm profile. The list entries are organized logical object name and then by alarm or condition name. Each entry refers to an alarm description in this chapter. Where appropriate, the alarm entries also contain troubleshooting procedures.

Note In a mixed network containing different types of nodes (such as an ONS 15310-CL, ONS 15454 SDH, and ONS 15600 SDH), 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 ONS 15600 SDH Alarm List by Logical Object in Alarm Profile

BITS: AIS (NR)	NE-SREF: FRCDSWTOSEC (NA)	STMN: FE-FRCDWKSWPR-RING (NA)
BITS: BPV (MN)	NE-SREF: FRCDSWTOTHIRD (NA)	STMN: FE-FRCDWKSWPR-SPAN (NA)
BITS: LOF (MN)	NE-SREF: FRNGSYNC (NA)	STMN: FE-LOCKOUTOFPR-ALL (NA)
BITS: LOS (MN)	NE-SREF: HLDOVRSYNC (NA)	STMN: FE-LOCKOUTOFPR-SPAN (NA)
BITS: SSM-DUS (NA)	NE-SREF: MANSWTOINT (NA)	STMN: FE-MANWKSWBK-SPAN (NA)
BITS: SSM-FAIL (MN)	NE-SREF: MANSWTOPRI (NA)	STMN: FE-MANWKSWPR-RING (NA)
BITS: SSM-LNC (NA)	NE-SREF: MANSWTOSEC (NA)	STMN: FE-MANWKSWPR-SPAN (NA)
BITS: SSM-OFF (NA)	NE-SREF: MANSWTOTHIRD (NA)	STMN: FE-SF-SPAN (NA)
BITS: SSM-PRC (NA)	NE-SREF: SSM-LNC (NA)	STMN: FEPRLF (MN)
BITS: SSM-RES (NA)	NE-SREF: SSM-PRC (NA)	STMN: FORCED-REQ-RING (NA)
BITS: SSM-SDH-TN (NA)	NE-SREF: SSM-SDH-TN (NA)	STMN: FORCED-REQ-SPAN (NA)
BITS: SSM-SETS (NA)	NE-SREF: SSM-SETS (NA)	STMN: FULLPASSTHR-BI (NA)

Table 2-8 ONS 15600 SDH Alarm List by Logical Object in Alarm Profile (continued)

BITS: SSM-SMC (NA)	NE-SREF: SSM-SMC (NA)	STMN: HELLO (MN)
BITS: SSM-STU (NA)	NE-SREF: SSM-STU (NA)	STMN: HI-LASERBIAS (MN)
BITS: SYNC-FREQ (NA)	NE-SREF: SWTOPRI (NA)	STMN: HI-RXPOWER (MN)
BPLANE: INVMACADR (MJ)	NE-SREF: SWTOSEC (NA)	STMN: HI-TXPOWER (MN)
BPLANE: PWR-FA (MN)	NE-SREF: SWTOTHIRD (NA)	STMN: ISIS-ADJ-FAIL (MN)
CAP: EQPT (MN)	NE-SREF: SYNCPRI (MJ)	STMN: KB-PASSTHR (NA)
CAP: IMPROPRMVL (MN)	NE-SREF: SYNCSEC (MN)	STMN: KBYTE-APS-CHANNEL-FAILURE (MN)
CAP: MFGMEM (MN)	NE: AUD-LOG-LOSS (NA)	STMN: LKOUTPR-S (NA)
CAP: PWR-FAIL-A (MN)	NE: AUD-LOG-LOW (NA)	STMN: LO-LASERBIAS (MN)
CAP: PWR-FAIL-B (MN)	NE: DATAFLT (MN)	STMN: LO-RXPOWER (MN)
ENVALRM: EXT (MN)	NE: DBOSYNC (MJ)	STMN: LO-TXPOWER (MN)
EQPT: AUTORESET (MN)	NE: DUP-IPADDR (MN)	STMN: LOCKOUT-REQ (NA)
EQPT: BKUPMEMP (CR)	NE: DUP-NODENAME (MN)	STMN: LOCKOUT-REQ-RING (NA)
EQPT: CIDMISMATCH-A (MN)	NE: IMPR-XC (MN)	STMN: LOF (CR)
EQPT: CIDMISMATCH-B (MN)	NE: INTRUSION-PSWD (NA)	STMN: LOS (CR)
EQPT: CLKFAIL (MJ)	NE: SNTP-HOST (MN)	STMN: LPBKFACILITY (NA)
EQPT: CONTBUS-CLK-A (MN)	NE: SYNCCLK (CR)	STMN: LPBKPAYLOAD (NA)
EQPT: CONTBUS-CLK-B (MN)	NE: SYSBOOT (MJ)	STMN: LPBKTERMINAL (NA)
EQPT: CONTBUS-IO-A (MN)	NE: UNPROT-SYNCCLK (MN)	STMN: MANUAL-REQ-RING (NA)
EQPT: CONTBUS-IO-B (MN)	NE: UNPROT-XCMTX (MN)	STMN: MANUAL-REQ-SPAN (NA)
EQPT: CONTCOM (MN)	NE: UNROUTEABLE-IP (MN)	STMN: MS-AIS (NR)
EQPT: CTNEQPT-PB-A (CR)	NE: UPGRADE (NA)	STMN: MS-DEG (NA)
EQPT: CTNEQPT-PB-B (CR)	NE: XCMTX (CR)	STMN: MS-EOC (MN)
EQPT: CXCHALT (MJ)	PIM: EQPT (CR)	STMN: MS-EXC (NA)
EQPT: EQPT (CR)	PIM: EQPT-CC-PIM (CR)	STMN: MS-RFI (NR)
EQPT: EQPT-BOOT (CR)	PIM: IMPROPRMVL (CR)	STMN: MS-SQUELCH-HP (NA)
EQPT: EQPT-HITEMP (MN)	PIM: MANRESET (NA)	STMN: MSSP-SW-VER-MISM (MN)
EQPT: FREQ-MISMATCH (MN)	PIM: MEA (CR)	STMN: PRC-DUPID (MJ)
EQPT: FSTSYNC (NA)	PIM: MFGMEM (CR)	STMN: RING-MISMATCH (MJ)
EQPT: IMPROPRMVL (CR)	POS: ENCAP-MISMATCH-P (CR)	STMN: RING-SW-EAST (NA)
EQPT: LASER-BIAS (CR)	POS: GFP-LFD (MJ)	STMN: RING-SW-WEST (NA)
EQPT: LASER-OVER-TEMP (CR)	POS: GFP-UP-MISMATCH (MJ)	STMN: RS-EOC (MN)
EQPT: MANRESET (NA)	POS: TPTFAIL (MJ)	STMN: RS-TIM (CR)
EQPT: MATECLK (MN)	PPM: EQPT (CR)	STMN: SSM-DUS (NA)
EQPT: MEA (CR)	PPM: EQPT-PIM-PPM (CR)	STMN: SSM-FAIL (MN)
EQPT: MEM-GONE (MJ)	PPM: HI-LASERBIAS (MN)	STMN: SSM-LNC (NA)

Table 2-8 ONS 15600 SDH Alarm List by Logical Object in Alarm Profile (continued)

EQPT: MEM-LOW (MN)	PPM: HI-TXPOWER (MN)	STMN: SSM-OFF (NA)
EQPT: MFGMEM (CR)	PPM: IMPROPRMVL (CR)	STMN: SSM-PRC (NA)
EQPT: OPEN-SLOT (MN)	PPM: LASER-BIAS (CR)	STMN: SSM-SDH-TN (NA)
EQPT: PWR-FAIL-A (MN)	PPM: LASER-OVER-TEMP (CR)	STMN: SSM-SETS (NA)
EQPT: PWR-FAIL-B (MN)	PPM: LO-LASERBIAS (MN)	STMN: SSM-SMC (NA)
EQPT: PWR-FAIL-RET-A (MN)	PPM: LO-TXPOWER (MN)	STMN: SSM-STU (NA)
EQPT: PWR-FAIL-RET-B (MN)	PPM: MANRESET (NA)	STMN: SYNC-FREQ (NA)
EQPT: PWRRESTART (NA)	PPM: MEA (CR)	STMN: WKSWPR (NA)
EQPT: SFTWDOWN (MN)	PPM: MFGMEM (CR)	STMN: WTR (NA)
EQPT: SW-VER (NA)	PPM: NON-CISCO-PPM (NR)	STMN: WVL-OUT-OF-LOCK (MJ)
EXT-SREF: FRCDSWTOPRI (NA)	PPM: PROV-MISMATCH (MN)	VCMON-HP: AU-AIS (NR)
EXT-SREF: FRCDSWTOSEC (NA)	PPM: UNQUAL-PPM (NR)	VCMON-HP: AU-LOP (CR)
EXT-SREF: FRCDSWTOTHIRD (NA)	PWR: EHIBATVG (MJ)	VCMON-HP: AUTOSW-AIS-SNCP (NR)
EXT-SREF: MANSWTOPRI (NA)	PWR: ELWBATVG (MJ)	VCMON-HP: AUTOSW-LOP-SNCP (NA)
EXT-SREF: MANSWTOSEC (NA)	PWR: HIBATVG (MJ)	VCMON-HP: AUTOSW-SDBER-SNCP (NA)
EXT-SREF: MANSWTOTHIRD (NA)	PWR: LWBATVG (MJ)	VCMON-HP: AUTOSW-SFBER-SNCP (NA)
EXT-SREF: SWTOPRI (NA)	PWR: PWR (MJ)	VCMON-HP: AUTOSW-UNEQ-SNCP (NA)
EXT-SREF: SWTOSEC (NA)	PWR: VOLT-MISM (NA)	VCMON-HP: FAILTOSW-HO (NA)
EXT-SREF: SWTOTHIRD (NA)	STMN: ALS (NA)	VCMON-HP: FORCED-REQ (NA)
EXT-SREF: SYNCPRI (MN)	STMN: APSB (MN)	VCMON-HP: HP-DEG (NA)
EXT-SREF: SYNCSEC (MN)	STMN: APSC-IMP (MN)	VCMON-HP: HP-EXC (NA)
EXT-SREF: SYNCTHIRD (MN)	STMN: APSCDFLTK (MN)	VCMON-HP: HP-PLM (CR)
FAN: FAN-DEGRADE (MN)	STMN: APSCINCON (MN)	VCMON-HP: HP-RFI (NR)
FAN: FAN-FAIL (CR)	STMN: APSCM (MJ)	VCMON-HP: HP-TIM (MN)
FAN: FAN-FAIL-PARTIAL (MJ)	STMN: APSCNMIS (MJ)	VCMON-HP: HP-UNEQ (CR)
FAN: FAN-PWR (MN)	STMN: CHANLOSS (NA)	VCMON-HP: LOCKOUT-REQ (NA)
FAN: IMPROPRMVL (CR)	STMN: E-W-MISMATCH (MJ)	VCMON-HP: LPBKCRS (NA)
FAN: MFGMEM (CR)	STMN: EXERCISE-RING-FAIL (NA)	VCMON-HP: MAN-REQ (NA)
GIGE: CARLOSS (MJ)	STMN: EXTRA-TRAF-PREEMPT (MJ)	VCMON-HP: ROLL (NA)
GIGE: LPBKFACILITY (NA)	STMN: FAILTOSW (NA)	VCMON-HP: ROLL-PEND (NA)
GIGE: LPBKTERMINAL (NA)	STMN: FAILTOSWR (NA)	VCMON-HP: WKSWPR (NA)
NE-SREF: FRCDSWTOINT (NA)	STMN: FAILTOSWS (NA)	VCMON-HP: WTR (NA)
NE-SREF: FRCDSWTOPRI (NA)	STMN: FE-FRCDWKSWBK-SPAN (NA)	—

2.5 Trouble Notifications

The ONS 15600 SDH system reports trouble by utilizing standard alarm and condition characteristics, standard severities following the rules in Telcordia GR-253-CORE, and graphical user interface (GUI) state indicators. These notifications are described in the following paragraphs.

The ONS 15600 SDH uses standard Telcordia categories to characterize levels of trouble. The system reports trouble notifications as alarms and status or descriptive notifications (if configured to do so) as conditions in the CTC Alarms window. Alarms typically signify a problem that the user needs to remedy, such as a loss of signal. Conditions do not necessarily require troubleshooting.

2.5.1 Alarm Characteristics

The ONS 15600 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 15600 SDH shelf. They might include standing or transient notifications. A snapshot of all current raised, standing conditions on the network, node, or card can be retrieved in the CTC Conditions window or using TL1's set of RTRV-COND commands. (In addition, some but not all cleared conditions are also found in the History tab.)

For a comprehensive list of all conditions, refer to the *Cisco ONS SDH TL1 Command Guide*. For a comprehensive list of all transient conditions, see Chapter 3, “Transient Conditions.”

2.5.3 Severities

The ONS 15600 SDH uses Telcordia-devised standard severities for alarms and conditions:

- A Critical (CR) alarm generally indicates severe, Service-Affecting (SA) trouble that needs immediate correction.
- A Major (MJ) alarm is a serious alarm, but the trouble has less impact on the network.
- Minor (MN) alarms generally are those that do not affect service. For example, the automatic protection switching (APS) byte failure (APSB) alarm indicates that line terminating equipment (LTE) detects a byte failure on the signal that could prevent traffic from properly executing a traffic switch.
- Not Alarmed (NA) conditions are information indicators, such as for the free-running synchronization (FRNGSYNC) state. They might or might not require troubleshooting, as indicated in the entries.
- Not Reported (NR) conditions occur as a secondary result of another event. For example, the alarm indication signal (AIS), with severity NR, is inserted by a downstream node when an LOS (CR or MJ) alarm occurs upstream. These conditions do not in themselves require troubleshooting, but are to be expected in the presence of primary alarms.

Severities can be customized for an entire network or for single nodes, from the network level down to the port level by changing or downloading customized alarm profiles. These custom severities are subject to the standard severity-demoting rules given in Telcordia GR-474-CORE and shown in the 2.5.4 Alarm Hierarchy section. Procedures for customizing alarm severities are located in the "Manage Alarms" chapter in the *Cisco ONS 15600 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 15600 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 15600 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

Table 2-10 Facility Alarm Hierarchy

Priority	Condition Type
—	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

Service-Affecting (SA) alarms—those that interrupt service—might be Critical (CR) or Major (MJ) severity alarms. Service-Affecting (SA) alarms indicate service is affected.
Non-Service-Affecting (NSA) alarms always have a Minor (MN), Not Alarmed (NA), or Not Reported (NR) severity.

2.5.6 States

The Alarms and History tab State (ST) columns indicate the disposition of alarms and conditions as follows:

- A raised (R) event is one that is active.
- A cleared (C) event is one that is no longer active.
- A transient (T) event is one that is automatically raised and cleared in CTC during system changes such as user login, logout, loss of connection to node view, etc. Transient events do not require user action. These are listed in Chapter 3, “Transient Conditions.”

2.5.7 Safety Summary

This section covers safety considerations to ensure safe operation of the ONS 15600 SDH system. Personnel should not perform any procedures in this manual unless they understand all safety precautions, practices, and warnings for the system equipment. Some troubleshooting procedures require installation or removal of cards. In these instances, users should pay close attention to the following caution:

⚠ **Caution** Hazardous voltage or energy might 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 optical cards. In these instances, users should pay close attention to the following warnings:

⚠ **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 may result in hazardous radiation exposure.** Statement 1057

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

Warning **Do not reach into a vacant slot or chassis while you install or remove a module or a fan. Exposed circuitry could constitute an energy hazard.** Statement 206

Warning **The power supply circuitry for the equipment can constitute an energy hazard. Before you install or replace the equipment, remove all jewelry (including rings, necklaces, and watches). Metal objects can come into contact with exposed power supply wiring or circuitry inside the DSLAM equipment. This could cause the metal objects to heat up and cause serious burns or weld the metal object to the equipment.** Statement 207

2.6 Alarm Procedures

This section lists alarms alphabetically and includes some conditions commonly encountered when troubleshooting alarms. The severities, descriptions, and troubleshooting procedures accompany alarms and conditions.

Note When an entity is put in the Out of Service and Maintenance (Locked,maintenance) administrative state, the ONS 15600 SDH suppresses all standing alarms on that entity. All alarms and events appear on the Conditions tab. You can change this behavior for the LPBKFACILITY, LPBKPAYLD, and LPBKTERMINAL alarms. To display these alarms on the Alarms tab, set the NODE.general.ReportLoopbackConditionsOnPortsInOOS-MT to TRUE on the NE Defaults tab.

2.6.1 AIS

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

Logical Object: BITS

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 the node sees the AIS instead of a real signal. In most cases when this condition is raised, an upstream node is raising an alarm to indicate a signal failure; all nodes downstream from it only raise some type of AIS. This condition clears when you resolved the problem on the upstream node.

Clear the AIS Condition

Step 1 Determine whether there are alarms on the upstream nodes and equipment, especially the "LOS (STMN)" alarm on page 2-84 or if there are out-of-service (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 call Cisco TAC (1-800-553-2447).

2.6.2 ALS

For information about this condition, refer to the "Alarm Troubleshooting" chapter of the *Cisco ONS 15454 DWDM Troubleshooting Guide*.

2.6.3 APSB

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

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 scheme with newer SDH nodes, such as the ONS 15600 SDH. These invalid codes cause an APSB alarm on an ONS 15600 SDH.

Note APS switches are hitless on the ONS 15600 SDH.

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 15600 SDH.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15600 SDH. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 2 If the alarm does not clear and the overhead shows inconsistent or invalid K bytes, you might need to replace the upstream cards for protection switching to operate properly. Complete the "Replace an I/O Card" procedure on page 2-133.

Caution For the ONS 15600 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 "2.8.5 Verify or Create Node DCC Terminations" section on page 2-138 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 the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.4 APSCDFLTK

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

Logical Object: STMN

The APS Default K Byte Received alarm occurs when a bidirectional line switched ring (MS-SPRing) is not properly configured—for example, when a four-node MS-SPRing has one node configured as a unidirectional path switched ring (SNCP). When this misconfiguration occurs, a node in an SNCP 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.

Clear the APSCDFLTK Alarm

Step 1 Complete the "Identify an MS-SPRing Ring ID or Node ID Number" procedure on page 2-120 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 2-121 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 "E-W-MISMATCH" alarm on page 2-48.) 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 15600 SDH Procedure Guide* contains procedures for fibering an MS-SPRing.

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 2-121.

Step 7 If nodes are not visible, complete the "2.8.5 Verify or Create Node DCC Terminations" procedure on page 2-138 to ensure that SDH data communication channel (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 call Cisco TAC (1-800-553-2447).

2.6.5 APSC-IMP

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

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.

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 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 may 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 15600 SDH. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

If the K byte is invalid, the problem lies with upstream equipment and not with the reporting ONS 15600 SDH. Troubleshoot the upstream equipment using the procedures in this chapter, as applicable. If the upstream nodes are not ONS 15600 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 ID or Node ID Number" procedure on page 2-120.

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 ID Number" procedure on page 2-121.

Step 5 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.6 APSCINCON

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

Logical Object: STMN

An APS Inconsistent alarm means that an inconsistent APS byte is present in the SDH overhead. The SDH overhead contains K1/K2 APS bytes that notify receiving equipment, such as the ONS 15600 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

Step 1 Look for other alarms, especially the "LOS (STMN)" alarm on page 2-84, the "LOF (STMN)" alarm on page 2-81, or the "AIS" condition on page 2-15. Clearing these alarms clears the APSCINCON alarm.

Step 2 If an APSINCON alarm occurs with no other alarms, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.7 APSCM

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

Logical Object: STMN

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

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 may result in hazardous radiation exposure.** Statement 1057

Note APS switches are hitless in the ONS 15600 SDH.

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 15600 SDH. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 2 If the fibers are correctly connected, 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 call Cisco TAC (1-800-553-2447) to report a Service-Affecting (SA) problem.

2.6.8 APSCNMIS

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

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. The APSCNMIS alarm could occur and clear when a MS-SPRing is being provisioned. If so, you can disregard the temporary occurrence. If the APSCNMIS remains, 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 ID or Node ID Number" procedure on page 2-120 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 2-121 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 Lock Out on a MS-SPRing Protect Span" procedure on page 2-127 to lock out the span.

Step 6 Complete the "Clear a MS-SPRing External Switching Command" procedure on page 2-128 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 call Cisco TAC (1-800-553-2447) to report a Service-Affecting (SA) problem.

2.6.9 AU-AIS

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

Logical Objects: VCMON-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 2-15.

Step 2 If the condition does not clear, complete the "Clear the APSB Alarm" procedure on page 2-16.

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.

2.6.10 AUD-LOG-LOSS

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

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. The log must be off-loaded using the following procedure 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 have to assign an extension to the file. It 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 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).

2.6.11 AUD-LOG-LOW

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

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. It does not require troubleshooting.

2.6.12 AU-LOP

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

Logical Objects: VCMON-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.

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

Warning **Use of controls, adjustments, or performing procedures other than those specified could result in hazardous radiation exposure.** Statement 1057

Clear the AU-LOP Alarm

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. Delete the circuit.

Step 5 Recreate the circuit for the correct size. For procedures, refer to the "Create Circuits" chapter in the *Cisco ONS 15600 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.

2.6.13 AUTORESET

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

Logical Object: EQPT

The Automatic System Reset alarm occurs when you change an IP address or perform any other operation that causes an automatic card-level reboot. Resets performed during a software upgrade also prompt the alarm. This condition clears automatically when the card finishes resetting.

Note If an optical card associated with an active port in a 1+1 protection group resets, all DCC traffic terminated or tunneled on the active port is lost while the card resets. No DCC traffic is lost during a reset of an optical card associated with a standby port.

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 "Replace an I/O Card" procedure on page 2-133. If the lack of communication continues, the AUTORESET alarm is cleared and the 2.6.47 EQPT-BOOT alarm occurs. In this case, no AUTORESET troubleshooting is required.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15600 SDH. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Caution For the ONS 15600 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 "2.8.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-121 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 call Cisco TAC (1-800-553-2447).

2.6.14 AUTOSW-AIS-SNCP

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

Logical Object: VCMON-HP

The Automatic SNCP Switch Caused by an AIS condition indicates that automatic SNCP protection switching occurred because of an "AU-AIS" alarm on page 2-21 condition. If the SNCP is configured for revertive switching, it reverts to the working path after the fault clears. The AU-AIS also clears when the upstream trouble is cleared.

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

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 resolve the problem on the upstream node.

Clear the AUTOSW-AIS-SNCP Condition

Step 1 Complete the "Clear the AU-AIS Condition" procedure on page 2-21.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.15 AUTOSW-LOP-SNCP

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

Logical Object: VCMON-HP

The Automatic SNCP Switch Caused by LOP condition indicates that automatic SNCP protection switching occurred because of the "AU-LOP" alarm on page 2-22. If the SNCP is configured for revertive switching, it reverts to the working path after the fault clears.

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

Clear the AUTOSW-LOP-SNCP Condition

Step 1 Complete the "Clear the AU-LOP Alarm" procedure on page 2-22.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.16 AUTOSW-SDBER-SNCP

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

Logical Object: VCMON-HP

The Automatic SNCP Switch Caused by Signal Degrade Bit Error Rate (SDBER) condition indicates that a "MS-DEG" condition on page 2-96 caused automatic SNCP protection switching to occur. If the SNCP is configured for revertive switching, the SNCP reverts to the working path when the MS-DEG is resolved.

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

Clear the AUTOSW-SDBER-SNCP Condition

Step 1 Complete the "Clear the MS-DEG Condition" procedure on page 2-97. (The clearing procedure is the same for all signal degrade and signal fail 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 call Cisco TAC (1-800-553-2447).

2.6.17 AUTOSW-SFBER-SNCP

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

Logical Object: VCMON-HP

The Automatic USPR Switch Caused by Signal Fail Bit Error Rate (SFBER) condition indicates that a "MS-EXC" condition on page 2-97 caused automatic SNCP protection switching to occur. If the SNCP is configured for revertive switching, the SNCP reverts to the working path when the MS-EXC is resolved.

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

Clear the AUTOSW-SFBER-SNCP Condition

Step 1 Complete the "Clear the MS-EXC Condition" procedure on page 2-97. (The clearing procedure is the same for all signal degrade and signal fail 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 call Cisco TAC (1-800-553-2447).

2.6.18 AUTOSW-UNEQ-SNCP

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

Logical Object: VCMON-HP

The Automatic SNCP Switch Caused by Unequipped Circuit condition indicates that an "HP-UNEQ" condition on page 2-69 alarm caused automatic SNCP protection switching to occur. If the SNCP is configured for revertive switching, it reverts to the working path after the fault clears.

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

Clear the AUTOSW-UNEQ-SNCP Condition

Step 1 Complete the "Clear the HP-UNEQ Alarm" procedure on page 2-69.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.19 BKUPMEMP

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

Logical Object: EQPT

The Primary Non-Volatile Backup Memory Failure alarm refers to a problem with the TSC card flash memory. The alarm occurs when the controller card is in use and has one of four problems:

- Flash manager fails to format a flash partition.
- Flash manager fails to write a file to a flash partition.
- Problem at the driver level.
- Code volume fails cyclic redundancy checking (CRC, a method to verify for errors in data transmitted to the TSC card).

The BKUPMEMP alarm can also cause the "EQPT (EQPT)" alarm on page 2-44. If the EQPT alarm is caused by BKUPMEMP, complete the following procedure to clear the BKUPMEMP and the EQPT alarm.

Caution It can take up to 30 minutes for software to be updated on a standby TSC card.

Clear the BKUPMEMP Alarm

Step 1 Verify that both TSC cards are powered and enabled by confirming lighted SRV LEDs on the TSC cards.

Step 2 Determine whether the active or standby TSC card that has the alarm.

Step 3 If both TSC cards are powered and enabled, reset the TSC card against which the alarm is raised. Complete the "Soft-Reset a Card Using CTC" procedure on page 2-129.

Wait ten minutes to verify that the card you reset completely reboots.

Step 4 If the TSC card you reset does not reboot successfully, or the alarm has not cleared, call Cisco TAC (1-800-553-2447). If the Cisco TAC technician tells you to reseat the card, complete the "Reset a Card with a Card Pull (Reseat)" procedure on page 2-131. If the Cisco TAC technician tells you to remove the card and reinstall a new one, follow the "Replace a TSC Card" procedure on page 2-134.

2.6.20 BPV

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

Logical Object: BITS

The Bipolar Violation alarm is generated when bipolar violation does not satisfy the requirements described in ITU-T recommendations.

Clear the BPV Alarm

Step 1 Check if the input signal is correct and that the externally synchronized node is correctly provisioned with the 64KHz signal.

Step 2 If the type of signal is correct then check if all two wires are firmly connected to the BITS-IN pins.

Step 3 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) in order to report a Service-Affecting (SA) problem.

2.6.21 CARLOSS

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

Logical Object: GIGE

The Carrier Loss for Gigabit Ethernet (GE) alarm occurs on ASAP ports supporting Gigabit Ethernet traffic. The loss can be due to a misconfiguration, fiber cut, or client equipment problem.

Clear the CARLOSS Alarm

Step 1 Ensure that the GIGE client is correctly configured by completing the following steps:

a. Double-click the ASAP card to display the card view.

b. Click the **Provisioning > Pluggable Port Modules** tabs.

c. View the Pluggable Port Modules area port listing in the **Actual Equipment Type** column and compare this with the client equipment. If no SFP (referred to as a PPM in CTC) is provisioned, refer to the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15600 SDH Procedure Guide* for provisioning instructions.

d. If an SFP (PPM) has been created, view the contents of the Selected PPM area **Rate** column for the port and compare this rate with the client equipment data rate. In this case, the rate should be ETHER. If the SFP (PPM) rate is differently provisioned, select the SFP (PPM), click **Delete**, then click **Create** and choose the correct rate for the equipment type.

Step 2 If there is no SFP (PPM) misprovisioning, check for a fiber cut.

Step 3 If there is no fiber cut or provisioning error, check the client-side equipment for any transmission errors on the line.

Step 4 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) in order to report a Service-Affecting (SA) problem.

2.6.22 CHANLOSS

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

Logical Object: STMN

The SDH Section Layer DCC Termination Failure condition occurs when the ONS 15600 SDH receives unrecognized data in the section layer DCC bytes.

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

Warning **Use of controls, adjustments, or performing procedures other than those specified may result in hazardous radiation exposure.** Statement 1057

Clear the CHANLOSS Condition

Step 1 In the absence of other alarms, determine whether the alarmed port is connected to another vendor's equipment. If so, you can mask the alarm on this path using a custom alarm profile. For more information about custom profiles, refer to the "Manage Alarms" chapter in the *Cisco ONS 15600 SDH Procedure Guide*.

Step 2 If alternate vendor equipment is not the cause of the alarm, complete the "Soft-Reset a Card Using CTC" procedure on page 2-129 for the traffic card.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15600 SDH. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 3 If the alarm does not clear, complete the "Replace an I/O Card" procedure on page 2-133.

Step 4 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.23 CIDMISMATCH-A

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

Logical Object: EQPT

A Connection ID Mismatch on SSXC A (in Slot 6) alarm occurs when at least one internal connection ID mismatch is present at the VC3 level on the traffic (STM-N) card outbound data path. The alarm occurs when the head end of the connection between traffic cards is removed.

Note This alarm can occur on a VT tunnel if it does not have VT circuits provisioned on it.

Note When an alarm includes a numeric or alphabetical designation, it indicates whether the alarm applies to the first or second card of a specific type on the shelf. A zero or A indicates that the alarm occurs against the first card of its type, from left to right, in the shelf. A one or B indicates that the alarm occurs against the second card of its type in the shelf.

Clear the CIDMISMATCH-A Alarm

Step 1 Depending on how many CIDMISMATCH alarms are raised, take one of the following actions:

- If two CIDMISMATCH alarms (CIDMISMATCH-A and the"CIDMISMATCH-B" alarm on page 2-30) are present, continue with Step 6.
- One CIDMISMATCH-x alarm indicates trouble related to one SSXC card. If an automatic switch to the alternate copy SSXC card occurred, the alarmed SSXC card can be serviced. If traffic has not switched, complete the "Request a Cross-Connect Card Preferred Copy Switch" procedure on page 2-130.

  To determine which SSXC card is the preferred copy and if it is currently being used, in node view click the **Maintenance > Preferred Copy** tabs. The Data Copy area Preferred field shows Copy A or Copy B. The Currently Used field shows the copy being used.

Note In CTC, Copy A refers to the SSXC card in Slot 6. Copy B refers to the SSXC card in Slot 8. Either copy can be chosen as the preferred copy SSXC card. The other SSXC card is called the alternate SSXC card in this chapter.

Step 2 Complete the "Soft-Reset a Card Using CTC" procedure on page 2-129 for the alarmed SSXC card.

Step 3 If the alarm does not clear, ensure that an automatic protection switch has moved traffic to the protect port. If an APS switch occurred, continue with Step 4.

- A SNCP APS is identified by an AUTOSW-type alarm or condition (such as AUTOSW-AIS, AUTOSW-LOP, AUTOSW-PDI, AUTOSW-SDBER, AUTOSW-SFBER, or AUTOSW-UNEQ).
- A 1+1 APS is identified in the node view Maintenance > Protection tab. If you click the protection group, under the Selected Group list, the ports are designated as Working/Standby and Protect/Active.

If the reporting traffic card has 1+1 active ports and traffic has not switched to the protect ports, complete the "Initiate a 1+1 Protection Port Force Switch Command" procedure on page 2-122.

Step 4 Complete the "Reset a Card with a Card Pull (Reseat)" procedure on page 2-131 for the SSXC card.

Step 5 If the alarm does not clear, complete the "Replace an SSXC Card" procedure on page 2-132, "Replace an I/O Card" procedure on page 2-133, or "Replace a TSC Card" procedure on page 2-134 as appropriate for the reporting card.

Step 6 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

Step 7 When the alarm clears, if an automatic switch to the alternate copy SSXC card occurred, traffic is restored to the preferred copy.

If the reporting card is a traffic card, traffic reverts to the working port if an automatic switch occurred. If traffic was manually switched in a 1+1 protection group, revert traffic to the original port by completing the "Clear a 1+1 Protection Port Force or Manual Switch Command" procedure on page 2-123. If traffic was manually switched in an SNCP, revert traffic to the original path by completing the "Clear a SNCP Span External Switching Command" procedure on page 2-126.

2.6.24 CIDMISMATCH-B

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

Logical Object: EQPT

A Connection ID Mismatch on SSXC-B (Slot 8) alarm occurs when at least one internal connection ID mismatch is present at the VC3 level on the STM-16 or STM-64 card outbound data path. The alarm occurs when the head end of the connection between traffic (STM-N) cards is removed.

Note This alarm can occur on a VT tunnel if it does not have VT circuits provisioned on it.

Clear the CIDMISMATCH-B Alarm

Step 1 Complete the "Clear the CIDMISMATCH-A Alarm" procedure on page 2-29.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.25 CLKFAIL

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

Logical Object: EQPT

The Clock Fail alarm occurs when an internal clock module fails. If this alarm occurs against the standby TSC card, the card must be replaced. If the alarm occurs against the active TSC card, the card automatically becomes standby because the traffic and SSXC cards can only take timing from the active TSC card.

Clear the CLKFAIL Alarm

Step 1 Complete the "Replace a TSC Card" procedure on page 2-134 for the reporting TSC card.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15600 SDH. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Note When there are different versions of system software on the two TSC cards, it takes approximately 20 minutes for the active TSC card to transfer the system software to the newly installed standby TSC card. When the transfer completes, the TSC card reboots and goes into standby mode after approximately three minutes.

Note If the active and standby TSC cards have the same versions of software, it takes approximately three minutes for software to be updated on a standby TSC card.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.26 CONTBUS-CLK-A

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

Logical Object: EQPT

An Inbound Interconnection Timing Control Bus 0 Failure alarm on the Slot 10 TSC card occurs if the timing signal from the Slot 5 TSC card has an error. If the Slot 10 TSC card and all other cards on the shelf raise this alarm, the alarm processor on the Slot 5 TSC card clears the alarm on the other cards and raises this alarm against the Slot 5 TSC card only.

Clear the CONTBUS-CLK-A Alarm

Step 1 If a single traffic card is reporting the alarm and it is part of an SNCP, complete the "Initiate a Force Switch for All Circuits on a SNCP Span" procedure on page 2-124. If the traffic card is part of a 1+1 protection group, complete the "Initiate a 1+1 Protection Port Force Switch Command" procedure on page 2-122.

Note If the reporting card is an SSXC card, traffic should have already switched from the errored copy of the card.

Note If the active TSC is reporting the alarm, shelf control should already have switched off the card.

Step 2 Complete the appropriate procedure in the "2.8.4 Physical Card Reseating, Resetting, and Replacement" section on page 2-131 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 call Cisco TAC (1-800-553-2447).

When the alarm clears, if an automatic switch to the alternate copy SSXC occurred, traffic is automatically restored to the preferred copy.

Step 4 If traffic was manually switched in a 1+1 protection group, revert traffic to the original port by completing the "Clear a 1+1 Protection Port Force or Manual Switch Command" procedure on page 2-123. If traffic was manually switched in an SNCP, revert traffic to the original path by completing the "Clear a SNCP Span External Switching Command" procedure on page 2-126.

Step 5 When the alarm has been cleared, if desired, complete the "Soft-Reset a Card Using CTC" procedure on page 2-129.

2.6.27 CONTBUS-CLK-B

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

Logical Object: EQPT

An Inbound Interconnection Timing Control Bus 1 Failure alarm on the Slot 5 TSC card occurs if the timing signal from the Slot 10 TSC card has an error. If the Slot 5 TSC card and all other cards on the shelf raise the alarm, the processor on the Slot 10 TSC card clears the alarm on the other cards and raises this alarm against the Slot 10 TSC card only.

Note When an alarm includes a numeric or alphabetical designation, it indicates whether the alarm applies to the first or second card of a specific type on the shelf. A zero or A indicates that the alarm occurs against the first card of its type, from left to right, in the shelf. A one or B indicates that the alarm occurs against the second card of its type in the shelf.

Clear the CONTBUS-CLK-B Alarm

Step 1 Complete the "Clear the CONTBUS-CLK-A Alarm" procedure on page 2-32.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.28 CONTBUS-IO-A

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

Logical Object: EQPT

A TSC Card A to Shelf A Slot Communication Failure alarm occurs when the active Slot 5 TSC card (TSC card 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 15600 SDH switches to the standby TSC card. In the case of a TSC card protection switch, the alarm clears after the other cards establish communication with the newly active TSC card. If the alarm persists, the problem lies with the physical path of communication from the TSC card to the reporting card. The physical path of communication includes the TSC 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 display the provisioned type.

If the actual card type and the provisioned card type do not match, see the "MEA" alarm on page 2-92 for the reporting card.

Step 2 Complete the "Soft-Reset a Card Using CTC" procedure on page 2-129 for the alarmed card. For the LED behavior, see the "2.7 LED Behavior" section on page 2-118.

Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card. (A reset standby card remains standby.)

Step 3 If CONTBUS-IO-A is raised on several cards at the same time, complete the "Reset a Card with a Card Pull (Reseat)" procedure on page 2-131.

Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card.

Step 4 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. A green SRV LED indicates an active card.

Step 5 If the CTC reset does not clear the alarm, complete the "Reset a Card with a Card Pull (Reseat)" procedure on page 2-131 for the reporting card.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15600 SDH. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 6 If the reset card has not rebooted successfully, or the alarm has not cleared, call Cisco TAC (1-800-553-2447). If the Cisco TAC technician tells you to reseat the card, complete the "Reset a Card with a Card Pull (Reseat)" procedure on page 2-131. If the Cisco TAC technician tells you to remove the card and reinstall a new one, follow the "Replace a TSC Card" procedure on page 2-134.

2.6.29 CONTBUS-IO-B

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

Logical Object: EQPT

A TSC Card B to Shelf Communication Failure alarm occurs when the active Slot 10 TSC card (TSC card 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 might appear briefly when the ONS 15600 SDH switches to the protect TSC card. In the case of a TSC card protection switch, the alarm clears after the other cards establish communication with the newly active TSC card. If the alarm persists, the problem lies with the physical path of communication from the TSC card to the reporting card. The physical path of communication includes the TSC 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 display the provisioned type.

If the actual card type and the provisioned card type do not match, see the "MEA" alarm on page 2-92 for the reporting card.

Step 2 Complete the "Soft-Reset a Card Using CTC" procedure on page 2-129 for the alarmed card. For the LED behavior, see the "2.7 LED Behavior" section on page 2-118.

Step 3 If the alarm object is the standby Slot 5 TSC card, complete the "Reset a Card with a Card Pull (Reseat)" procedure on page 2-131.

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 the same time, complete the "Soft-Reset a Card Using CTC" procedure on page 2-129.

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 SRV LED indicates an active card.

Step 6 If the CTC reset does not clear the alarm, complete the "Reset a Card with a Card Pull (Reseat)" procedure on page 2-131 for the reporting card.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15600 SDH. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 7 If the reset card has not rebooted successfully, or the alarm has not cleared, call Cisco TAC (1-800-553-2447). If the Cisco TAC technician tells you to reseat the card, complete the "Reset a Card with a Card Pull (Reseat)" procedure on page 2-131. If the Cisco TAC technician tells you to remove the card and reinstall a new one, follow the "Replace a TSC Card" procedure on page 2-134.

2.6.30 CONTCOM

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

Logical Object: EQPT

The Interconnection Control Communication Failure alarm occurs when the internal messaging processor on the reporting active TSC card fails.

A TSC card should boot and be in the ready state within approximately five minutes. If the CONTCOM alarm clears within this time frame and the TSC card goes to standby or active mode as applicable, no action is necessary.

If the communication equipment on the backplane fails, a CONTBUS alarm occurs instead of a CONTCOM alarm.

Clear the CONTCOM Alarm

Step 1 Complete the "Soft-Reset a Card Using CTC" procedure on page 2-129.

Step 2 If the CTC reset does not clear the alarm, complete the "Reset a Card with a Card Pull (Reseat)" procedure on page 2-131.

Step 3 If the alarm does not clear, complete the "Replace a TSC Card" procedure on page 2-134.

Step 4 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

Step 5 When the alarm has been cleared, complete the "Soft-Reset a Card Using CTC" procedure on page 2-129 as needed.

2.6.31 CTNEQPT-PB-A

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

Logical Object: EQPT

The SSXC-0 Data Payload Bus Interconnect Failure alarm occurs when the data path interconnection between equipment from SSXC-0 (Slot 6) to inbound or outbound traffic (STM-N) card slots has a failure. The SSXC card and the reporting card are no longer communicating through the backplane. The problem exists in the SSXC card, the reporting traffic card, or the backplane. If more than one traffic card on the shelf raises this alarm, the TSC card clears this alarm on the traffic cards and raises it alarm against SSXC-0.

Note When an alarm includes a numeric or alphabetical designation, it indicates whether the alarm applies to the first or second card of a specific type on the shelf. A zero or A indicates that the alarm occurs against the first card of its type, from left to right, in the shelf. A one or B indicates that the alarm occurs against the second card of its type in the shelf.

Note If you insert a new TSC card that has the same version of software as the active and standby TSC card, it takes approximately three minutes for the standby TSC card to become available.

Note It takes approximately 20 minutes for the active TSC card to transfer the system software to the newly installed TSC card. Software transfer occurs in instances where different software versions exist on the two cards. When the transfer completes, the TSC card reboots and goes into standby mode after approximately three minutes.

Clear the CTNEQPT-PB-A Alarm

Step 1 If the alarm occurs against a single traffic (STM-N) card, continue with Step 2. If the alarm occurs against multiple traffic cards, it indicates a problem with the SSXC card. Continue with Step 6.

Step 2 If the traffic card ports are part of an SNCP, switch the single circuit on the span using instructions in the "Maintain the Node" chapter in the *Cisco ONS 15600 SDH Procedure Guide*. If the ports are part of a 1+1 protection group, complete the "Initiate a 1+1 Protection Port Force Switch Command" procedure on page 2-122.

Step 3 Complete the "Hard-Reset a Card Using CTC" procedure on page 2-129.

Step 4 If the CTC reset does not clear the alarm, complete the "Reset a Card with a Card Pull (Reseat)" procedure on page 2-131 for the reporting card.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15600 SDH. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 5 If the alarm does not clear, complete the appropriate procedure in the "2.8.4 Physical Card Reseating, Resetting, and Replacement" section on page 2-131.

Note If the traffic card is implicated and you are able to continue using the traffic card with one port out of service, perform a bridge and roll to move the port traffic to a free port. Refer to the "Manage Circuits" chapter in the *Cisco ONS 15600 SDH Procedure Guide* for instructions. Label the bad port and take it out of service until the card can be replaced.

Step 6 If you replace the traffic card and the alarm does not clear, an SSXC card problem is indicated. If an automatic switch to the alternate copy SSXC card occurred, the SSXC card can be serviced. If traffic has not switched, request a preferred copy switch by completing the "Request a Cross-Connect Card Preferred Copy Switch" procedure on page 2-130.

To determine which SSXC card is the preferred copy and whether it is currently being used, in node view go to the Maintenance > Preferred Copy window. The Data Copy area Preferred field shows Copy A or Copy B. The Currently Used field shows the copy being used.

Note In CTC, Copy A refers to the SSXC card in Slot 6. Copy B refers to the SSXC card in Slot 8. Either copy might be chosen as the preferred copy SSXC card. The other SSXC card is called the alternate SSXC card in this chapter.

Continue with Step 7.

Step 7 Perform a CTC soft reset on the SSXC card by completing the following steps:

a. Display node view.

b. Position the CTC cursor over the card.

c. Right-click and choose **Soft-reset Card** from the shortcut menu.

d. Click **Yes** in the Soft-reset Card dialog box.

Step 8 If the CTC reset does not clear the alarm, complete the "Reset a Card with a Card Pull (Reseat)" procedure on page 2-131 for the alarmed card.

Step 9 If the alarm does not clear, complete the "Replace an SSXC Card" procedure on page 2-132.

Step 10 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) to report a Service-Affecting (SA) problem.

Step 11 Depending on which card raised the alarm, perform the following actions:

- If traffic was manually switched in a 1+1 protection group, revert traffic to the original port by completing the "Clear a 1+1 Protection Port Force or Manual Switch Command" procedure on page 2-123.
- If traffic was manually switched in an SNCP, revert traffic to the original path by completing the "Clear a SNCP Span External Switching Command" procedure on page 2-126.

Note If an automatic switch to the alternate copy SSXC card occurred, traffic is automatically restored to the preferred copy.

2.6.32 CTNEQPT-PB-B

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

Logical Object: EQPT

The SSXC-1 Data Payload Bus Interconnect Failure alarm occurs when the data path interconnection fails between equipment from SSXC-1 (Slot 8) and traffic card slots. If more than one traffic card on the shelf raises this alarm, the TSC card clears the alarm on the traffic cards and raises the alarm against the SSXC-1.

Note In CTC, Copy A refers to the SSXC card in Slot 6/7. Copy B refers to the SSXC card in Slot 8/9. Either copy might be chosen as the preferred copy SSXC card. The other SSXC card is called the alternate SSXC card in this chapter.

Clear the CTNEQPT-PB-B Alarm

Step 1 Complete the "Clear the CTNEQPT-PB-A Alarm" procedure on page 2-36.

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.

2.6.33 CXCHALT

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

Logical Object: EQPT

An SSXC Operation Suspended alarm indicates that operation on the alternate SSXC card has halted because of problems in Fan Tray 2, which services controller cards including the SSXC cards.

The CXCHALT alarm occurs five minutes after a fan failure alarm such as the "FAN-DEGRADE" alarm on page 2-56, the "FAN-FAIL" alarm on page 2-56, the "IMPROPRMVL (EQPT, PIM, PPM)" alarm on page 2-71, or the "FAN-FAIL-PARTIAL" alarm on page 2-57 halts alternate SSXC operation.

Caution If a CXCHALT occurs due to a fan failure, you should move a working fan assembly from Tray 1 or 3 and install it in the Tray 2 position because the remaining working SSXC card can be damaged in as little as 15 minutes. If damage occurs to the remaining SSXC card, it restarts and then fails. Traffic is dropped until a replacement is installed.

Clear the CXCHALT Alarm

Step 1 Troubleshoot the fan alarm by following the "Clear the FAN-FAIL Alarm" procedure on page 2-57, which includes fan replacement.

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.

2.6.34 DATAFLT

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

Logical Object: NE

The Software Data Integrity Fault alarm occurs when the TSC exceeds its flash memory capacity.

Caution Configurations more than three minutes old are saved. Those newer than three minutes are not saved.

Clear the DATAFLT Alarm

Step 1 Complete the "Soft-Reset a Card Using CTC" procedure on page 2-129.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.35 DBOSYNC

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

Logical Object: NE

The Standby Database Out of Synchronization alarm occurs when the standby TSC card "To be Active" database does not synchronize with the active database on the active TSC card.

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

Clear the DBOSYNC Alarm

Step 1 Save a backup copy of the active TSC card database. Refer to the "Maintain the Node" chapter in the *Cisco ONS 15600 SDH Procedure Guide* for instructions.

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 call Cisco TAC (1-800-553-2447).

2.6.36 DISCONNECTED

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

Logical Object: SYSTEM

The Disconnected is raised when CTC has been disconnected from the node. The alarm is cleared when CTC is reconnected to the node.

Clear the DISCONNECTED Alarm

Step 1 Restart the CTC application.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.37 DUP-IPADDR

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

Logical Object: NE

The Duplicate IP Address alarm indicates that the alarmed node IP address is already in use within the same 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 15600 SDH chassis.
- **b.** Begin a CTC session.
- **c.** In the login dialog box, uncheck the **Network Discovery** check box.

Step 2 In node view, click the **Provisioning > Network > General** tabs.

Step 3 In the IP Address field, change the IP address to a unique number.

Step 4 Click **Apply**.

Step 5 Restart any CTC sessions that are logged into either of the formerly duplicated node IDs. (For instructions to log in or log out, refer to the "Set Up PC and Log Into the GUI" chapter in the *Cisco ONS 15600 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 call Cisco TAC (1-800-553-2447).

2.6.38 DUP-NODENAME

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

Logical Object: NE

The Duplicate Node Name alarm indicates that the alarmed node alphanumeric name is already being used within the same DCC area.

Clear the DUP-NODENAME Alarm

Step 1 In node view, click the **Provisioning > General > General** tabs.

Step 2 In the Node Name field, enter a unique name for the node.

Step 3 Click **Apply**.

Step 4 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.39 EHIBATVG

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

Logical Object: PWR

The Extreme High Voltage Battery alarm occurs in a –48 VDC environment when a battery lead input voltage exceeds the extreme high power threshold. This threshold, with a default value of –56.5 VDC, is user-provisionable. The alarm remains raised until the voltage remains under the threshold for 120 seconds.

Clear the EHIBATVG Alarm

Step 1 The problem is external to the ONS 15600 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 call Cisco TAC (1-800-553-2447) in order to report a Service-Affecting (SA) problem.

2.6.40 ELWBATVG

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

Logical Object: PWR

The Extreme Low Voltage Battery alarm occurs in a –48 VDC environment when a battery lead input voltage falls below the extreme low power threshold. This threshold, with a default value of –40.5 VDC, is user-provisionable. The alarm remains raised until the voltage remains over the threshold for 120 seconds.

Clear the ELWBATVG Alarm

Step 1 The problem is external to the ONS 15600 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 call Cisco TAC (1-800-553-2447) in order to report a Service-Affecting (SA) problem.

2.6.41 ENCAP-MISMATCH-P

The ENCAP-MISMATCH-P alarm is not used in this platform in this release. It is reserved for development.

2.6.42 EOC

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

Logical Object: STMN

The SDH DCC Termination Failure alarm occurs when the ONS 15600 SDH loses its DCC. Although this alarm is primarily SDH, it can apply to dense wavelength division multiplexing (DWDM) in other platforms.

The Regenerator-Section DCC (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 15600 SDH uses the DCC on the SDH Section layer to communicate network management information.

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

Warning **Use of controls, adjustments, or performing procedures other than those specified may result in hazardous radiation exposure.** Statement 1057

Note If a circuit shows an incomplete state when this alarm is raised, the logical circuit is in place. The circuit is able to carry traffic when the connection issue is resolved. You do not need to delete the circuit when troubleshooting this alarm.

Clear the EOC Alarm

Step 1 If the "LOS (STMN)" alarm on page 2-84 is also reported, complete the "Clear the LOS (STMN) Alarm" procedure on page 2-84. (This procedure is also used for EOC.)

Step 2 If the "MS-EXC" condition on page 2-97 is reported, complete the "Clear the MS-DEG Condition" procedure on page 2-97. (This procedure is also used for EOC.)

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 fiber connections and terminations, refer to the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15600 SDH Procedure Guide*.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15600 SDH. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

If the physical connections are correct and configured to carry DCC traffic, ensure that both ends of the fiber span have fully operational (Unlocked-enabled) ports. Verify that the SRV LED on each STM-N card is green.

Step 4 When the LEDs on the STM-N cards are correctly illuminated, complete the "2.8.5 Verify or Create Node DCC Terminations" procedure on page 2-138.

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 STM-N card shows a green LED in CTC or on the physical card.

A green SRV LED indicates an active 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 click **Unlocked** from the drop-down list. Click **Apply**.

Note If ports managed into Unlocked administrative state are not receiving signals, the LOS alarm is either raised or remains, and the port service state transitions to Unlocked-disabled,failed.

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 the STM-N card. It could be necessary to manually switch traffic carrying circuits over to a protection path. Refer to the "2.8.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-121 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 "1.9.3 Optical Traffic Card Transmit and Receive Levels" section on page 1-76 for information.

Step 9 If budget loss is within parameters, ensure that fiber connectors are securely fastened and properly terminated. For more information refer to the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15600 SDH Procedure Guide*.

Step 10 If fiber connectors are properly fastened and terminated, complete the "Soft-Reset a Card Using CTC" procedure on page 2-129.

Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card.

Resetting the active TSC card switches control to the standby TSC card. If the alarm clears when the ONS 15600 SDH node switches to the standby TSC card, the user can assume that the previously active card is the cause of the alarm.

Step 11 If the TSC 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 15600 SDH Procedure Guide* for instructions.

Step 13 Verify that both ends of the DCC have been recreated at the optical ports.

Step 14 If the alarm has not cleared, call Cisco TAC (1-800-553-2447). If the Cisco TAC technician tells you to reseat the card, complete the "Reset a Card with a Card Pull (Reseat)" procedure on page 2-131. If the Cisco TAC technician tells you to remove the card and reinstall a new one, follow the "Replace a TSC Card" procedure on page 2-134.

2.6.43 EQPT (CAP)

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

Logical Object: CAP

An Equipment Failure alarm for the CAP indicates that the customer access panel has a physical failure. Log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.44 EQPT (EQPT)

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

Logical Object: EQPT

An Equipment Failure alarm indicates that a hardware failure has occurred on the reporting card. If the EQPT alarm occurs with a BKUPMEMP alarm, refer to the "2.6.19 BKUPMEMP" section on page 2-26. The BKUPMEMP procedure also clears the EQPT alarm.

This alarm is also invoked if a diagnostic circuit detects a card application-specific integrated circuit (ASIC) failure. In this case, if the card is part of a protection group, an APS switch occurs. If the card is the protect card, switching is inhibited. The standby path generates a path-type alarm.

Clear the EQPT Alarm

Step 1 Complete the appropriate procedure in the "2.8.3 CTC Card Resetting and Switching" section on page 2-129 section.

Step 2 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. For LED appearance, see the "2.7 LED Behavior" section on page 2-118.

Step 3 If the CTC reset does not clear the alarm, complete the appropriate procedure in the "2.8.4 Physical Card Reseating, Resetting, and Replacement" section on page 2-131 section procedure for the reporting card.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15600 SDH. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 4 If the physical reseat of the card fails to clear the alarm, complete the "Replace an I/O Card" section on page 2-133 procedure 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 "2.8.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-121 for more 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 5 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) to report a Service-Affecting (SA) problem.

2.6.45 EQPT (PIM)

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

Logical Object: PIM

The EQPT alarm for the ASAP card 4PIO module (or PIM) is raised when all ports on the four-port module fail.

Clear the EQPT (PIM) Alarm

Step 1 Complete the "Replace an ASAP 4PIO (PIM) Module" procedure on page 2-136.

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.

2.6.46 EQPT (PPM)

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

Logical Object: PPM

The EQPT alarm for the SFP (PPM) is raised when one of the SFP (PPM) ports on a four-port 4PIO (PIM) module fails.

Clear the EQPT (PPM) Alarm

Step 1 Replace the alarmed SFP (PPM) by completing the "Replace an ASAP SFP (PPM) Module" procedure on page 2-137.

Step 2 If the alarm does not clear, move traffic off any active PPMs (SFPs). See the "Initiate a 1+1 Protection Port Force Switch Command" procedure on page 2-122. After switching traffic, replace the 4PIO (PIM) using the instructions in the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15600 SDH Procedure Guide*.

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) to report a Service-Affecting (SA) problem.

2.6.47 EQPT-BOOT

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

Logical Object: EQPT

An Equipment Boot Failure alarm occurs when a TSC card, SSXC card, or traffic (STM-N) card does not fully boot from the restart point after self-rebooting three times.

Clear the EQPT-BOOT Alarm

Step 1 Complete the "Clear the EQPT 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 call Cisco TAC (1-800-553-2447) to report a Service-Affecting (SA) problem.

2.6.48 EQPT-CC-PIM

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

Logical Object: PIM

The EQPT Alarm on a Carrier or 4PIO (PIM) is raised when an LOF or LOS alarm is shown on an ASAP card but this alarm is not also shown against the 4PIO (PIM) that carries the affected traffic. If multiple four-port 4PIOs (PIMs) do not show this LOF or LOS alarm, the EQPT-CC-PIM alarm raises against the ASAP carrier card itself.

Clear the EQPT-CC-PIM Alarm

Step 1 Complete the "Replace an ASAP 4PIO (PIM) Module" procedure on page 2-136.

Step 2 If the alarm does not clear, move traffic off any active 4PIOs (PIMs). Procedures and guidelines to do this are located in the "Maintain the Node" chapter in the *Cisco ONS 15600 SDH Procedure Guide*. Then complete the "Replace an ASAP Carrier Module" procedure on page 2-136 and reinstall the 4PIOs (PIMs) by completing the "Replace an ASAP 4PIO (PIM) Module" procedure on page 2-136. For more information about removing or installing these modules, refer to the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15600 SDH Procedure Guide*.

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) to report a Service-Affecting (SA) problem.

2.6.49 EQPT-HITEMP

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

Logical Object: EQPT

The Equipment Failure High Temperature alarm occurs when the TSC card, SSXC card, or traffic (STM-N) card internal temperature exceeds 185 degrees Fahrenheit (85 degrees Celsius).

Clear the EQPT-HITEMP Alarm

Step 1 Ensure that the room temperature is not abnormally high.

Step 2 If the room temperature is not the cause of the alarm, ensure that filler modules are installed in the ONS 15600 SDH empty slots. Filler modules help airflow.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15600 SDH. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 3 If the "FAN-DEGRADE" alarm on page 2-56 or the "FAN-FAIL" alarm on page 2-56 accompanies the alarm, complete the "Clear the FAN-FAIL Alarm" procedure on page 2-57.

Step 4 If the alarm does not clear, check the condition of the air filter to see if it needs cleaning or replacement. Replace the air filter using the procedure located in the "Maintain the Node" chapter in the *Cisco ONS 15600 SDH Procedure Guide* as needed.

Step 5 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.50 EQPT-PIM-PPM

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

Logical Object: PPM

The EQPT alarm for an SFP (PPM) is raised when a 4PIO (PIM) is reporting low electrical amplitude from an SFP (PPM). If this symptom shows up from multiple SFPs (PPMs) then the alarm should be against the 4PIO (PIM). Otherwise the alarm will be against the SFP (PPM) creating the problem.

Clear the EQPT-PIM-PPM Alarm

Step 1 Move any traffic away from the affected SFP (PPM), using guidelines and instructions in the "Maintain the Node" chapter in the *Cisco ONS 15600 SDH Procedure Guide*, then replace the alarmed SFP (PPM) module using instructions in that guide.

Step 2 If the alarm does not clear, move any traffic away from the affected 4PIO (PIM), using the instructions in the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15600 SDH Procedure Guide*, and replace the 4PIO (PIM).

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) to report a Service-Affecting (SA) problem.

2.6.51 E-W-MISMATCH

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

Logical Object: STMN

A Procedural Error Misconnect East/West Direction alarm occurs during MS-SPRing setup, or when nodes in a ring have slots misconnected. An east slot can be misconnected to another east slot, or a west slot can be 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 set up of a ring with its East-West slots configured correctly. If the alarm appears during the initial setup, the alarm clears itself shortly after the ring setup is complete.

Note The lower-numbered slot at a node is traditionally labeled the west slot and the higher numbered slot is labeled the east slot. For example, in the ONS 15600 SDH system, Slot 2 is west and Slot 12 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.

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 15600 SDH Procedure Guide* for more information about cable installation in 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 **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 may 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 call Cisco TAC (1-800-553-2447) 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 ID or Node ID Number" procedure on page 2-120 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 call Cisco TAC (1-800-553-2447) to report a Service-Affecting (SA) problem.

2.6.52 EXERCISE-RING-FAIL

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

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.

Clear the EXERCISE-RING-FAIL Condition

Step 1 Look for and clear, if present, the "LOF (STMN)" alarm on page 2-81, the "LOS (STMN)" alarm on page 2-84, or a MS-SPRing alarm.

Step 2 Complete the "Initiate an Exercise Ring Switch on an MS-SPRing" procedure on page 2-128.

Step 3 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.53 EXERCISE-SPAN-FAIL

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

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.

Clear the EXERCISE-SPAN-FAIL Condition

Step 1 Look for and clear, if present, the "LOF (STMN)" alarm on page 2-81, the "LOS (STMN)" alarm on page 2-84, or a MS-SPRing alarm.

Step 2 Complete the "Initiate an Exercise Ring Switch on an MS-SPRing" procedure on page 2-128.

Step 3 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.54 EXT

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

Logical Object: ENVALRM

A Failure Detected External to the NE alarm occurs because an environmental alarm is present. For example, a door could be open or flooding might have occurred.

Clear the EXT Alarm

Step 1 Click the **Maintenance > Alarm Extenders > External Alarms** tabs to gather further information about the EXT alarm.

Step 2 Follow your standard operating procedure to remedy environmental conditions that cause alarms. The alarm clears when the situation is remedied.

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).

2.6.55 EXTRA-TRAF-PREEMPT

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

Logical Object: STMN

An Extra Traffic Preempted alarm occurs on STM-N cards in two-fiber and four-fiber MS-SPRings when 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 checking the Conditions tab.

Step 2 If a ring switch has occurred, clear the ring switch on the working system by following the appropriate alarm in this chapter. For more information about protection switches, refer to the “Maintain the Node” chapter in the *Cisco ONS 15600 SDH Procedure Guide*.

Step 3 If the alarm occurred on a four-fiber MS-SPRing and the span switch occurred on this STM-N, clear the span switch on the working system.

Step 4 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) to report a Service-Affecting (SA) problem.

2.6.56 FAILTOSW

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

Logical Object: STMN

The Failure to Switch to Protection Facility condition occurs when a working or protect electrical 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.

Step 2 If the condition does not clear, replace the working electrical (traffic) card that is reporting the higher priority alarm by following the correct replacement procedure in the "2.8.4 Physical Card Reseating, Resetting, and Replacement" procedure on page 2-131. This card is the working electrical card using the protect card and not reporting FAILTOSW.

Replacing the working electrical 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 If an ONS 15600 SDH traffic (STM-N) card is implicated and you are able to continue using the traffic card with one port out of service, perform a bridge and roll to move the port traffic to a free port; refer to the "Manage Circuits" chapter in the *Cisco ONS 15600 SDH Procedure Guide* for instructions. Label the bad port, and place it out of service until such time as the card can be replaced.

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 Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.57 FAILTOSW-HO

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

SDH Logical Objects: 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 2-52.

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.

2.6.58 FAILTOSWR

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

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 TSC card (done under Cisco TAC supervision).
- 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 "MS-DEG" condition on page 2-96 or the "MS-EXC" condition on page 2-97) clears.

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 may result in hazardous radiation exposure.** Statement 1057

Clear the FAILTOSWR Condition in a Two-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** from 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 FAILTOSW-RING 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 SRV LED indicates an active 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**.

Note If ports managed into Unlocked administrative state are not receiving signals, the LOS alarm is either raised or remains, and the port service state transitions to Unlocked-disabled,failed.

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 "2.8.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-121 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 in the "Maintain the Node" chapter in the *Cisco ONS 15600 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 "1.9.3 Optical Traffic Card Transmit and Receive Levels" section on page 1-76 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 "Replace an I/O Card" procedure on page 2-133 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 "2.8.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-121 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 Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.59 FAILTOSWS

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

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 TSC card done under Cisco TAC supervision.
- A node power cycle.
- A higher-priority event such as an external switch command occurs.
- The next span switch succeeds.
- The cause of the APS switch (such as the "MS-DEG" condition on page 2-96 or the "MS-EXC" alarm on page 2-97) 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 west card or the east 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 SRV LED indicates an active 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**.

Note If ports managed into Unlocked administrative state are not receiving signals, the LOS alarm is either raised or remains, and the port service state transitions to Unlocked-disabled,failed.

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 "2.8.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-121 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 in the "Maintain the Node" chapter in the *Cisco ONS 15600 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 "1.9.3 Optical Traffic Card Transmit and Receive Levels" section on page 1-76 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 "Replace an I/O Card" procedure on page 2-133 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 "2.8.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-121 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 Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.60 FAN-DEGRADE

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

Logical Object: FAN

The Partial Fan Failure Speed Control Degradation alarm occurs if fan speed for one of the fans in the fan-tray assembly falls under 500 RPM when read by a tachometry counter.

Clear the FAN-DEGRADE Alarm

Step 1 Complete the "Clear the FAN-FAIL Alarm" procedure on page 2-57.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.61 FAN-FAIL

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

Logical Object: FAN

The Fan Failure alarm occurs when two or more fans (out of a total of six) have failed. The ONS 15600 SDH has no standby fan. All fans should be active. The FAN-FAIL alarm can be accompanied by the "MFGMEM (FAN)" alarm on page 2-94 against the fan. This alarm can also be raised in conjunction with a "PWR" alarm on page 2-101.

Clear the FAN-FAIL Alarm

Step 1 If the "MFGMEM (FAN)" alarm on page 2-94 is also reported against the fan, complete the "Clear the MFGMEM (FAN) Alarm" procedure on page 2-94.

Step 2 If the alarm does not clear, check the condition of the air filter to see if it needs cleaning or replacement using the procedure located in the "Maintain the Node" chapter in the *Cisco ONS 15600 SDH Procedure Guide*.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15600 SDH. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 3 If the alarm does not clear and if the filter is clean, remove the reporting fan trays from the ONS 15600 SDH.

Step 4 Reinsert the fan trays, making sure you can hear the fans start operating.

Fans should run immediately when correctly inserted.

Step 5 If the alarm does not clear or if the fans do not run, replace the fan trays using the procedure located in the "Maintain the Node" chapter in the *Cisco ONS 15600 SDH Procedure Guide*.

Step 6 If the alarm does not clear or if the replacement fan trays do not operate correctly, 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.

2.6.62 FAN-FAIL-PARTIAL

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

Logical Object: FAN

The Partial Fan Failure alarm occurs when one of the six fans in the shelf fails.

Troubleshoot with the "Clear the FAN-FAIL Alarm" procedure on page 2-57 procedure. If the alarm does not clear, log on to http://www.cisco.com/tac for more information or call Cisco TAC at 1-800-553-2447.

2.6.63 FAN-PWR

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

Logical Object: FAN

The Fan Power Failure alarm occurs when a power feed (A or B) from the shelf to Fan Tray 1, 2, or 3 fails. Because fans are not able to differentiate the power feeds, there is only one alarm for A or B failure.

Clear the FAN-PWR Alarm

Step 1 Remove the reporting fan trays from the ONS 15600 SDH.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15600 SDH. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 2 Reinsert the fan trays, making sure you hear the fans start to operate.

Fans should run immediately when correctly inserted.

Step 3 If the alarm does not clear or if the fans do not run, replace the fan trays using the procedure located in the "Maintain the Node" chapter in the *Cisco ONS 15600 SDH Procedure Guide*.

Step 4 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.64 FE-FRCDWKSWBK-SPAN

The FE-FRCDWKSWBK-SPAN condition is not used in this platform in this release. It is reserved for development.

2.6.65 FE-FRCDWKSWPR-RING

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

Logical Object: STMN

The Far End Ring Working Facility Forced to Switch to Protection condition occurs when a far-end node ring is forced from working to protect using the FORCE RING command. This condition is only visible on the network view Conditions tab.

The prefix FE means the main alarm is occurring at the far-end node and not at the node reporting the FE-FRCDWKSWPR-RING condition. Troubleshoot the FE condition by troubleshooting the main alarm at its source. The secondary alarms or conditions clear when the primary alarm clears.

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 a MS-SPRing External Switching Command" procedure on page 2-128.

Step 5 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.66 FE-FRCDWKSWPR-SPAN

The FE-FRCDWKSWPR-SPAN condition is not used in this platform in this release. It is reserved for development.

2.6.67 FE-LOCKOUTOFPR-ALL

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

Logical Object: STMN

The Far End Lockout of Protection All condition occurs on far-end MS-SPRing nodes when traffic is locked on a node using the LKOUTPR-S command.

The prefix FE means the main alarm is occurring at the far-end node and not at the node reporting this condition. Troubleshoot the FE condition by troubleshooting the main alarm at its source. Both the alarms or conditions clear when the main alarm clears.

Clear the FE-LOCKOUTOFPR-ALL Condition

Step 1 To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE alarm.

Step 2 Log into the node that links directly to the card reporting the FE condition.

Step 3 Ensure there is no lockout set. Complete the "Clear a MS-SPRing External Switching Command" procedure on page 2-128.

Step 4 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.68 FE-LOCKOUTOFPR-SPAN

The FE-LOCKOUTOFPR-SPAN condition is not used in this platform in this release. It is reserved for development.

2.6.69 FE-MANWKSWBK-SPAN

The FE-MANWKSWBK-SPAN condition is not used in this platform in this release. It is reserved for development.

2.6.70 FE-MANWKSWPR-RING

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

Logical Object: STMN

The Far End Ring Manual Switch of Working to Protect condition occurs when a 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-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 Complete the "Clear a MS-SPRing External Switching Command" procedure on page 2-128.

Step 4 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.71 FE-MANWKSWPR-SPAN

The FE-MANWKSWPR-SPAN condition is not used in this platform in this release. It is reserved for development.

2.6.72 FEPRLF

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

Logical Object: STMN

The Far-End Protection Line Failure alarm occurs when there is an "MS-EXC" condition on page 2-97 condition on the protect card's APS channel coming into the node.

Note The FEPRLF alarm occurs on the ONS 15600 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.

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.

2.6.73 FE-SF-SPAN

The FE-SF-SPAN condition is not used in this platform in this release. It is reserved for development.

2.6.74 FORCED-REQ

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

Logical Object: VCMON-HP

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 2-123.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.75 FORCED-REQ-RING

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

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 a MS-SPRing External Switching Command" procedure on page 2-128.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.76 FORCED-REQ-SPAN

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

Logical Object: STMN

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 not only the facility, but the span.

Clear the FORCED-REQ-SPAN Condition

Step 1 Complete the “Clear a MS-SPRing External Switching Command” procedure on page 2-128.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.77 FRCDSWTOINT

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

Logical Object: NE-SREF

The Force Switch to Internal Timing condition occurs when the user issues a Force command to switch to an internal timing source.

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

2.6.78 FRCDSWTOPRI

The FRCDSWTOPRI condition is not used in this platform in this release. It is reserved for development.

2.6.79 FRCDSWTOSEC

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

Logical Objects: EXT-SREF, NE-SREF

The Force Switch to Second Timing Source condition occurs when the user issues a Force command to switch to the second timing source.

Note FRCDSWTOSEC is an informational condition. It does not require troubleshooting.

2.6.80 FRCDSWTOTHIRD

The FRCDSWTOTHIRD condition is not used in this platform in this release. It is reserved for development.

2.6.81 FREQ-MISMATCH

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

Logical Object: EQPT

The Frequency Mismatch alarm occurs when one of the two TSC cards has a timing module failure that causes an inconsistency between the TSC card timing frequencies. This alarm can be caused by the active or standby TSC card.

The ONS 15600 SDH checks timing frequency synchronization in 83-minute (1 hour and 23 minutes) cycles. The FREQ-MISMATCH alarm occurs if two consecutive timing check cycles show frequency mismatches. The alarm is cleared if one cycle shows a timing frequency match between the TSC cards.

Clear the FREQ-MISMATCH Alarm

Step 1 Complete the "Replace a TSC Card" procedure on page 2-134 for the standby TSC card.

Step 2 Wait for two intervals of 83 minutes (2 hours and 46 minutes) and check the node view Alarms tab to see whether the alarm is cleared.

During the initial 83-minute synchronization check cycle while the replacement standby TSC card is booting up, the replacement TSC card is attaining the timing from the BITS or internal source so it is normal that the two TSC cards are not synchronized. The ONS 15600 SDH system disregards the result of this check cycle and begins keeping track of synchronization in the second 83-minute cycle. If the result of the cycle shows that the TSC cards are synchronized properly, the alarm is cleared.

Step 3 If the FREQ-MISMATCH alarm did not clear after two timing check cycles, it means that the second timing cycle resulted in a mismatch. Wait a third 83-minute cycle and check the alarm again.

If the alarm has cleared, it means a third cycle showed that the TSC card timing modules were synchronized. If the alarm remains, it means that the ONS 15600 SDH system has had two frequency mismatch cycles, and indicates a problem with the other TSC card.

Step 4 If the FREQ-MISMATCH alarm remains after three 83-minute cycles, complete the "Soft-Reset a Card Using CTC" procedure on page 2-129 to make the TSC card standby.

Step 5 Complete the "Reset a Card with a Card Pull (Reseat)" procedure on page 2-131 for the standby TSC card.

The card removal and reboot temporarily clears the alarm.

Step 6 Wait for three intervals of 83 minutes (4 hours and 9 minutes) and check CTC to see if the FREQ-MISMATCH alarm has recurred. If it has not recurred, the problem is solved.

Step 7 If the alarm has recurred after both TSC cards have been replaced, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.82 FRNGSYNC

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

Logical Object: NE-SREF

The Free Running Synchronization Mode condition occurs when the reporting ONS 15600 SDH is in free-run synchronization mode. External timing sources have been disabled and the node is using its internal clock, or the node has lost its designated BITS timing source. After the 24-hour holdover period expires, timing slips could begin to occur on an ONS 15600 SDH node relying on an internal clock.

Note If the ONS 15600 SDH is configured to operate from its internal clock, disregard the FRNGSYNC condition.

Clear the FRNGSYNC Condition

Step 1 If the ONS 15600 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 15600 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 2-113 and the "SYNCSEC" alarm on page 2-114.

Step 3 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.83 FSTSYNC

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

Logical Object: EQPT

The Fast Synchronization Mode condition occurs when the ONS 15600 SDH synchronizes its clock modules. Since the ONS 15600 SDH uses Stratum 3E timing, synchronization can take about 12 minutes. This condition occurs on the TSC card where the timing distribution is sourced. Whenever this condition is active, any timing or controller switching might affect the traffic. Errorless switching is not guaranteed.The "UNPROT-SYNCCLK" alarm on page 2-115 can accompany this condition if there is no timing protection is available while the clock is synchronizing.

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

2.6.84 FULLPASSTHR-BI

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

Logical Object: STMN

The Bidirectional Full Pass-Through Active condition occurs on a nonswitching node in a MS-SPRing when the protect channels on the node are active and carrying traffic and a change is present in the receive K byte from "No Request." (Both data and K bytes are in pass-through mode.)

Clear the FULLPASSTHR-BI Condition

Step 1 Complete the "Clear a MS-SPRing External Switching Command" procedure on page 2-128.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) to report a Service-Affecting (SA) problem.

2.6.85 GFP-LFD

The GFP-LFD condition is not used in this platform in this release. It is reserved for development.

2.6.86 GFP-UP-MISMATCH

For information about this condition, refer to the "Alarm Troubleshooting" chapter of the *Cisco ONS 15454 DWDM Troubleshooting Guide*.

2.6.87 HELLO

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

Logical Object: STMN

The Open Shortest Path First (OSPF) Hello Fail alarm occurs when SDH DCC termination OSPF area IDs are mismatched between two DCC terminations for a span. On a span between two ONS 15600 SDHs, this alarm occurs at both nodes containing the mismatched DCC area IDs. On a span between an ONS 15600 SDH and an ONS 15454 SDH, this alarm is raised only on the ONS 15600 SDH node. Mismatched OSPF area IDs can cause CTC to lose management across the link.

Clear the HELLO Alarm

Step 1 Log into both end nodes with the DCC terminations.

Step 2 On the nodes where the alarm occurred, record the slot and port (from the Slot column and Port column in the Alarms window) that the Hello alarm occurs against. This information helps you determine which DCC termination is mismatched.

Tip You can log into another node by going to network view and double-clicking the node.

Step 3 On one node, in node view, click the **Provisioning > Network > OSPF** tabs.

Step 4 In the DCC OSPF Area ID Table area, locate the alarmed DCC termination by comparing slot and port numbers to the slot and port number indicated in the alarm on the node.

Step 5 Click the Area ID column cell for the mismatched DCC termination.

Step 6 Change the area ID in the cell to the same ID as its partner DCC termination. (The ONS 15600 SDH defaults to 0.0.0.0 format addresses.)

Step 7 Click **Apply**.

Step 8 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.88 HIBATVG

The HIBATVG condition is not used in this platform in this release. It is reserved for development.

2.6.89 HI-LASERBIAS

For information about this condition, refer to the “Alarm Troubleshooting” chapter of the *Cisco ONS 15454 DWDM Troubleshooting Guide*.

2.6.90 HI-RXPOWER

For information about this condition, refer to the “Alarm Troubleshooting” chapter of the *Cisco ONS 15454 DWDM Troubleshooting Guide*.

2.6.91 HI-TXPOWER

For information about this condition, refer to the “Alarm Troubleshooting” chapter of the *Cisco ONS 15454 DWDM Troubleshooting Guide*.

2.6.92 HLDOVRSYNC

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

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 15600 SDH relying on an internal clock.

Clear the HLDOVRSYNC Condition

Step 1 Clear additional alarms that relate to timing, such as:

- 2.6.82 FRNGSYNC, page 2-64
- 2.6.83 FSTSYNC, page 2-64
- 2.6.116 LOF (BITS), page 2-80
- 2.6.123 LOS (BITS), page 2-84
- 2.6.135 MANSWTOINT, page 2-90
- 2.6.136 MANSWTOPRI, page 2-90
- 2.6.137 MANSWTOSEC, page 2-90
- 2.6.138 MANSWTOTHIRD, page 2-91
- 2.6.181 SWTOPRI, page 2-111
- 2.6.182 SWTOSEC, page 2-111
- 2.6.183 SWTOTHIRD, page 2-112
- 2.6.186 SYNC-FREQ, page 2-113
- 2.6.187 SYNCPRI, page 2-113
- 2.6.188 SYNCSEC, page 2-114
- 2.6.189 SYNCTHIRD, page 2-114

Step 2 Reestablish a primary and secondary timing source according to local site practice. If none exists, refer to the "Change Node Settings" chapter in the *Cisco ONS 15600 SDH Procedure Guide* to find one.

Step 3 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) in order to report a Service-Affecting (SA) problem.

2.6.93 HP-DEG

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

Logical Object: VCMON-HP

The High-Order Path Signal Degrade condition occurs when the B3 error count in the SDH overhead exceeds the limit.

Clear the HP-DEG Condition

Step 1 Troubleshoot using the "Clear the MS-DEG Condition" procedure on page 2-97.

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.

2.6.94 HP-EXC

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

Logical Object: VCMON-HP

The High Order Path-Excessive BER condition occurs when the B3 error count in the SDH overhead exceeds the limit.

Clear the HP-DEG Condition

Step 1 Troubleshoot using the "Clear the MS-DEG Condition" procedure on page 2-97.

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.

2.6.95 HP-PLM

The HP-PLM condition is not used in this platform in this release. It is reserved for development.

2.6.96 HP-RFI

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

Logical Object: VCMON-HP

The High-Order Remote Failure Indication (RFI) condition indicates that there is a remote failure indication in the high-order (VC-4 or VC-3) path, and that the failure has persisted beyond the maximum time allotted for transmission system protection. The HP-RFI is sent as the protection switch is initiated. Resolving the fault in the adjoining node clears the HP-RFI condition in the reporting node.

Clear the HP-RFI Condition

Step 1 Log into the node at the far end of the reporting ONS 15600 SDH.

Step 2 Determine whether there are any related alarms, especially the "LOS (STMN)" alarm on page 2-84.

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.

2.6.97 HP-TIM

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

SDH Logical Objects: VCMON-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 2-113.

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.

2.6.98 HP-UNEQ

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

Logical ObjectS: VCMON-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. Delete the circuit.

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.

Step 10 Recreate the circuit with the correct circuit size. Refer to the "Create Circuits and Tunnels" chapter in the *Cisco ONS 15600 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 15600 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, replace the optical and/or Ethernet 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 15600 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.

2.6.99 IMPROPRMVL (CAP)

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

Logical Object: CAP

The Improper Removal CAP alarm occurs when a CAP is not correctly installed on the backplane or is missing altogether. The problem is not user serviceable. Contact the Cisco TAC at 1-800-553-2447.

2.6.100 IMPROPRMVL (EQPT, PIM, PPM)

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

Logical Objects: EQPT, PIM, PPM

The Improper Removal equipment alarm occurs when a card is physically removed from its slot before it is deleted from CTC. The card does not need to be in service to cause the IMPROPRMVL alarm; it only needs to be recognized by CTC. The alarm does not appear if you delete the card from CTC before you physically remove the card from the node. It can also occur if the card is inserted into a slot but is not preprovisioned or fully plugged into the backplane. For ASAP card SFPs (PPMs), the alarm occurs if you provision an SFP (PPM) but no physical module is inserted on the port, or if no SFP (PPM) is inserted into the 4PIO (PIM).

Caution If CTC begins to reboot a card before you remove the card, allow the card to finish rebooting. After the card reboots, delete the card in CTC and physically remove the card before it begins to reboot. When you delete the card, CTC loses connection with node view and goes to network view.

Note It can take up to 30 minutes for software to be updated on a standby TSC card.

Clear the IMPROPRMVL (EQPT, PIM, PPM) 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. However if none of these services is provisioned, you can delete an Unlocked card.

Step 3 If any ports on the card are in service, place them out of service (Locked,maintenance) by completing the following steps:

Caution Before placing a port out of service (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** tabs.

c. Click the **Admin State** column of any in-service (Unlocked) ports.

d. Choose **Locked,maintenance** to take the ports out of service.

Step 4 If a circuit has been mapped to the card, delete it using the procedure in the “Manage Circuits” chapter in the *Cisco ONS 15600 SDH Procedure Guide*.

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 node view **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.

Step 7 If the card is used as a timing reference, change the timing reference by completing the following steps:

a. Click the **Provisioning > Timing > General** tabs.

b. Under NE Reference, click the drop-down arrow for **Ref-1**.

c. Change Ref-1 from the listed STM-N card to **Internal Clock**.

d. Click **Apply**.

Step 8 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) in order to report a Service-Affecting (SA) problem.

2.6.101 IMPROPRMVL (EQPT for the SSXC or TSC Card)

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

Logical Object: EQPT

The Improper Removal SSXC, Traffic Card, or TSC card alarm occurs when a TSC card, SSXC card, or traffic (STM-N) card is physically removed from its slot. This alarm can occur if the card is recognized by CTC and the active TSC card but is not in service. For example, it could be inserted in the slot but not fully plugged into the backplane.

If the removed TSC card or SSXC card is the last one on the shelf, the severity is Critical (CR) and traffic is affected. Otherwise, the alarm is Minor (MN).

Caution Do not remove and reinsert (reseat) a card during a card reboot. If CTC begins to reboot a card before you remove the card, 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 After deleting a card in CTC, the software allows you approximately 15 seconds to physically remove the card before CTC begins a card reboot.

Clear the IMPROPRMVL (SSXC, TSC) Alarm

Step 1 Complete the "Reset a Card with a Card Pull (Reseat)" procedure on page 2-131 for the TSC card or SSXC. (The procedure is similar for both.)

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.102 IMPROPRMVL (FAN)

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

Logical Object: FAN

The Improper Removal Fan alarm occurs when Fan Tray 1, 2, or 3 is physically removed from its slot.

Clear the IMPROPRMVL (FAN) Alarm

Step 1 Refer to the "Maintain the Node" chapter in the *Cisco ONS 15600 SDH Procedure Guide* for procedures to replace the fan-tray assembly.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15600 SDH. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 2 If the fan tray does not run immediately, troubleshoot with the "Clear the FAN-FAIL Alarm" procedure on page 2-57.

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).

2.6.103 IMPR-XC

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

Logical Object: NE

The Improper Cross-Connect Card alarm indicates that the CXC card is being used rather than the SSXC (the preferred cross-connect card for Software R5.0 and later). The alarm remains standing as long as a CXC is present on the node. Since a CXC card is still capable of passing traffic, the alarm is not Service-Affecting (SA). However, a system containing a CXC card and the current software release is not fully guaranteed for functionality.

Note IMPR-XC is an informational alarm and does not require troubleshooting. However, if you are experiencing cross-connect related problems at this site, also report this alarm to the Cisco TAC.

2.6.104 INCOMPATIBLE-SEND-PDIP

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

Logical Object: SYSTEM

The Incompatible Send-PDIP alarm is raised when CTC's send-PDIP provisioning differs from the host node's provisioning.

Clear the INCOMPATIBLE-SEND-PDIP Alarm

Step 1 Reconfigure CTC's send-PDI-P alarm capability to align with the host node settings.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.105 INCOMPATIBLE-SW

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

Logical Object: SYSTEM

The Incompatible Software alarm is raised when CTC cannot connect to the NE due to incompatible versions of software between CTC and the NE. The alarm is cleared by restarting CTC in order to redownload the CTC JAR files from the NE.

Clear the INCOMPATIBLE-SW Alarm

Step 1 Restart the CTC application.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.106 INTRUSION-PSWD

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

Logical Object: NE

The Security Intrusion Incorrect Password condition occurs after a user attempts a provisionable (by Superuser) number of unsuccessful logins, a login with an expired password, or an invalid password. The alarmed user is locked out of the system, and INTRUSION-PSWD condition is raised. This condition is only shown in Superuser login sessions, not in login sessions for lower-level users. The INTRUSION-PSWD condition is automatically cleared when a provisionable lockout timeout expires, or it can be manually cleared in CTC by the Superuser if 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 Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.107 INVMACADR

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

Logical Object: BPLANE

The Invalid MAC Address alarm occurs when the ONS 15600 SDH MAC address retrieval fails and the node does not have a valid MAC address to support the operating system (OS). Do not attempt to troubleshoot an INVMACADR alarm. Contact the Cisco TAC at (1-800-553-2447).

2.6.108 ISIS-ADJ-FAIL

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

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 15600 SDH Reference Manual*. For more information about configuring OSI, refer to the "Turn Up Node" chapter in the *Cisco ONS 15600 SDH Procedure Guide*.

Clear the ISIS-ADJ-FAIL Alarm

Step 1 Ensure that both ends of the comm 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 > RS-DCC** tabs.
- **b.** Click the row of the circuit. Click **Edit**.
- **c.** In the Edit RS-DCC 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 15600 SDH Procedure Guide* for the procedure.

Step 3 If the nodes use Point-to-Point Protocol (PPP) Layer 2, complete the "Clear the EOC Alarm" procedure on page 2-42. 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 RS-DCC 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 RS-DCC 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 RS-DCC dialog box and click **OK**.

Step 7 If all of the preceding settings are correct, ensure that OSI routers are enabled for the communication channels at both ends by completing the following steps:

- **a.** Click the **Provisioning > OSI > Routers > Setup** tabs.
- **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 comm 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 in the *Cisco ONS 15600 SDH Procedure Guide* for instructions to do this.

Step 9 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.109 KB-PASSTHR

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

Logical Object: STMN

The K Byte Pass Through Active condition occurs on a nonswitching node in a MS-SPRing when the protect channels on the node are not active and the node is in K Byte pass-through state. It also occurs when a MS-SPRing ring is being exercised using the Exercise Ring command.

Clear the KB-PASSTHR Condition

Step 1 Complete the "Clear a MS-SPRing External Switching Command" procedure on page 2-128.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.110 KBYTE-APS-CHANNEL-FAILURE

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

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 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 AIS-P, LOF, LOS, or SF-BER 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 with the same parameters. To do this, refer to the "Manage Circuits" chapter in the *Cisco ONS 15600 SDH Procedure Guide* for procedures.

Step 2 If the error is not caused by incorrect provisioning, it is because of checksum errors within an STM-N, cross-connect, or TSC card. In this case, complete the "Request a Cross-Connect Card Preferred Copy Switch" procedure on page 2-130 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 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).

2.6.111 LASER-BIAS

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

Logical Objects: EQPT, PPM

The High Laser Bias Current alarm occurs when a port on an STM-64 card is transmitting a laser current outside of the acceptable preset range. The alarm occurs at the card level rather than at the port level. The alarm is typically accompanied by signal or bit errors on the downstream node.

Note The difference between this alarm and the laser bias current performance-monitoring parameter is that the alarm indicates a serious physical condition in the transmitter.

Clear the LASER-BIAS Alarm

Step 1 If the alarm is reported against the working STM-64 facility and traffic has not automatically switched to protect, initiate a Force switch. If it is part of an SNCP, complete the "Initiate a Force Switch for All Circuits on a SNCP Span" procedure on page 2-124. If is part of a 1+1 protection group, complete the "Initiate a 1+1 Protection Port Force Switch Command" procedure on page 2-122.

Step 2 Complete the "Replace an I/O Card" procedure on page 2-133 for the reporting card.

Step 3 If the alarm does not clear after replacing the card, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) to report a Service-Affecting (SA) problem.

Step 4 Traffic reverts to the working port if working port if an automatic switch occurred. If the alarm cleared and traffic was switched in Step 1, revert traffic by completing the "Clear a 1+1 Protection Port Force or Manual Switch Command" procedure on page 2-123. If traffic was manually switched in an SNCP, revert traffic to the original path by completing the "Clear a SNCP Span External Switching Command" procedure on page 2-126.

2.6.112 LASER-OVER-TEMP

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

Logical Objects: EQPT, PPM

The Port-Level High Temperature STM-64 equipment alarm accompanies a fault in one of the four STM-64 ports. The fault causes output signal bit errors that are detected by the downstream node, which performs an APS.

If more than one card has this condition, troubleshoot with the "Clear the EQPT-HITEMP Alarm" procedure on page 2-47. Any time an STM-64 card or port reports an over-temperature condition, follow the "Clear the LASER-BIAS Alarm" procedure on page 2-78. 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.

2.6.113 LKOUTPR-S

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

Logical Object: STMN

The Lockout of Protection Span condition occurs on a BSLR node when traffic is locked out of a protect span using the LOCKOUT SPAN command. This condition is visible on the network view Alarms, Conditions, and History tabs 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 a MS-SPRing External Switching Command" procedure on page 2-128.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.114 LOCKOUT-REQ

Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Objects: STMN, VCMON-HP

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 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 2-124.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.115 LOCKOUT-REQ-RING

Not Alarmed (NA), Non-Service-Affecting (NSA)

Logical Object: STMN

The Lockout Switch Request on Ring condition occurs when a user initiates a lockout switch request for an STM-N card or a lockout switch request on the MS-SPRing ring level. A lockout prevents protection switching. Clearing the lockout again allows protection switching and clears the LOCKOUT-REQ-RING condition.

Clear the LOCKOUT-REQ-RING Condition

Step 1 Complete the "Clear a MS-SPRing External Switching Command" procedure on page 2-128.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.116 LOF (BITS)

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

Logical Object: BITS

The Loss of Frame (BITS) alarm is Major (MJ) if there is no backup TSC card BITS source and Minor (MN) if one of the TSC cards BITS sources fails. If one of the pair fails, a timing APS is activated on the second source.

Clear the LOF (BITS) Alarm

Step 1 Verify that the framing and coding match between the BITS input and the TSC card by completing the following steps:

a. Find the coding and framing formats of the external BITS timing source. This should be in the user documentation for the external BITS timing source or on the external timing source itself.

b. Click the node view **Provisioning > Timing > BITS Facilities** tabs.

c. Verify that the Coding setting matches the Coding setting of the BITS timing source (either B8ZS or AMI).

d. If the coding does not match, click **Coding** to display a drop-down list. Choose the appropriate coding.

e. Verify that the Framing matches the framing of the BITS timing source (either ESF or SF [D4]).

f. If the framing does not match, click **Framing** to display the drop-down list. Choose the appropriate framing.

Note In the Timing window, the B8ZS coding field is normally paired with ESF in the Framing field, and the AMI coding field is normally paired with SF (D4) in the Framing field.

Step 2 Ensure that the BITS clock is operating properly.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15600 SDH. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 3 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.117 LOF (STMN)

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

Logical Object: STMN

The Line Loss of Frame Alignment alarm occurs when a port on the reporting traffic (STM-N) card has an LOF. LOF indicates that the receiving ONS 15600 SDH has lost frame delineation in the incoming data and when the SDH overhead loses a valid framing pattern for three milliseconds. Receiving two consecutive valid A1/A2 framing patterns clears the alarm.

LOF on a traffic card is sometimes an indication that the port reporting the alarm expects a specific line rate and the input line rate source does not match the input line rate of the optical receiver.

If the port is in 1+1 protection and successfully switches, the alarm severity is MN, NSA. If the port is unprotected or if protection switching is prevented, the severity is CR, SA.

Clear the LOF (STMN) Alarm

Step 1 Verify that the automatic protection switch to the protect port was successful.

- A SNCP APS is identified by an AUTOSW-type alarm or condition (such as AUTOSW-AIS, AUTOSW-LOP, AUTOSW-PDI, AUTOSW-SDBER, AUTOSW-SFBER, or AUTOSW-UNEQ).
- A 1+1 APS is identified on the node view Maintenance > Protection tab. If you click the protection group, under the Selected Group list, the ports are designated as Working/Standby and Protect/Active.

Step 2 Verify that the traffic (STM-N) card and port on the upstream node is in service.

- On an in-service traffic card, the green SRV and Laser On LEDs are illuminated.
- If the card ports are in service, in the card view Provisioning tab, the Status column for the port(s) show In Service. If the ports are not in service, click the port column and choose **In Service**, then click **Apply**.

Step 3 If the alarm does not clear, clean the optical fiber connectors by completing the following steps:

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15600 SDH. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

a. Clean the fiber connectors according to local site practice.

b. If no local practice exists, use a CLETOP Real-Type or equivalent fiber-optic cleaner and follow the instructions accompanying the product and/or refer to the procedures in the "Maintain the Node" chapter in the *Cisco ONS 15600 SDH Procedure Guide*.

Step 4 If you continue to receive the LOF alarm, see the "1.9.3 Optical Traffic Card Transmit and Receive Levels" section on page 1-76 for acceptable standards.

Step 5 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) to report a Service-Affecting (SA) problem.

2.6.118 LOGBUFR90

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

Logical Object: SYSTEM

The Log Buffer Over 90 alarm indicates that the per-NE queue of incoming alarm, event, or update capacity of 5,000 entries is over 90 percent full. LOGBUFR90 will clear if CTC recovers. If it does not clear, LOGBUFROVFL occurs.

Note LOGBUFR90 is an informational alarm and does not require troubleshooting.

2.6.119 LOGBUFROVFL

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

Logical Object: SYSTEM

The Log Buffer Overflow alarm indicates that the CTC per-NE queue of incoming alarm, event, or updates, which has a capacity of 5,000 entries, has overflowed. This happens only very rarely. However if it does, you must restart the CTC session. It is likely that some updates will have been missed if this alarm occurs.

Clear the LOGBUFROVFL Alarm

Step 1 Restart the CTC session.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.120 LO-LASERBIAS

For information about this condition, refer to the "Alarm Troubleshooting" chapter of the *Cisco ONS 15454 DWDM Troubleshooting Guide*.

2.6.121 LOP-P

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

Logical Object: VCMON-HP

A Loss of Pointer Path alarm indicates that the transmitted optical circuit size is different from the provisioned optical circuit size. LOP-P occurs when valid H1/H2 pointer bytes are missing from the SDH overhead. Receiving equipment monitors the H1/H2 pointer bytes to locate the SDH payload. An LOP-P alarm means that eight, nine, or ten consecutive frames do not have valid pointer values. The alarm clears when three consecutive valid pointers are received.

One of the conditions that can cause this alarm is a transmitted VC circuit that is different from the provisioned VC. This condition causes a mismatch of the path type on the concatenation facility. It occurs when there are eight to ten new data flags received, or eight to ten invalid pointers. For example, if an VC4 or VC3 is sent across a path provisioned for VC4-4c, an LOP alarm occurs.

Clear the LOP-P Alarm

Step 1 Complete the "Initiate a Force Switch for All Circuits on a SNCP Span" procedure on page 2-124 or the "Initiate a 1+1 Protection Port Force Switch Command" procedure on page 2-122 as appropriate.

Step 2 Use a test set to verify that the incoming signal is valid; refer to the "Create Circuits" chapter in the *Cisco ONS 15600 SDH Procedure Guide* for instructions on testing optical circuits. If the upstream signal is not valid, troubleshoot upstream.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15600 SDH. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 3 If the incoming signal is valid, complete the "Replace an I/O Card" procedure on page 2-133 for the reporting card.

Note If the traffic (STM-N) card is implicated and you are able to continue using the traffic card with one port out of service, perform a bridge and roll to move the port traffic to a free port. Refer to the "Manage Circuits" chapter in the *Cisco ONS 15600 SDH Procedure Guide* for instructions. Label the bad port, and place it out of service until the card can be replaced.

Step 4 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) to report a Service-Affecting (SA) problem.

2.6.122 LO-RXPOWER

For information about this condition, refer to the "Alarm Troubleshooting" chapter of the *Cisco ONS 15454 DWDM Troubleshooting Guide*.

2.6.123 LOS (BITS)

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

Logical Object: BITS

The Loss of Signal BITS alarm is Major (MJ) if there is no backup TSC card BITS source, and Minor (MN) if one of the TSC card BITS sources fails. If one of the pair fails, a timing APS is activated on the second source.

Clear the LOS (BITS) Alarm

Step 1 Check the wiring connection from the ONS 15600 SDH backplane BITS clock pin fields to the timing source. For more information about backplane wiring connections, refer to the "Install the Bay and Backplane Connections" chapter in the *Cisco ONS 15600 SDH Procedure Guide*.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15600 SDH. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 2 Ensure that the BITS clock is operating properly.

Step 3 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) to report a Service-Affecting (SA) problem.

2.6.124 LOS (STMN)

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

Logical Object: STMN

A Loss of Signal Line alarm for either an STM-16 or STM-64 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 ports, or no signal exists on the line. Possible causes for a loss of signal include upstream equipment failure or a fiber cut. It clears when two consecutive valid frames are received.

Clear the LOS (STMN) Alarm

Step 1 Verify fiber continuity to the port. To verify cable continuity, follow site practices.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15600 SDH. Plug the wristband cable into the ESD jack located on the lower-right 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 illuminated on the physical card.

A green SRV LED indicates an active card.

b. To determine whether the STM-N port is in service, double-click the card in CTC to display the card view by completing the following steps:

c. Click the **Provisioning > Line** tabs.

d. Verify that the Admin State column lists the port as Locked.

e. If the Admin State column lists the port as Locked,maintenance or Locked,disabled, click the column and choose **Locked**.

f. Click **Apply**.

Note If ports managed into Unlocked administrative state are not receiving signals, the LOS alarm is either raised or remains, and the port service state transitions to Unlocked-disabled,failed.

Step 3 If the correct port is in service, clean the fiber according to site practice. If no site practice exists, complete the procedure in the "Maintain the Node" chapter in the *Cisco ONS 15600 SDH Procedure Guide*.

Step 4 If the alarm does not clear, verify that the power level of the optical signal is within the STM-N card receiver specifications. The "1.9.3 Optical Traffic Card Transmit and Receive Levels" section on page 1-76 lists these specifications for each STM-N card.

Step 5 If the optical power level is within specifications, use an optical test set to verify that a valid signal exists on the line. For specific procedures to use the test set equipment, consult the manufacturer. Test the line as close to the receiving card as possible.

Step 6 If a valid signal exists, replace the connector on the backplane.

Step 7 Repeat Steps 1 to 6 for any other port on the card reporting the LOS (STM-N).

Step 8 If the alarm does not clear, look for and troubleshoot any other alarm that could identify the source of the problem.

Step 9 If no other alarms exist that could be the source of the LOS, or if clearing an alarm did not clear the LOS, complete the "Replace an I/O Card" procedure on page 2-133 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 "2.8.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-121 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 10 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) in order to report a Service-Affecting (SA) problem.

2.6.125 LO-TXPOWER

For information about this condition, refer to the "Alarm Troubleshooting" chapter of the *Cisco ONS 15454 DWDM Troubleshooting Guide*.

2.6.126 LPBKCRS

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

Logical Object: VCMON-HP

The Loopback Cross-Connect condition indicates that a software cross-connect loopback is active between a traffic (STM-N) card and a cross-connect card.

Loopback is a commonly used troubleshooting technique. A signal is sent out on a link or section of the network and returned to the sending device. If the signal does not return or returns with errors, the test confirms that the problem is present in the tested link. By setting up loopbacks on various parts of the node and excluding other parts, you can logically isolate the source of the problem. For more information about loopbacks, see the “Troubleshooting Optical Circuits with Loopbacks” procedure in Chapter 1.

Four types of loopbacks are available: Cross-Connect, Facility, Terminal, and Payload. Cross-connect loopbacks troubleshoot any kind of VC (meaning there must be a cross connect) on any card type. Facility loopbacks troubleshoot STM-16-16 and ASAP ports only and are generally performed locally or at the near end. Payload loopbacks troubleshoot STM-64-4 ports only and are generally performed locally or at the near end. Terminal loopbacks are performed only on the ASAP card.

Clear the LBKCRS Condition

Step 1 To remove the loopback cross-connect condition, double-click the traffic (STM-N) card in node view.

Step 2 Click the **Provisioning > VC3 or VC4** tabs.

Step 3 In the XC Loopback column, deselect the check box for the port.

Step 4 Click **Apply**.

Step 5 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.127 LPBKFACILITY (GIGE)

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

Logical Object: GIGE

A Loopback Facility condition for a Gigabit Ethernet (GE) port occurs when a software facility (line) loopback is active for an ASAP card client 4PIO (PIM) provisioned at the ONE_GE port rate.

For information about troubleshooting these circuits with loopbacks, refer to the “1.3 Troubleshooting an Ethernet Circuit Path With Loopbacks” section on page 1-29.

Note For more information about ASAP cards, refer to the *Cisco ONS 15600 SDH Reference Manual*.

Clear the LPBKFACILITY (GIGE) Condition

Step 1 Complete the “Clear the LBKFACILITY (STMN) Condition” procedure on page 2-87.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.128 LPBKFACILITY (STMN)

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

Logical Object: STMN

A Facility Loopback Active condition for an STM-N occurs on STM-16 cards when a software facility loopback is active for a port on the reporting card, and the facility entity is out of service.

Caution Before performing a facility loopback on an STM-16 card, make sure the card contains at least two section DCC paths to the node where the card is installed. A second section DCC path provides a nonlooped path to log into the node after the loopback is applied, thus enabling you to remove the facility loopback. Ensuring a second section DCC is not necessary if you are directly connected to the ONS 15600 SDH containing the loopback STM-N.

Clear the LBKFACILITY (STMN) Condition

Step 1 To remove the loopback facility condition, double-click the reporting card in node view.

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

Step 3 In the Loopback Type column, click the correct row for the port and choose **None** from the drop-down list.

Step 4 Click **Apply**.

Step 5 Click the **Provisioning > Line** tabs.

Step 6 In the Admin State column, click the correct row for the port and choose **Unlocked** from the drop-down list.

Note If ports managed into Unlocked administrative state are not receiving signals, the LOS alarm is either raised or remains, and the port service state transitions to Unlocked-disabled,failed.

Step 7 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.129 LPBKPAYLOAD

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

Logical Object: STMN

A Payload Loopback Active condition occurs on STM-64 cards when a software payload loopback is active for a port on the STM-64 card, and the facility entity is out of service.

Clear the LPBKPAYLOAD Condition

Step 1 To remove the loopback payload condition, double-click the reporting card in node view.

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

Step 3 In the Loopback Type column, click the correct row for the port and choose **None** from the drop-down list.

Step 4 Click **Apply**.

Step 5 Click the **Provisioning > Line** tabs.

Step 6 In the Admin State column, click the correct row for the port and choose **Unlocked** from the drop-down list.

Note If ports managed into Unlocked administrative state are not receiving signals, the LOS alarm is either raised or remains, and the port service state transitions to Unlocked-disabled,failed.

Step 7 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.130 LPBKTERMINAL (GIGE)

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

Logical Object: GIGE

A Loopback Terminal condition for a Gigabit Ethernet port occurs when a software terminal (inward) loopback is active for an ASAP card client SFP (PPM) provisioned at the ONE_GE port rate.

For information about troubleshooting these circuits with loopbacks, refer to the "1.3 Troubleshooting an Ethernet Circuit Path With Loopbacks" section on page 1-29].

Clear the LPBKTERMINAL (GIGE) Condition

Step 1 Complete the "Clear the LBKTERMINAL (STMN) Condition" procedure on page 2-89.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.131 LPBKTERMINAL (STMN)

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

Logical Object: STMN

A Terminal Loopback Active condition for STM-N occurs on STM-16 cards or ASAP cards when a software facility loopback is active for a port on the reporting card, and the facility entity is out of service.

Caution Before performing a terminal loopback on an STM-16 card, make sure the card contains at least two section DCC paths to the node where the card is installed. A second section DCC path provides a nonlooped path to log into the node after the loopback is applied, thus enabling you to remove the terminal loopback. Ensuring a second section DCC is not necessary if you are directly connected to the ONS 15600 SDH containing the loopback STM-N.

Clear the LBKTERMINAL (STMN) Condition

Step 1 To remove the loopback facility condition, double-click the reporting card in node view.

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

Step 3 In the Loopback Type column, click the correct row for the port and choose **None** from the drop-down list.

Step 4 Click **Apply**.

Step 5 Click the **Provisioning > Line** tabs.

Step 6 In the Admin State column, click the correct row for the port and choose **Unlocked** from the drop-down list.

Note If ports managed into Unlocked administrative state are not receiving signals, the LOS alarm is either raised or remains, and the port service state transitions to Unlocked-disabled,failed.

Step 7 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.132 LWBATVG

The LWBATVG condition is not used in this platform in this release. It is reserved for development.

2.6.133 MAN-REQ

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

Logical Object: VCMON-HP

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 2-122.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.134 MANRESET

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

Logical Objects: EQPT, PIM, PPM

A Manual System Reset condition occurs when you right-click a TSC card, SSXC card, or traffic (STM-N) card in CTC and choose Hard-reset Card or Soft-reset Card.

Note The hard-reset option is enabled only when the card is placed in the Locked-enabled,maintenance service state.

2.6.135 MANSWTOINT

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

Logical Object: NE-SREF

The Manual Synchronization Switch to Internal Clock condition occurs when the NE (node) timing source is manually switched to an internal timing source.

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

2.6.136 MANSWTOPRI

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

Logical Objects: EXT-SREF, NE-SREF

The Manual Synchronization Switch to Primary Reference condition occurs when the NE (node) timing source is manually switched to the primary source.

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

2.6.137 MANSWTOSEC

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

Logical Objects: EXT-SREF, NE-SREF

The Manual Synchronization Switch to Second Reference condition occurs when the NE (node) timing source is manually switched to a second source.

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

2.6.138 MANSWTOTHIRD

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

Logical Objects: EXT-SREF, NE-SREF

The Manual Synchronization Switch to Third Reference condition occurs when the NE (node) timing source is manually switched to a third source.

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

2.6.139 MANUAL-REQ-RING

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

Logical Object: STMN

The Manual Switch Request on Ring condition occurs when a user initiates a MANUAL RING command on a MS-SPRing ring to switch 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 MANUAL RING command originated is marked with an “M” on the network view detailed circuit map.

When you release the manual ring request, traffic automatically switches back to working—even if the ring is set to nonrevertive switching.

Clear the MANUAL-REQ-RING Condition

Step 1 Complete the “Clear a MS-SPRing External Switching Command” procedure on page 2-128.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.140 MANUAL-REQ-SPAN

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

Logical Object: STMN

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 a MS-SPRing External Switching Command" procedure on page 2-128.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.141 MATECLK

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

Logical Object: EQPT

The Mate Clock alarm occurs when the active TSC card cannot detect the clock from the standby TSC card.

Clear the MATECLK Alarm

Step 1 In CTC, check for any alarms that indicate that there are faulty clock references, such as the "HLDOVRSYNC" alarm on page 2-66 or the "FRNGSYNC" alarm on page 2-64, and resolve these alarms.

Step 2 If the MATECLK persists, complete the "Reset a Card with a Card Pull (Reseat)" procedure on page 2-131 for the standby TSC card and wait 15 minutes.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15600 SDH. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 3 If the MATECLK still persists, complete the "Replace a TSC Card" procedure on page 2-134 for the active TSC card, using the standby TSC card to replace the active TSC 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 call Cisco TAC (1-800-553-2447) to report a Service-Affecting (SA) problem.

2.6.142 MEA

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

Logical Objects: EQPT, PIM, PPM

The Mismatch Between Equipment Type and Provisioned Attributes alarm is reported against a card slot when the physical card or port does not match the card type provisioned in CTC. Deleting the incompatible card or port, SFP (PPM), or 4PIO (PIM) in CTC or physically removing the card clears the alarm.

Clear the MEA Alarm

Step 1 Physically verify the type of card that sits in the slot reporting the MEA alarm.

Step 2 In CTC, click the node view **Inventory** tab to display the provisioned card type.

Step 3 If you prefer the card type depicted by CTC, complete the "Replace an I/O Card" procedure on page 2-133 for the reporting card and replace it with the card type depicted by CTC (provisioned for that slot).

Note CTC does not allow you to delete a card if at least one port on the card is in service, has a path mapped to it, is paired in a working-protection scheme, has DCC enabled, or is used as a timing reference.

Step 4 If you want to leave the installed card in the slot but it is not in service, delete any circuits mapped to it. Refer to the "Manage Circuits" chapter in the *Cisco ONS 15600 SDH Procedure Guide* for procedures.

Step 5 Place the cursor over the provisioned card in CTC and right-click to choose **Delete Card**.

When the card is deleted in CTC, the card that physically occupies the slot automatically reboots and appears in CTC.

Step 6 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447) to report a Service-Affecting (SA) problem.

2.6.143 MEM-GONE

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

Logical Object: EQPT

The Memory Gone alarm occurs when data generated by software operations exceeds the memory capacity of the TSC card. The TSC 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.

2.6.144 MEM-LOW

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

Logical Object: EQPT

The Free Memory of Card Almost Gone alarm occurs when data generated by software operations is close to exceeding the memory capacity of the TSC 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 For assistance with this alarm, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.145 MFGMEM (CAP)

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

Logical Object: CAP

The Manufacturing Data Memory Failure CAP alarm occurs if the ONS 15600 SDH cannot access the data in the EEPROM on the backplane. MFGMEM is caused by EEPROM failure on the backplane, or fuse failure for the EEPROM.

The EEPROM stores manufacturing data that is needed for compatibility and inventory issues. If the alarm is accompanied by the "PWR-FA" alarm on page 2-102, the 5-VDC fuse for the EEPROM might be tripped. If that is the case, use the procedure below to eliminate the TSC card as the cause of the alarm, but do not attempt to troubleshoot it further. Contact the Cisco TAC at 1-800-553-2447.

Clear the MFGMEM Alarm on the CAP by Resetting the TSC Card

Step 1 Complete the "Soft-Reset a Card Using CTC" procedure on page 2-129.

Wait for the "FSTSYNC" condition on page 2-64 to clear.

Step 2 If the alarm does not clear, complete the "Soft-Reset a Card Using CTC" procedure on page 2-129.

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). The standby TSC card might also need replacement. If the alarm continues after both TSC cards have been replaced, the problem lies in the EEPROM on the CAP, and this must be replaced.

Step 3 When the alarm is cleared, you can make the standby TSC card active again by completing the "Soft-Reset a Card Using CTC" procedure on page 2-129.

2.6.146 MFGMEM (FAN)

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

Logical Object: FAN

The Manufacturing Data Memory Fan alarm occurs if the ONS 15600 SDH EEPROM on a fan tray fails. MFGMEM can be accompanied by the "FAN-FAIL" alarm on page 2-56.

Clear the MFGMEM (FAN) Alarm

Step 1 Pull out the fan tray.

Step 2 Reinsert the fan trays, making sure you can hear the fans start operating. Fans should run immediately when correctly inserted.

Step 3 If a fan does not run or the alarm persists, refer to the "Maintain the Node" chapter in the *Cisco ONS 15600 SDH Procedure Guide* for instructions to replace the fan tray.

Step 4 If a replacement fan tray does not operate correctly, 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.

2.6.147 MFGMEM (for the PIM, PPM, SSXC, Traffic Card, or TSC Card)

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

Logical Objects: EQPT, PIM, PPM

The Manufacturing Data Memory Failure SSXC, Traffic (STM-N), or TSC Card alarm occurs if the ONS 15600 SDH EEPROM on one of these cards fails.

Clear the MFGMEM Alarm (for the PIM,PPM, SSXC, Traffic Card, or TSC Card)

Step 1 If the alarm is reported against a TSC card, troubleshoot with the "Clear the MFGMEM Alarm on the CAP by Resetting the TSC Card" procedure on page 2-94.

Step 2 If the reporting card is an active traffic line port in a 1+1 protection group or an SNCP, ensure that an APS traffic switch has occurred to move traffic to the protect port.

- A SNCP APS is identified by an AUTOSW-type alarm or condition (such as AUTOSW-AIS, AUTOSW-PDI, AUTOSW-SDBER, AUTOSW-SFBER, or AUTOSW-UNEQ).
- A 1+1 APS is identified on the node view Maintenance > Protection tab. If you click the protection group, under the Selected Group list, the ports are designated as Working/Standby and Protect/Active.

Step 3 If the reporting port is part of an SNCP, complete the "Initiate a Force Switch for All Circuits on a SNCP Span" procedure on page 2-124. If the port is part of a 1+1 protection group, complete the "Initiate a 1+1 Protection Port Force Switch Command" procedure on page 2-122.

Step 4 If the reporting card is a SSXC card and an automatic switch to the preferred copy SSXC card occurred, traffic automatically switches to the alternate copy.

Complete a "Hard-Reset a Card Using CTC" procedure on page 2-129 for the reporting card (or "Soft-Reset a Card Using CTC" procedure on page 2-129 for the SSXC.

Step 5 If the reset does not clear the alarm, complete the "Reset a Card with a Card Pull (Reseat)" section on page 2-131 for the TSC card, or complete the "Request a Cross-Connect Card Preferred Copy Switch" section on page 2-130 for the SSXC.

Step 6 If the physical reseat of the card or switch does not clear the alarm, complete the appropriate procedure in the "Replace a TSC Card" section on page 2-134 or "Replace an SSXC Card" section on page 2-132 as needed.

Note If the traffic (STM-N) card is implicated and you are able to continue using the traffic card with one port out of service, perform a bridge and roll to move the port traffic to a free port using the "Bridge and Roll Traffic" procedure in the "Manage Circuits" chapter in the *Cisco ONS 15600 SDH Procedure Guide*. Label the bad port, and place it out of service until such time as the card can be replaced.

Step 7 If the MFGMEM alarm continues to report after you replaced the card, the problem lies in the EEPROM. Log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

Step 8 If the alarm clears and it was reported by a traffic card, traffic reverts to the working port if an automatic switch occurred. If traffic was manually switched in a 1+1 protection group, revert traffic to the original port by completing the "Clear a 1+1 Protection Port Force or Manual Switch Command" procedure on page 2-123. If traffic was manually switched in an SNCP, revert traffic to the original path by completing the "Clear a SNCP Span External Switching Command" procedure on page 2-126.

If an automatic switch to the alternate copy SSXC card occurred, traffic is automatically restored to the preferred copy.

Step 9 If the reporting card is a TSC card and you want to make the standby TSC card active again, complete the "Soft-Reset a Card Using CTC" procedure on page 2-129.

2.6.148 MS-AIS

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

Logical Object: 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 2-15.

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.

2.6.149 MS-DEG

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

Logical Object: STMN

The Multiplex Section Signal Degrade condition occurs when the multiplex section overhead of the STMN object falls within the degrade threshold set on the node.

Clear the MS-DEG Condition

Step 1 Determine the threshold. 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 2 Verify the input fiber cable connections to the reporting card.

Step 3 Clean the input fiber cable ends according to site practice.

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.

2.6.150 MS-EOC

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

Logical Object: STMN

The MS-DCC Termination Failure alarm occurs when the ONS 15600 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 15600 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 2-42.

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.

2.6.151 MS-EXC

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

Logical Object: STMN

The Multiplex Section Excessive Errors condition occurs when the multiplex section overhead of the STM1E object falls past the fail threshold set on the node.

Clear the MS-EXC Condition

Step 1 Determine the threshold. 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 2 Verify the input fiber cable connections to the reporting card.

Step 3 Clean the input fiber cable ends according to site practice.

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.

2.6.152 MS-RFI

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

SDH Logical Objects: STMN

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 15600 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 15600 SDH.

Step 2 Determine whether there are other alarms, especially the "LOS (STMN)" alarm on page 2-84.

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.

2.6.153 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 TSC 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 TSC 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.

2.6.154 MS-SQUELCH-HP

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

SDH Logical Object: STMN

The Multiplex Section Ring is Squelching High-Order Path Traffic condition is raised on an STM-N facility. If the node failure scenario includes the source node, the node that drops the signal will squelch traffic. The condition resolves when the node recovers.

This condition is raised with an NA severity by default. However, it indicates that traffic is squelched due to node failure (traffic outage). Traffic outages can be caused by different problems, such as multiple LOS alarms, MS-AIS, or node power outages. MS-SQUELCH-HP is symptomatic and indicates that the user must investigate which node in a ring is being isolated and what is causing the node isolation.

Note MS-SQUELCH-HP is an informational condition.

2.6.155 NOT-AUTHENTICATED

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

Logical Object: SYSTEM

The NOT-AUTHENTICATED alarm is raised by CTC (not by the NE) when 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 2-75 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.

2.6.156 NON-CISCO-PPM

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

Logical Object: PPM

The Non-Cisco PPM Inserted condition occurs when a PPM that is plugged into a card's port fails the security code check. The check fails when the PPM used is not a Cisco PPM.

Clear the NON-CISCO-PPM Condition

Step 1 Obtain the correct Cisco PPM and replace the existing PPM with the new one.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.157 OPEN-SLOT

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

Logical Object: EQPT

The OPEN-SLOT alarm indicates that one of the I/O slots (Slot 1 through 4 and 11 through 14) does not contain a traffic card or filler card.

Clear the OPEN-SLOT Alarm

Step 1 Insert a filler card or STM-N card into the empty slot.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.158 PRC-DUPID

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

Logical Object: STMN

The Procedural Error Duplicate Node ID alarm indicates that two identical node IDs exist in the same MS-SPRing. The ONS 15600 SDH requires each node in the MS-SPRing to have a unique node ID.

Clear the PRC-DUPID Alarm

Step 1 Log into a node on the ring.

Step 2 Find the node ID by completing the "Identify an MS-SPRing Ring ID or Node ID Number" procedure on page 2-120.

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 2-121 so that each node ID is unique.

Step 5 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.159 PROV-MISMATCH

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

Logical Object: PPM

The Provisioning Mismatch for an SFP alarm is raised against an SFP (PPM) connector on the ASAP card under one of the following circumstances:

- The physical SFP (PPM) range or wavelength does not match the provisioned value. PPMs (SFPs) have static wavelength values which must match the wavelengths provisioned for the port.
- The SFP (PPM) reach (loss) value does not meet the reach value needed for the port.

Clear the PROV-MISMATCH Alarm

Step 1 Determine what the SFP (PPM) wavelength range should be by viewing the frequency provisioned for the card by completing the following steps:

a. Double-click the card to display the card view.

b. Click the **Provisioning > Optical** tabs (or **Ethernet** tab, as appropriate).

c. Record the values shown in the **Reach** and **Wavelength** columns.

Step 2 Complete the "Replace an ASAP SFP (PPM) Module" procedure on page 2-137.

Step 3 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.160 PWR

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

Logical Object: PWR

The NE Power Failure at Connector 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 alarm is necessary for troubleshooting.

Effects of this alarm depend upon the shutdown order of the two power supplies. If PWR B of the right-side power feed and PWR A of the left-side power feed are shut down, this causes all three fans to turn off and a "FAN-FAIL" alarm on page 2-56 to be raised. In this case, after power is restored all three fans work in high-speed mode for a few minutes until CTC returns them to normal speed. All alarms are cleared.

Clear the PWR Alarm

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

Step 2 Remove the power cable from the faulty supply. For instructions, refer to the "Install the Bay and Backplane Cable" chapter in the *Cisco ONS 15600 SDH Procedure Guide* and reverse the power cable installation procedure.

Step 3 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.161 PWR-FA

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

Logical Object: BPLANE

The Backplane Power Fuse Failure alarm indicates that the backplane EEPROM memory 5-VDC fuse fails, but the equipment is still in service. Service is not currently affected, but network management can be affected because the ONS 15600 SDH system uses a default NE (node) IP address instead of a programmed one in this case. This alarm might be accompanied by the "INVMACADR" alarm on page 2-75, which appears in the alarm history when network management capability is restored.

Do not attempt to troubleshoot the alarm. 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).

2.6.162 PWR-FAIL-A

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

Logical Objects: CAP, 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 CAP, SSXC card, traffic (STM-N) cards, or TSC card.

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 one of the following actions depending what kind of card reported it:

- If the reporting card is an active traffic line port in a 1+1 protection group or part of an SNCP, ensure that an APS traffic switch has occurred to move traffic to the protect port.
  - A SNCP APS is identified by an AUTOSW-type alarm or condition (such as AUTOSW-AIS, AUTOSW-PDI, AUTOSW-SDBER, AUTOSW-SFBER, or AUTOSW-UNEQ).
  - A 1+1 APS is identified on the node view Maintenance > Protection tab. If you click the protection group, under the Selected Group list, the ports are designated as Working/Standby and Protect/Active.
  - If the reporting port is part of an SNCP, complete the "Initiate a Force Switch for All Circuits on a SNCP Span" procedure on page 2-124. If the port is part of a 1+1 protection group, complete the "Initiate a 1+1 Protection Port Force Switch Command" procedure on page 2-122. Continue with Step 3.
- If an automatic switch to the alternate copy SSXC card occurred, the SSXC card can be serviced. If the switch has not occurred, complete the "Request a Cross-Connect Card Preferred Copy Switch" procedure on page 2-130. Continue with Step 3.

To determine which SSXC card is the preferred copy and if it is currently being used, open the node view Maintenance > Preferred Copy window. The Data Copy area Preferred field shows Copy A or Copy B. The Currently Used field shows the copy being used.

Note In CTC, Copy A refers to the SSXC card in Slot 6/7. Copy B refers to the SSXC card in Slot 8/9. Either copy might be chosen as the preferred copy SSXC card. The other SSXC card is called the alternate SSXC card in this chapter.

Step 2 Complete the "Soft-Reset a Card Using CTC" procedure on page 2-129 for the reporting card.

Step 3 If the alarm does not clear, complete the "Reset a Card with a Card Pull (Reseat)" procedure on page 2-131.

Step 4 Check the pins on the backplane connector, including the power pins on the edge of the card. Also inspect the pins on the backplane. A bent pin can cause power failure.

Caution If a backplane pin is bent, do not insert another card in the slot until the problem is remedied.

Step 5 If the alarm does not clear, complete the "Replace an SSXC Card" procedure on page 2-132, "Replace an I/O Card" procedure on page 2-133, or "Replace a TSC Card" procedure on page 2-134 as needed.

Step 6 If the single card reseat and replacement does not clear the alarm, or if multiple cards report the alarm, verify the office power; refer to the "Install the Bay and Backplane Connections" chapter in the *Cisco ONS 15600 SDH Procedure Guide* for power installation instructions.

Step 7 If the alarm does not clear, reseat the power cable connection to the connector. For more information about ONS 15600 SDH power connections, refer to the "Install the Bay and Backplane Connections" chapter in the *Cisco ONS 15600 SDH Procedure Guide*.

Step 8 If the alarm does not clear, physically replace the power cable connection to the connector.

Step 9 If the alarm does not clear, a problem with the power distribution unit (PDU) is indicated and it could need to be replaced. Complete the procedure located in the "Maintain the Node" chapter in the *Cisco ONS 15600 SDH Procedure Guide*.

Step 10 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

Step 11 If the alarm clears and it was reported by a traffic (STM-N) card, traffic reverts to the working port if an automatic switch occurred. If traffic was manually switched to a 1+1 protect port, revert traffic by completing the "Clear a 1+1 Protection Port Force or Manual Switch Command" procedure on page 2-123. If traffic was manually switched in an SNCP, revert traffic to the original path by completing the "Clear a SNCP Span External Switching Command" procedure on page 2-126.

Step 12 If the alarm was reported by a SSXC card and an automatic switch to the alternate copy SSXC card occurred, traffic is automatically restored to the preferred copy.

Step 13 If the reporting card was reported by a TSC card and you want to make the standby card active, complete the "Soft-Reset a Card Using CTC" procedure on page 2-129.

2.6.163 PWR-FAIL-B

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

Logical Objects: CAP, 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 CAP, SSXC card, traffic (STM-N) cards, or TSC card.

Troubleshoot this alarm with the "Clear the PWR-FAIL-A Alarm" procedure on page 2-102.

2.6.164 PWR-FAIL-RET-A

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

Logical Object: EQPT

The Equipment Power Failure at Power Return A alarm occurs when the main power return path is not available. This alarm occurs on the TSC card, SSXC card, or traffic (STM-N) cards. Troubleshoot using the "Clear the PWR-FAIL-A Alarm" procedure on page 2-102.

2.6.165 PWR-FAIL-RET-B

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

Logical Object: EQPT

The Equipment Power Failure at Power Return B alarm occurs when the main power return path is not available. This alarm occurs on the TSC card, SSXC card, or traffic (STM-N) cards.

Troubleshoot using the "Clear the PWR-FAIL-A Alarm" procedure on page 2-102.

2.6.166 PWRRESTART

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

Logical Object: EQPT

The Power-Up Restart condition occurs when the shelf is restarted while no CTC connection is present. The Slot 5 TSC card on the shelf does not report this condition because the card is inactive when the condition occurs. You can see this condition in the Alarm History window when the CTC connection resumes.

2.6.167 RING-MISMATCH

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

Logical Object: STMN

At least one node in the MS-SPRing has an incorrect node ID. The RING-MISMATCH alarm clears when all nodes in the MS-SPRing have the correct node IDs.

Clear the RING-MISMATCH Alarm

Step 1 Complete the "Identify an MS-SPRing Ring ID or Node ID Number" procedure on page 2-120 to verify each node's ID number.

Step 2 Repeat Step 1 for all nodes in the ring.

Step 3 If one node has an incorrect node ID number, complete the "Change an MS-SPRing Node ID Number" procedure on page 2-121 to change one node's ID number so that each node ID is unique.

Step 4 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.168 RING-SW-EAST

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

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 and does not require troubleshooting.

2.6.169 RING-SW-WEST

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

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 and does not require troubleshooting.

2.6.170 ROLL

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

Logical Object: VCMON-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.

2.6.171 ROLL-PEND

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

Logical Object: VCMON-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.

2.6.172 RS-EOC

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

SDH Logical Objects: STMN

DWDM Logical Object: TRUNK

The SDH Data Communications Channel (DCC) Termination Failure alarm occurs when the ONS 15600 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 15600 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 information about DWDM cards, refer to the *Cisco ONS 15454 DWDM Reference Manual*.

Clear the RS-EOC Alarm

Step 1 If the "LOS (STMN)" alarm on page 2-84 is also reported, complete the "Clear the LOS (STMN) Alarm" procedure on page 2-84.

Step 2 If the "LOF (STMN)" condition on page 2-81 is reported, complete the "Clear the LOF (STMN) Alarm" procedure on page 2-81.

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 15600 SDH Procedure Guide*. For more information about OSCM fiber connections and terminations, refer to the *Cisco ONS 15454 DWDM Troubleshooting Guide*.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15600 SDH. Plug the wristband cable into the ESD jack located lower-right edge of the shelf assembly.

If the physical connections are correct and configured to carry DCC traffic, ensure that both ends of the fiber span have unlocked ports. Verify that the ACT/SBY LED on each card is green.

Step 4 When the LEDs on the cards are correctly illuminated, complete the "2.8.5 Verify or Create Node DCC Terminations" procedure on page 2-138 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 **Locked**.

e. If the **Admin State** column lists the port as Locked,maintenance or Locked,disabled, click the column and click **Locked** from the drop-down list. Click **Apply**.

Note If a port in the unlocked admin state does not receive a signal, the LOS alarm is raised and the port service state transitions to Locked-disabled, automaticInService & failed.

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 "2.8.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-121 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 "1.9.3 Optical Traffic Card Transmit and Receive Levels" section on page 1-76 for non-DWDM card levels and refer to the *Cisco ONS 15454 DWDM Reference Manual* for 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 15600 SDH Procedure Guide*.

Step 10 If fiber connectors are properly fastened and terminated, complete the "Soft-Reset a Card Using CTC" procedure on page 2-129.

Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card.

Resetting the active TSC card switches control to the standby TSC card. If the alarm clears when the ONS 15600 SDH node switches to the standby TSC card, the user can assume that the previously active card is the cause of the alarm.

Step 11 If the TSC 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 15600 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 "Reset a Card with a Card Pull (Reseat)" procedure on page 2-131. If the Technical Support technician tells you to remove the card and reinstall a new one, follow the "Replace a TSC Card" procedure on page 2-134.

2.6.173 SFTWDOWN

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

Logical Object: EQPT

A Software Download in Progress condition occurs when a TSC card is downloading or transferring software. No action is necessary. Wait for the transfer or the software download to complete. If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

Note It takes approximately 20 minutes for the active TSC card to transfer the system software to the newly installed TSC card. Software transfer occurs in instances where different software versions exist on the two cards. When the transfer completes, the TSC card reboots and goes into standby mode after approximately three minutes.

Note If the active and standby TSC cards have the same versions of software, it takes approximately three minutes for software to be updated on a standby TSC card.

2.6.174 SNTP-HOST

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

Logical Object: NE

The Simple Network Timing Protocol (SNTP) Host Failure alarm indicates that an ONS 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 forwarding failure can result from two causes, either 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 "Ping the ONS 15600" procedure on page 1-59.

Step 2 If the ping fails, contact the network administrator who manages the IP network that supplies the SNTP information to the proxy and determine whether the network is experiencing problems which might affect the SNTP server/router connecting to the proxy ONS 15600 SDH.

Step 3 If no network problems exist, ensure that the ONS 15600 SDH proxy is provisioned correctly by completing the following steps:

a. In node view for 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, click it.

d. Ensure that the Use NTP/SNTP Server field contains a valid IP address for the server.

Step 4 If proxy is correctly provisioned, refer to the "Management Network Connectivity" chapter in the *Cisco ONS 15600 SDH Reference Manual* for more information on SNTP Host.

Step 5 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.175 SSM-DUS

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

Logical Objects: BITS, STMN

The Synchronization Status Messaging (SSM) Changed to Do Not Use (DUS) condition occurs when the synchronization status message quality level changes to DUS.

The port that reports the condition is not at fault. The condition applies to the timing source. SSM-DUS prevents timing loops by providing a termination point for the signal usage.

2.6.176 SSM-FAIL

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

Logical Objects: BITS, STMN

The SSM Failed to Receive Synchronization alarm occurs when SSM received by the ONS 15600 SDH fails. The problem is external to the ONS 15600 SDH. If one of two sources fails, the alarm is Minor (MN). If there is no backup source, the alarm is Major (MJ). This alarm indicates that although the ONS 15600 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 whether the external timing source is delivering SSM; refer to the "Create Circuits" chapter in the *Cisco ONS 15600 SDH Procedure Guide* for circuit test procedures.

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).

2.6.177 SSM-OFF

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

Logical Objects: BITS, STMN

The SSM Changed to Off condition occurs when SSM is disabled by a user.

SSM communicates information about the quality of the timing source. SSM is carried on the S1 byte of the SDH line layer. It enables SDH devices to automatically select the highest quality timing reference and to avoid timing loops. Troubleshoot with the "Clear the SSM-FAIL Alarm" procedure on page 2-110 if desired.

2.6.178 SSM-RES

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

Logical Objects: BITS

The SSM Quality Level Changed to Reserved (RES) condition occurs when the synchronization message quality level changes to RES.

2.6.179 SSM-SMC

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

Logical Objects: BITS, NE-SREF, STMN

The SSM Quality Level Changed to SDH Minimum Clock Traceable (SMC) condition occurs when the synchronization message quality level changes to SMC.

2.6.180 SSM-STU

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

Logical Objects: BITS, NE-SREF, STMN

The SSM Synchronization Traceability Unknown condition occurs when the reporting node is timed to a reference that does not support SSM, but the ONS 15600 SDH has SSM support enabled. SSM-STU can also be raised if the timing source is sending out SSM messages but SSM is not enabled on the ONS 15600 SDH.

Clear the SSM-STU Condition

Step 1 Click the node view **Provisioning > Timing > BITS Facilities** tabs.

Step 2 If the Sync. Messaging Enabled check box is checked, click the box to deselect it.

Step 3 If the Sync. Messaging Enabled check box is unchecked, click the box to select it.

Step 4 Click **Apply**.

Step 5 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.181 SWTOPRI

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

Logical Objects: EXT-SREF, NE-SREF

The Synchronization Switched to Primary Reference condition occurs when the ONS 15600 SDH switches to the primary timing source (reference 1). The ONS 15600 SDH uses three ranked timing references. The timing references are typically two BITS-level or line-level sources and an internal reference.

2.6.182 SWTOSEC

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

Logical Objects: EXT-SREF, NE-SREF

The Synchronization Switched to Second Reference condition occurs when the ONS 15600 SDH has switched to a second timing source (reference 2). To clear the SWTOSEC condition, complete the "Clear the SYNCPRI Alarm" procedure on page 2-113.

2.6.183 SWTOTHIRD

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

Logical Objects: EXT-SREF, NE-SREF

The Synchronization Switched to Third Reference condition occurs when the ONS 15600 SDH has switched to a third timing source (reference 3). To clear the SWTOTHIRD condition, complete the "Clear the SYNCPRI Alarm" procedure on page 2-113.

2.6.184 SW-VER

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

Logical Object: EQPT

The Software Version condition is reported when a new software version is activated on the ONS 15600 SDH. When a new version of software is uploaded, it results in the active TSC card running the new version and the standby TSC card running the old version. This situation raises the SW-VER condition. It remains until the user accepts the new version in the CTC. The acceptance causes the standby TSC card to reboot and upload the new version.

If the user does not accept the version, the active TSC card switches to the standby TSC card with the original version. After the switch, the new standby TSC card reverts to the previous version.

2.6.185 SYNCCLK

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

Logical Object: NE

A Synchronization Clock Unavailable alarm occurs when both TSC cards lose their timing function.

Clear the SYNCCLK Alarm

Step 1 From node view, click the **Provisioning > Timing > General** tabs.

Step 2 Check the current configuration for REF-1 of the NE Reference.

Step 3 If the primary reference is a BITS input, complete the "Clear the LOF (BITS) Alarm" procedure on page 2-80.

Step 4 If the primary reference clock is an incoming port on the ONS 15600 SDH, complete the "Clear the LOF (STMN) Alarm" procedure on page 2-81.

Step 5 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.186 SYNC-FREQ

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

Logical Objects: BITS, STMN

The Synchronization Reference Frequency Out of Bounds alarm occurs when the synchronization frequency reference for the NE (node) is not within acceptable boundaries.

Clear the SYNC-FREQ Alarm

Step 1 Verify that the internal or BITS timing reference is stable. The timing reference is located on the active TSC card. Check for any alarms against this card and troubleshoot them.

Step 2 If the alarm does not clear, complete the "Soft-Reset a Card Using CTC" procedure on page 2-129.

Step 3 If the alarm clears, complete the "Replace a TSC Card" procedure on page 2-134.

Note It takes approximately 20 minutes for the active TSC card to transfer the system software to the newly installed TSC card. Software transfer occurs in instances where different software versions exist on the two cards. When the transfer completes, the TSC card reboots and goes into standby mode after approximately three minutes.

Note If the active and standby TSC cards have the same versions of software, it takes approximately three minutes for software to be updated on a standby TSC card.

Step 4 If the SYNC-FREQ alarm continues to report after replacing the TSC card, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.187 SYNCPRI

Default Severity: Minor (MN), Non-Service-Affecting (NSA) for EXT-SREF; Major (MJ), Service-Affecting (SA) for NE-SREF

Logical Objects: EXT-SREF, NE-SREF

A Primary Synchronization Reference Failure alarm occurs at the NE (node) level when the ONS 15600 SDH loses the primary timing source (reference 1). The ONS 15600 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 15600 SDH should switch to its second timing source (reference 2). This switch also triggers the SWTOSEC alarm.

Clear the SYNCPRI Alarm

Step 1 From node view, click the **Provisioning > Timing > General** tabs and identify the timing source in REF-1 of the NE Reference.

Step 2 If REF-1 is Internal, this refers to the active TSC card. Look for any alarms related to the TSC card and troubleshoot them.

Step 3 If REF-1 is BITS, follow the "Clear the LOF (BITS) Alarm" procedure on page 2-80.

Step 4 If the primary reference clock is an incoming port on the ONS 15600 SDH, follow the "Clear the LOF (STMN) Alarm" procedure on page 2-81.

Step 5 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.188 SYNCSEC

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

Logical Objects: EXT-SREF, NE-SREF

A Second Synchronization Reference Failure Alarm occurs at the NE (node) level when the ONS 15600 SDH loses the second timing source (reference 2). If SYNCSEC occurs, the ONS 15600 SDH should switch to a third timing source (reference 3) to obtain valid timing for the ONS 15600 SDH. This switch also triggers the "SWTOTHIRD" condition on page 2-112.

Clear the SYNCSEC Alarm

Step 1 From node view, click the **Provisioning > Timing > General** tabs.

Step 2 Check the current configuration of REF-2 for the NE Reference.

Step 3 If the second reference is a BITS input, follow the "Clear the LOS (BITS) Alarm" procedure on page 2-84.

Step 4 If the second timing source is an incoming port on the ONS 15600 SDH, follow the "Clear the LOF (STMN) Alarm" procedure on page 2-81.

Step 5 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.189 SYNCTHIRD

The SYNCTHIRD condition is not used in this platform in this release. It is reserved for development.

2.6.190 SYSBOOT

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

Logical Object: NE

The System Reboot alarm indicates that new software is booting on the node or shelf TSC card. No action is required. The alarm clears when all cards finish rebooting the new software. The reboot takes approximately three minutes.

2.6.191 TPTFAIL

The TPTFAIL alarm for packet over SDH (POS) is not used in this platform in this release. It is reserved for development.

2.6.192 UNPROT-SYNCCLK

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

Logical Object: NE

The Unprotected Synchronization or Clock Equipment alarm indicates that only one TSC card has acquired the primary timing reference. The alarm is reported if there is no standby TSC card, or if the standby TSC card has restarted and 700 seconds (in FSTSYNC mode) have not elapsed.

This condition is normal following a change to the system timing reference (such as BITS to Line or Line to BITS). Changing the clock reference causes both TSC cards to raise the "FSTSYNC" condition on page 2-64, for 700 seconds. The UNPROT-SYNCCLK alarm occurs during this period. If both TSC cards are reset within 700 seconds of each other, this alarm occurs also and remains until both TSC cards attains the clock reference. If the alarm does not clear, follow the "Clear the UNPROT-SYNCCLK Alarm" procedure on page 2-115.

Clear the UNPROT-SYNCCLK Alarm

Step 1 Determine whether one or both TSC cards have the "FSTSYNC" condition on page 2-64 raised. If either TSC card has a FSTSYNC condition, wait 700 seconds for the condition and the UNPROT-SYNCCLK alarm to clear.

Step 2 If FSTSYNC was reported and continues after 700 seconds, replace the standby TSC card. Continue with Step 7.

Step 3 If FSTSYNC is not reported, from node view, click the **Provisioning > Timing > General** tabs.

Step 4 Verify the current configuration for REF-1 of the NE Reference.

If the primary reference clock is an incoming port on the ONS 15600 SDH, follow the "Clear the LOF (STMN) Alarm" procedure on page 2-81.

Step 5 If no protect TSC card is installed, install one. Refer to the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15600 SDH Procedure Guide* for instructions.

Step 6 If the alarm persists, remove and reinsert (reseat) the standby TSC card by completing the following steps and wait 700 seconds for the TSC card to acquire the reference.

a. Open the card ejectors.

b. Slide the card out of the slot.

c. Slide the card into the slot along the guide rails.

d. Close the ejectors.

Step 7 If the alarm reappears after you perform the switch, complete the "2.8.5 Verify or Create Node DCC Terminations" procedure on page 2-138 on the standby TSC card and wait 700 seconds for the TSC card to acquire the reference.

Note It takes approximately 20 minutes for the active TSC card to transfer the system software to the newly installed TSC card. Software transfer occurs in instances where different software versions exist on the two cards. When the transfer completes, the TSC card reboots and goes into standby mode after approximately three minutes.

Note If the active and standby TSC cards have the same versions of software, it takes approximately three minutes for software to be updated on a standby TSC card.

2.6.193 UNPROT-XCMTX

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

Logical Object: NE

The Unprotected Cross-Connection Matrix Equipment alarm indicates that only one functional SSXC card on the node supports the cross-connection. The alarm clears if the redundant SSXC card is installed. This alarm could be accompanied by the "IMPROPRMVL (EQPT for the SSXC or TSC Card)" alarm on page 2-72 or the "EQPT (EQPT)" alarm on page 2-44.

Clear the UNPROT-XCMTX Alarm

Step 1 If there is no protect SSXC card installed, install one.

Allow the newly installed SSXC card to boot.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.194 UNQUAL-PPM

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

SDH Logical Objects: PPM

The Unqualified PPM Inserted condition occurs when a PPM with a nonqualified product ID is plugged into the card's port; that is, the PPM passes the security code check as a Cisco PPM but is not qualified for use on the particular card.

Clear the UNQUAL-PPM Condition

Step 1 Obtain the correct Cisco PPM and replace the existing PPM with the new one.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.195 UNROUTEABLE-IP

The UNROUTEABLE-IP is not used in this platform in this release. It is reserved for development.

2.6.196 UPGRADE

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

Logical Object: NE

The System Upgrade in Progress condition indicates that a system upgrade is occurring on the TSC card.

When software is downloaded, it is loaded into the available code volume on the active TSC card. The software is copied to the available code volume on the standby TSC card next. The "SFTWDOWN" condition on page 2-108 occurs at that time. When the user activates the load, the UPGRADE condition occurs.

Note Whenever TSC cards are changed from active to standby, it takes approximately 12 minutes to completely synchronize to the timing source because the Stratum 3E timing module is being adopted.

2.6.197 VOLT-MISM

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

Logical Object: PWR

The Power Monitoring Mismatch Between Control Cards alarm is raised against the shelf when the power voltages of both TSC 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 15600 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).

2.6.198 WKSWPR

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

Logical Objects: VCMON-HP

The Working Switched To Protection condition occurs when a line has a failure, the "LOS (STMN)" alarm on page 2-84 or the "MS-DEG" condition on page 2-96.

This condition is also raised when you use the FORCE RING, FORCE SPAN, or MANUAL SPAN command at the network level. WKSWPR is visible on the network view Alarms, Conditions, and History tabs.

Clear the WKSWPR Condition

Step 1 Complete the "Clear the LOF (STMN) Alarm" procedure on page 2-81. (It is also used for LOS.)

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1-800-553-2447).

2.6.199 WTR

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

Logical Objects: STMN, VCMON-HP

The Wait to Restore condition indicates that revertive switching is specified and that a switch to protection occurred. When the working path is viable, this condition occurs while the wait to restore timer has not expired. The condition clears when the timer expires and traffic switches back to the working path.

2.6.200 XCMTX

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

Logical Object: NE

The Unavailable Cross-Connection Matrix Equipment alarm indicates no cross-connection matrix on the NE (node). If there was previously a single SSXC card running in unprotected mode, that card fails. If there were two cards running in protected mode, the matrix has become unavailable on both. Troubleshoot with the "Clear the UNPROT-XCMTX Alarm" procedure on page 2-116.

2.7 LED Behavior

The following the subsections describe LED behaviors of the TSC card, SSXC card, and STM-N cards.

2.7.1 TSC Card-Level Indicators

Table 2-13 lists typical card-level TSC card LED behaviors.

Table 2-13 TSC Card-Level Indicators

Indicator LED	Color	Definition
STAT	Red	Indicates a hardware fault; this LED is off during normal operation. Replace the card if the STAT LED persists. During diagnostics, the LED flashes quickly during initialization and slowly during configuration synchronization.
SRV	Green	The service mode of the card; green indicates that the card is in use and no light indicates that the card can be removed for service.
ACT/STBY	Green	The ACT/STBY (Active/Standby) LED indicates that the TSC card is active (green) or standby (off). It is not present on the optical cards.

2.7.2 TSC Card Network-Level Indicators

Table 2-14 lists typical network-level TSC card LED behaviors.

Table 2-14 TSC Card Network-Level Indicators

Indicator LED	Color	Definition
LINE	Green	Node timing is synchronized to a line timing reference.
EXTERNAL	Green	Node timing is synchronized to an external timing reference.
FREE RUN	Green	The node is not using an external timing reference. Indicated when the timing mode is set to an internal reference or after all external references are lost.
HOLDOVER	Amber	External/line timing references have failed. The TSC card has switched to internal timing and the 24-hour holdover period has not elapsed.
ACO	Amber	The alarm cutoff (ACO) push button has been activated. After pressing the ACO button, the amber ACO LED turns on. The ACO button opens the audible closure on the backplane. The ACO state is stopped if a new alarm occurs. After the originating alarm is cleared, the ACO LED and audible alarm control are reset.

2.7.3 SSXC Card-Level Indicators

Table 2-15 describes the functions of the card-level LEDs on the SSXC card faceplate.

Table 2-15 SSXC Card-Level Indicators

Indicators LED	Color	Definition
STAT	Red	Indicates a hardware fault; this LED is off during normal operation. Replace the card if the STAT LED persists. During diagnostics, the LED flashes quickly during initialization and flashes slowly during configuration synchronization.

Table 2-15 SSXC Card-Level Indicators (continued)

Indicators LED	Color	Definition
SRV	Green	The service mode of the card. Green indicates the card is in use; no light indicates that the card can be removed for service.
	Amber	The service mode of the card. Amber indicates the card is in use; no light indicates that the card can be removed for service.

2.7.4 STM-N Card Indicators

Table 2-16 describes the functions of the card-level LEDs on the STM-16 and STM-64 cards.

Note STM-N card SF and SD card-level LEDs are not displayed in CTC.

Table 2-16 STM-N Card-Level Indicators

Indicators	Color	Description
STAT LED	Red	Indicates a hardware fault; this LED is off during normal operation. Replace the card if the STAT LED persists. During diagnostics, the LED flashes quickly during initialization and flashes slowly during configuration synchronization.
SRV LED	Green	The service mode of the card; green indicates that the card is in use and no light indicates that the card can be removed for service.
LASER ON	Green	The green LASER ON LED indicates that at least one of the card's lasers is active.

2.8 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 more detailed procedures in the *Cisco ONS 15600 SDH Procedure Guide*.

2.8.1 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 ID or Node ID Number

Step 1 In node view, click **View > Go to Network View**.

Step 2 Click the **Provisioning > MS-SPRing** tabs.

Step 3 From the Ring ID column, record the Ring ID, 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.

Change an MS-SPRing Ring ID Number

Step 1 In node view, click **View > Go to Network View**.

Step 2 Click the **Provisioning > MS-SPRing** tabs.

Step 3 Highlight the ring and click **Edit**.

Step 4 In the MS-SPRing window, enter the new ID in the Ring ID field.

Step 5 Click **Apply**.

Step 6 Click **Yes** in the Changing Ring ID dialog box.

Change an MS-SPRing Node ID Number

Step 1 In node view, click **View > Go to Network View**.

Step 2 Click the **Provisioning > MS-SPRing** tabs.

Step 3 Highlight the ring and click **Edit**.

Step 4 In the MS-SPRing window, right-click the node on the ring map.

Step 5 Select **Set Node ID** from the shortcut menu.

Step 6 Enter the new ID in the field.

Step 7 Click **Apply**.

Verify Node Visibility for Other Nodes

Step 1 In node view, click the **Provisioning > MS-SPRing** tabs.

Step 2 Highlight an MS-SPRing.

Step 3 Click **Ring Map**.

Step 4 Verify that each node in the ring appears on the ring map with a node ID and IP address.

Step 5 Click **Close**.

2.8.2 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 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 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 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 that 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 that you want to clear.

Step 3 In the Selected Group list, click the card that 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 Force Switch for All Circuits on a SNCP Span

This procedure forces all circuits in a 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 a 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 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 3 Click the **Perform SNCP span switching** field.

Step 4 Choose **Manual** from the drop-down list.

Step 5 Click **Apply**.

Step 6 In the Confirm SNCP Switch dialog box, click **Yes**.

Step 7 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 overrides 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 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 3 Click the **Perform SNCP span switching** field.

Step 4 Choose **Lock Out of Protect** from the drop-down list.

Step 5 Click **Apply**.

Step 6 In the Confirm SNCP Switch dialog box, click **Yes**.

Step 7 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 a SNCP Span External Switching Command

Note If the ports terminating a span are configured as revertive, clearing a Force or Manual switch to protect moves traffic back to the working port. If ports are not configured as nonrevertive, 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 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 3 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 Manual Span Switch on a 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 Span** from the drop-down list.

Step 6 Click **OK**.

Step 7 Click **Yes** in the two Confirm MS-SPRing Operation dialog boxes.

Initiate a Manual Ring Switch on a 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**.

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 Lock Out on a 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 a 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.

2.8.3 CTC Card Resetting and Switching

This section gives instructions for TSC cards and SSXC cross-connect cards.

Soft-Reset a Card Using CTC

A soft reset on the active TSC causes the standby TSC card to become active. A soft reset on the preferred copy SSXC causes the alternate copy to come into service. If a line card is reset, there is no resulting traffic switch.

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

Note Whenever TSC cards are changed from active to standby, it takes approximately 12 minutes to completely synchronize to the timing source because the Stratum 3E timing module is being adopted.

Step 1 If you are resetting a TSC card, determine whether it is active and which is standby by positioning the cursor over the active card. An active TSC card has a green ACT/STBY LED illuminated.

Step 2 Right-click the card to display the shortcut menu.

Step 3 Click **Soft-reset Card**.

Step 4 Click **Yes** when the confirmation dialog box appears.

Step 5 Click **OK** when the "Lost connection to node, changing to Network View" dialog box appears.

Note The TSC card takes several minutes to reboot. Refer to the *"Card Features and Functions"* chapter in the *Cisco ONS 15600 SDH Reference Manual* for more information about LED behavior during TSC card reboots.

Step 6 If you reset a TSC card, confirm that it is in standby mode after the reset.

Tip If you run the cursor over the TSC card in CTC, a popup displays the card's status (whether active or standby).

Hard-Reset a Card Using CTC

This procedure is used to force system control from the active TSC card to the standby TSC card, or it is used to reset the SSXC or an optical (traffic) card. This kind of reset reboots the card and clears the flash memory, making it appear like a newly inserted card.

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

Caution Use hard resets with caution. There could be up to 15 other sets of bandwidth affected by a hard reset.

Note The hard-reset option is enabled only when the card is placed in the Locked-enabled,maintenance service state.

Note When a TSC card changes from active to standby, the node takes approximately 12 minutes to synchronize completely to the timing source because of the more accurate Stratum 3E timing module being adopted.

Step 1 If you are resetting a TSC card, determine which one is the active card and which is the standby card. (Position the cursor over the active card. An active TSC card has a green ACT/STBY LED illuminated.)

Step 2 Right-click the card (or active TSC card) to display the shortcut menu.

Step 3 Click **Hard-reset Card**.

Step 4 Click **Yes** when the confirmation dialog box appears.

Step 5 Click **OK** when the “Lost connection to node, changing to Network View” dialog box appears.

Note The TSC card takes several minutes to reboot. Refer to the *“Card Features and Functions”* chapter in the *Cisco ONS 15600 SDH Reference Manual* for more information about LED behavior during TSC card reboots.

Step 6 If you reset a TSC card, confirm that this TSC card you reset is in standby mode.

Tip If you run the cursor over the TSC card in CTC, a popup displays the card’s status (whether active or standby).

Request a Cross-Connect Card Preferred Copy Switch

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

Step 1 Determine which SSXC card is the preferred copy and which is currently in use.

In node view, click the **Maintenance > Preferred Copy** tabs.

Step 2 In the Set Preferred drop-down list, select the alternate copy. (For example, if the Slot 8 Copy B is preferred and in use, select the Slot 6 Copy A.)

Caution Do not select the copy that you want to replace.

Step 3 Click **Apply**.

Step 4 Click **Yes** in the confirmation dialog box.

Note If you attempt a preferred copy switch and the switch is unsuccessful, it indicates a problem on the alternate SSXC card.

Step 5 Click **Refresh** until the tab shows that the alternate copy you selected is now the preferred copy. The Currently Used field dynamically changes to display the newly selected preferred copy.

.

2.8.4 Physical Card Reseating, Resetting, and Replacement

This section gives instructions for physically reseating and replacing TSC card, SSXC cards, and traffic cards.

Reset a Card with a Card Pull (Reseat)

Note If you are pulling a TSC card, determine whether a TSC card is active or standby by positioning the cursor over the TSC card graphic to view the status.

Note Resetting a standby TSC card does not change its status to active.

Step 1 Ensure that the card you want to reset is in standby mode.

(A TSC card that is ready for service has a green SRV LED illuminated. An active TSC card has a green ACT/STBY LED illuminated, but a standby card does not have this LED illuminated.)

If you run the cursor over the TSC card in CTC, a popup displays the card's status (whether active or standby).

Step 2 Unlatch the top and bottom ejector levers on the 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 ejector levers.

Note The TSC card takes several minutes to reboot. Refer to the *"Card Features and Functions"* chapter in the *Cisco ONS 15600 SDH Reference Manual* for more information about LED behavior during TSC card reboots.

Note When a standby TSC card is removed and reinserted (reseated), all three fan lights might momentarily illuminate, indicating that the fan controller cards have also reset.

Replace an SSXC Card

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

Note The ONS 15600 SDH system dynamically changes the preferred copy status from one SSXC to the redundant copy if an error is detected on a card port. You can see this change in the CTC node view Maintenance > Preferred Copy window Currently Used field. If errors are detected on both SSXC copies, the Currently Used field says Both.

Note You do not need to make any changes to the database if you are replacing it with a card of exactly the same type.

Note Card removal raises an IMPROPRMVL alarm, but this clears after the card replacement is complete.

Step 1 Physically remove the card to be replaced from the ONS 15600 SDH shelf by completing the following steps:

a. Open the card ejectors.

b. Slide the card out of the slot.

Step 2 Physically replace the SSXC card in the shelf by completing the following steps:

a. Open the ejectors on the replacement card.

b. Slide the replacement card into the slot along the guide rails until it contacts the backplane.

c. Close the ejectors.

Note When you replace a card with the identical type of card, you do not need to make any changes to the database.

.

Replace an I/O Card

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

Note Card removal raises an IMPROPRMVL alarm, but this clears after the card replacement is completed.

Step 1 Ensure that the card you are replacing does not carry traffic in a 1+1 protection group by completing the following steps:

a. In node view, click the **Maintenance > Protection** tabs.

b. Choose the first group listed under Protection Groups.

c. Verify that the slot number for the card you are replacing does not appear in the Selected Groups list. For example, if you are replacing the STM-16 card in Slot 3, ensure Selected Groups does not contain any entries that start with s3, regardless of the port.

d. Repeat Steps b and c for each protection group.

e. If any of the groups contain a port on the card you want to replace, complete the "Initiate a 1+1 Protection Port Force Switch Command" procedure on page 2-122.

Step 2 Ensure that the card you are replacing does not carry SNCP circuit traffic by completing the following steps:

Note A port can be part of a 1+1 protection group or part of an SNCP, but it cannot be configured for both. However, different ports on one card can be configured in different ways. If you move all of the traffic off some 1+1 ports, you still need to check whether the remaining ports are carrying SNCP traffic.

a. From the **View menu, choose Go to Parent View**.

b. Click the **Circuits** tab.

c. View the circuit source and destination ports and slots. If any circuits originate or terminate in the slot containing the card you are replacing, perform the "Initiate a Force Switch for All Circuits on a SNCP Span" procedure on page 2-124.

Note If the card you are replacing is not configured for any port or circuit protection, but does carry traffic, bridge and roll this traffic onto another card. Follow the "Bridge and Roll Traffic" procedure in the "Manage Circuits" chapter in the *Cisco ONS 15600 SDH Procedure Guide*.

Step 3 Ensure that the card you are replacing does not carry MS-SPRing circuit traffic by completing the following steps.

a. In CTC node view, click **View > Go to Parent View**.

b. Click the **Circuits** tab.

c. View the circuit source and destination ports and slots. If any circuits originate or terminate in the slot containing the card you are replacing, perform the "Initiate a Manual Span Switch on a MS-SPRing" procedure on page 2-127.

Note If the card you are replacing is not configured for any port or circuit protection, but does carry traffic, bridge and roll this traffic onto another card. Refer to the "Manage Circuits" chapter in the *Cisco ONS 15600 SDH Procedure Guide*.

Step 4 Remove any fiber optic cables from the ports.

Step 5 Physically remove the card that you want to replace from the ONS 15600 SDH shelf by completing the following steps:

a. Open the card ejectors.

b. Slide the card out of the slot.

Step 6 Physically replace the STM-16 or STM-64 card in the shelf by completing the following steps:

a. Open the ejectors on the replacement card.

b. Slide the replacement card into the slot along the guide rails until it contacts the backplane.

c. Close the ejectors.

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 Clear the Force switches.

- To clear 1+1 Force switches, complete the "Clear a 1+1 Protection Port Force or Manual Switch Command" procedure on page 2-123.
- To clear SNCP Force switches, complete the "Clear a SNCP Span External Switching Command" procedure on page 2-126.

Step 8 When the card is in service and receiving traffic, reset the card's physical receive power level threshold in CTC by completing the following steps:

a. Double-click the newly installed card in CTC node view.

b. Click the **Provisioning > Threshold** tabs.

c. Click the **Physical** radio button.

d. Click **Set OPM** for each port on the card.

Replace a TSC Card

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

Note When an error is detected on a TSC card, the ONS 15600 SDH system switches control to the second TSC card; therefore, so it should not be necessary to change control when you replace the card.

Note You do not need to make any changes to the database if you are replacing it with a card of exactly the same type.

Note Card removal raises an IMPROPRMVL alarm, but this clears after the card replacement is completed.

Step 1 Ensure that the card you are replacing is not the active TSC card: Run the mouse over the card in CTC. If the card says Active, switch it to Standby by completing the following steps:

a. Right-click the active TSC card to display the shortcut menu.

b. Click **Soft-reset Card**.

c. Click **Yes** when the confirmation dialog box appears.

d. Click **OK** when the “Lost connection to node, changing to Network View” dialog box appears.

Note The TSC card takes several minutes to reboot. Refer to the *“Card Features and Functions”* chapter in the *Cisco ONS 15600 SDH Reference Manual* for more information about LED behavior during TSC card reboots.

Note Whenever TSC cards are changed from active to standby, it takes approximately 12 minutes to completely synchronize to the new system clock source due to the more accurate Stratum 3E timing module being adopted.

Step 2 Confirm that the TSC card you reset is in standby mode after the reset.

A TSC card that is ready for service has a green SRV LED illuminated. An active TSC card has a green ACT/STBY LED illuminated, but a standby card does not have this LED illuminated.

Tip If you run the cursor over the TSC card in CTC, a popup displays the card’s status (whether active or standby).

Step 3 Physically remove the card you want to replace from the ONS 15600 SDH by completing the following steps:

a. Open the card ejectors.

b. Slide the card out of the slot.

Step 4 Insert the replacement TSC card into the empty slot by completing the following steps:

a. Open the ejectors on the replacement card.

b. Slide the replacement card into the slot along the guide rails until it contacts the backplane.

c. Close the ejectors.

Step 5 If you want to make the replaced TSC card active, complete Steps b through d in Step 2 again.

Replace an ASAP Carrier Module

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

Note You do not need to make any changes to the database if you are replacing it with a card of exactly the same type.

Note Card removal raises an IMPROPRMVL alarm, but this clears after the card replacement is completed.

Step 1 Verify that the card is not carrying any traffic. If it is, switch it using the appropriate procedure.

Step 2 Physically remove the ASAP carrier module from the ONS 15600 SDH by completing the following steps:

a. Open the card ejectors.

b. Slide the card out of the slot.

Step 3 Insert the replacement carrier module into the empty slot by completing the following steps:

a. Open the ejectors on the replacement card.

b. Slide the replacement card into the slot along the guide rails until it contacts the backplane.

c. Close the ejectors.

Replace an ASAP 4PIO (PIM) Module

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

Note You do not need to make any changes to the database if you are replacing it with a card of exactly the same type.

Note Card removal raises an IMPROPRMVL alarm, but this clears after the card replacement is completed.

Step 1 Use a Phillips screwdriver to loosen the screws at the top right and bottom left of the 4PIO (PIM) module.

Step 2 Carefully slide the motherboard of the module along the top and bottom guide rails out of the slot.

Step 3 Carefully slide the motherboard of the new module into the slot.

Step 4 Tighten the screws at the top right and bottom left of the 4PIO (PIM) module.

Note The 4PIO (PIM) LEDs do not light until a fixed-rate PIM is installed in the associated slot or a multirate optical (MRO) PIM is installed and an optical rate is provisioned.

Note If you insert a card into a slot provisioned for a different card, all red LEDs turn on and you will see an MEA alarm for that slot when you open CTC.

Step 5 After you have logged into CTC, verify that the card appears in CTC card view.

Replace an ASAP SFP (PPM) Module

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

Note You do not need to make any changes to the database if you are replacing it with a card of exactly the same type.

Note Card removal raises an MPROPRMVL alarm, but this clears after the card replacement is completed.

Step 1 Unlatch the bail clasp by moving it to the left before removing the bad SFP (PPM) from the slot.

Step 2 Slide the SFP (PPM) out of the slot.

Step 3 Verify that the new SFP (PPM) is correct for your network and ASAP card. Refer to the *Cisco ONS 15600 SDH Reference Manual* for more information.

Step 4 Orient the new SFP so that the Cisco serial number label is facing away from the shelf (to the right).

Step 5 Slide the SFP into the slot and move the bail clasp to the right to secure the SFP.

Caution Do not remove the protective caps until you are ready to attach the network fiber-optic cable.

Note Multirate SFPs (PPMs) must be provisioned in CTC; single-rate SFPs (PPMs) do not need to be provisioned. Refer to the “Install Cards and Fiber-Optic Cable” chapter in the *Cisco ONS 15600 SDH Procedure Guide* for provisioning instructions.

2.8.5 Verify or Create Node DCC Terminations

Step 1 In node view, click the **Provisioning > Comm Channels > RS-DCC** tabs (or **Provisioning > Comm Channels > MS-DCC** tabs as appropriate).

Step 2 View the Port column entries to see where terminations are present for a node. If terminations are missing, proceed to Step 3.

Step 3 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**.

Set the Optical Power Received Nominal Value

Step 1 In node view, double-click the STM-N card that you want to provision. The card view appears.

Step 2 For a fixed-rate card, click the **Provisioning > SDH Thresholds** tabs. For the ASAP card, click the **Provisioning > Optical >Optics Thresholds** tabs.

Step 3 From the Types list, choose **Physical** and click **Refresh**.

Step 4 For the port you want to provision, click the **Set** button in the Set OPR column. In the confirmation dialog box, click **OK**.

CHAPTER 3

Transient Conditions

This chapter gives a description, entity, Simple Network Management Protocol (SNMP) number, and trap for each commonly encountered Cisco ONS 15600 SDH transient condition.

3.1 Transients Indexed By Alphabetical Entry

Table 3-1 alphabetically lists all ONS 15600 SDH transient conditions and their entity, SNMP number, and SNMP trap.

Note The Cisco Transport Controller (CTC) default alarm profile might contain conditions that are not currently implemented but are reserved for future use.

Table 3-1 ONS 15600 SDH Transient Condition Alphabetical Index

Transient Condition	Entity	SNMP Number	SNMP Trap
3.3.1 ADMIN-DISABLE, page 3-3	NE	5270	disableInactiveUser
3.3.2 ADMIN-DISABLE-CLR, page 3-3	NE	5280	disableInactiveClear
3.3.3 ADMIN-LOCKOUT, page 3-3	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 3-4	NE	5350	suspendUserClear
3.3.8 AUTH-FAIL, page 3-4	NE	6310	remoteAuthenticationFailSeeAuditLog
3.3.9 DBBACKUP-FAIL, page 3-4	EQPT	3724	databaseBackupFailed
3.3.10 DBRESTORE-FAIL, page 3-4	EQPT	3726	databaseRestoreFailed
3.3.11 ETHERNET-PORT-SWITCH, page 3-5	NE	7195	etherPortSwitch
3.3.12 EXERCISING-RING, page 3-5	OCN	3400	exercisingRingSuccessfully
3.3.13 FIREWALL-DIS, page 3-5	NE	5230	firewallHasBeenDisabled
3.3.14 INTRUSION, page 3-5	NE	5250	securityIntrusionDetUser

Table 3-1 ONS 15600 SDH Transient Condition Alphabetical Index (continued)

Transient Condition	Entity	SNMP Number	SNMP Trap
3.3.15 LOGIN-FAIL-LOCKOUT, page 3-5	NE	5080	securityInvalidLoginLockedOutSeeAuditLog
3.3.16 LOGIN-FAIL-ONALRDY, page 3-5	NE	5090	securityInvalidLoginAlreadyLoggedOnSeeAuditLog
3.3.17 LOGIN-FAILURE-PSWD, page 3-6	NE	5070	securityInvalidLoginPasswordSeeAuditLog
3.3.18 LOGOUT-IDLE-USER, page 3-6	—	5110	automaticLogoutOfIdleUser
3.3.19 MSSP-RESYNC, page 3-6	STMN	4340	msspMultiNodeTableUpdateCompleted
3.3.20 PM-TCA, page 3-6	—	2120	performanceMonitorThresholdCrossingAlert
3.3.21 SWFTDOWNFAIL, page 3-6	EQPT	3480	softwareDownloadFailed
3.3.22 USER-LOCKOUT, page 3-6	NE	5030	userLockedOut
3.3.23 USER-LOGIN, page 3-7	NE	5100	loginOfUser
3.3.24 USER-LOGOUT, page 3-7	NE	5120	logoutOfUser
3.3.25 WKSWBK, page 3-7	EQPT, OCN	2640	switchedBackToWorking
3.3.26 WKSWPR, page 3-7	2R, TRUNK, EQPT, ESCON, FC, GE, ISC, STMN, VCMON-HP, VCMON-LP	2650	switchedToProtection

3.2 Trouble Notifications

The ONS 15600 SDH reports trouble by using standard condition characteristics that follow the rules in ITU-T G.784 and graphical user interface (GUI) state indicators.

The ONS 15600 SDH uses standard ITU 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 15600 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 Transaction Language One (TL1).

Note Some cleared conditions are found on the History tab.

For a comprehensive list of conditions, refer to the *Cisco ONS 15454 and Cisco ONS 15600 SDH 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, logout, 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 9.0. The description, entity, SNMP number, and SNMP trap accompany each condition.

3.3.1 ADMIN-DISABLE

The Disable Inactive User (ADMIN-DISABLE) 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 Disable Inactive Clear (ADMIN-DISABLE-CLR) 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 of User (ADMIN-LOCKOUT) 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 Clear (ADMIN-LOCKOUT-CLR) 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 of User (ADMIN-LOGOUT) 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 Suspend User (ADMIN-SUSPEND) 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 Suspend User Clear (ADMIN-SUSPEND-CLR) condition occurs when the user or administrator changes the password.

This transient condition does not result in a standing condition.

3.3.8 AUTH-FAIL

The Remote Authentication Fail - See Audit Log (AUTH-FAIL) condition indicates that an attempt to validate a login remotely has failed.

This transient condition does not result in a standing condition.

3.3.9 DBBACKUP-FAIL

The Database Backup Failed (DBBACKUP-FAIL) condition occurs when the system fails to back up the database when the backup command is initiated.

This condition can occur when the server is not able to handle the backup operation due to network or server issues. Repeat the same operation again and check to see if it is successful. If the backup fails, it could be due to a network issue or software program failure. Contact the Cisco Technical Assistance Center (Cisco TAC) for assistance; see the "Obtaining Documentation and Submitting a Service Request" section on page xxxi as needed.

3.3.10 DBRESTORE-FAIL

The Database Restore Failed (DBRESTORE-FAIL) condition occurs when the system fails to restore the backed up database when the restore command is initiated.

This condition can be due to server issues, network issues, or human error (pointing to a file that does not exist, wrong file name, etc.). Retrying the database restore with the correct file will usually succeed. If the network issue persists, you must contact network lab support. If the condition is caused by a network element (NE) failure, contact Cisco TAC for assistance. See the "Obtaining Documentation and Submitting a Service Request" section on page xxxi as needed.

3.3.11 ETHERNET-PORT-SWITCH

The TSC Switched to Alternate Ethernet Port (ETHERNET-PORT-SWITCH) condition occurs when an alternate Ethernet port becomes active. If it occurs after startup, it means that the backplane Ethernet connection that was active is not active anymore. Onsite technical support must check the connection between the ONS 15600 SDH and the router or switch.

3.3.12 EXERCISING-RING

The Exercising Ring Successfully (EXERCISING-RING) condition occurs whenever you issue an Exercise-Ring command from CTC or Transaction Language 1 (TL1). This condition indicates that a command is being executed. You must issue another command to clear the exercise and the condition.

3.3.13 FIREWALL-DIS

The Firewall Has Been Disabled (FIREWALL-DIS) condition occurs when you provision the firewall to Disabled.

This transient condition does not result in a standing condition.

3.3.14 INTRUSION

The Invalid Login Username (INTRUSION) condition occurs when you attempt to log in with an invalid user ID.

This transient condition does not result in a standing condition.

3.3.15 LOGIN-FAIL-LOCKOUT

The Invalid Login–Locked Out (LOGIN-FAIL-LOCKOUT) condition occurs when you attempt to log into a locked account.

This transient condition does not result in a standing condition.

3.3.16 LOGIN-FAIL-ONALRDY

The Security: Invalid Login–Already Logged On (LOGIN-FAIL-ONALRDY) condition occurs when you attempt to log into a node where you already have an existing session and a Single-User-Per-Node (SUPN) policy exists.

This transient condition does not result in a standing condition.

3.3.17 LOGIN-FAILURE-PSWD

The Invalid Login–Password (LOGIN-FAILURE-PSWD) condition occurs when you attempt to log in with an invalid password.

This transient condition does not result in a standing condition.

3.3.18 LOGOUT-IDLE-USER

The Automatic Logout of Idle User (LOGOUT-IDLE-USER) condition occurs when a user session is idle for too long (the idle timeout expires) and the session terminates as a result. You must log in again to restart your session.

3.3.19 MSSP-RESYNC

The MS-SPRing Multi-Node Table Update Completed (MSSP-RESYNC) condition occurs when a node receives all relevant information such as payload, path state, Routing Information Protocol (RIP), cross-connect tables, and cross-connect VT tables from the other nodes in the ring. This condition is raised on all nodes in the ring while a node is added or a circuit is provisioned. This transient condition will not be cleared and is seen in the History tab of CTC.

You must check this condition on all the nodes and then remove the Forced Ring Switch commands.

3.3.20 PM-TCA

The Performance Monitor Threshold Crossing Alert (PM-TCA) condition occurs when network collisions cross the rising threshold for the first time.

3.3.21 SWFTDOWNFAIL

The Software Download Failed (SFTDOWN-FAIL) condition occurs when the system fails to download the required software.

An incorrect input that points to the wrong place or file, network issues, or a bad (corrupt) package can cause this failure. Retrying the operation with the correct name/location will usually succeed. If network issues persist, you must contact the network lab support. If the package is corrupt, contact Cisco TAC. See the "Obtaining Documentation and Submitting a Service Request" section on page xxxi for details.

3.3.22 USER-LOCKOUT

The User Locked Out (USER-LOCKOUT) condition occurs when the system locks an account because of a failed login attempt. To proceed, the administrator must unlock the account or the lockout time must expire.

3.3.23 USER-LOGIN

The Login of User (USER-LOGIN) occurs when you begin a new session by verifying your User ID and password.

This transient condition does not result in a standing condition.

3.3.24 USER-LOGOUT

The Logout of User (USER-LOGOUT) condition occurs when you stop a login session by logging out of your account.

This transient condition does not result in a standing condition.

3.3.25 WKSWBK

The Switched Back to Working (WKSWBK) condition occurs when traffic switches back to the working port/card in a nonrevertive protection group.

This transient condition does not result in a standing condition.

3.3.26 WKSWPR

The Switched to Protection (WKSWPR) condition occurs when traffic switches to the protect port/card in a nonrevertive protection group.

This transient condition does not result in a standing condition.

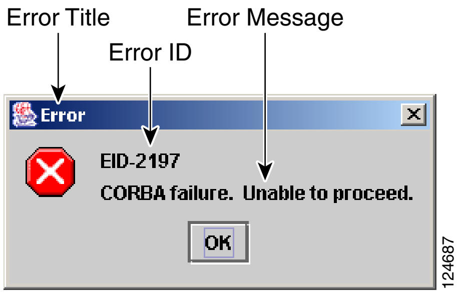
CHAPTER 4

Error Messages

This chapter lists the ONS 15454 SDH and ONS 15600 SDH error messages. Table 4-1 gives a list of all error message numbers, the messages, and a brief description of each message. The table lists two types of messages: error messages (EID-*nnnn*) and warning messages (WID-*nnnn*). An error message is an alert that an unexpected or undesirable operation has occurred that either indicates the risk of loss of traffic or an inability to properly manage devices in the network. A warning is an alert that the requested operation could lead to an error. Warnings are sometimes used to convey important information.

The error dialog box in Figure 4-1 consists of three parts: the error title, error ID, and the error message.

Figure 4-1 Error Dialog Box



EID-2197
CORBA failure. Unable to proceed.

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/Warning ID	Error/Warning Message	Description
EID-0	Invalid error ID.	The error ID is invalid.
EID-1	A null pointer encountered in {0}.	Cisco Transport Controller (CTC) encountered a null pointer in the area described by the specified item.
EID-1000	The host name of the network element cannot be resolved to an address.	Refer to the error message text.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-1001	Unable to launch CTC due to applet security restrictions. Please review the installation instructions to make sure that the CTC launcher is given the permissions it needs. Note that you must exit and restart your browser in order for the new permissions to take effect.	Refer to the error message text.
EID-1002	The host name (e.g., for the network element) was successfully resolved to its address, but no route can be found through the network to reach the address.	The node is not reachable from CTC client station.
EID-1003	An error was encountered while attempting to launch CTC. {0}	Unexpected exception or error while launching CTC from the applet.
EID-1004	Problem Deleting CTC Cache: {0} {1}	Unable to delete the CTC cached JARs, because another application may have the JAR files running; for example, another instance of CTC.
EID-1005	An error occurred while writing to the {0} file.	CTC encountered an error while writing to log files, preference files, etc.
EID-1006	The URL used to download {0} is malformed.	The URL used to download the specified JAR file is incorrect.
EID-1007	An I/O error occurred while trying to download {0}.	An input or output exception was encountered when CTC tried to download the specified JAR file.
EID-1018	Password shall not contain the associated user-ID.	The password is invalid.
EID-1019	Could not create {0}. Please enter another filename.	CTC could not create the file due to an invalid filename.
EID-1020	Fatal exception occurred, exiting CTC. Unable to switch to the Network view.	CTC was unable to switch from the node or card view to the network view and is now shutting down.
EID-1021	Unable to navigate to {0}.	CTC was unable to display the requested view (node or network).
EID-1022	An IOS session cannot be opened right now with this slot. Most likely someone else (using a different CTC) already has a session opened with this slot. Please try again later.	Refer to the error message text. Ensure that the shell access in CTC (Provisioning>Security>Access) is set to non-secure mode.
EID-1023	This IOS session has been terminated. Terminations are caused when the session has timed out, the card resets, there is already a session with the slot, or password configuration is required.	Refer to the error message text.
EID-1025	Unable to create Help Broker.	CTC was unable to create the help broker for the online help.
EID-1026	Error found in the Help Set file.	CTC encountered an error in the online help file.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-1027	Unable to locate help content for Help ID: "{0}".	CTC was unable to locate the content for the help ID.
EID-1028	Error saving table. {0}	There was an error while saving the specified table.
EID-1031	CTC cannot locate the online user manual files. The files may have been moved, deleted, or not installed. To install online user manuals, run the CTC installation wizard on the software or documentation CD.	Refer to the error message text.
EID-1032	CTC cannot locate Acrobat Reader. If Acrobat Reader is not installed, you can install the Reader using the CTC installation wizard provided on the software or documentation CD.	Refer to the error message text.
EID-1035	CTC experienced an I/O error while working with the log files. Usually this means that the computer has run out of disk space. This problem may or may not cause CTC to stop responding. Ending this CTC session is recommended, but not required.	Refer to the error message text.
WID-1036	WARNING: Deleting the CTC cache may cause any CTC running on this system to behave in an unexpected manner.	Refer to the warning message text.
EID-1037	Could not open {0}. Please enter another filename.	Invalid file name. CTC is unable to open the specified file. Ensure that the file exists and the filename was typed correctly.
EID-1038	The file {0} does not exist.	The specified file does not exist.
EID-1039	The version of the browser applet does not match the version required by the network element. Please close and restart your browser in order to launch the Cisco Transport Controller.	Refer to the error message text.
WID-1041	An error occurred while closing the {0} connection.	CTC encountered an error while closing the specified connection.
WID-1042	You have selected Java version {0}. This version is outside of the recommended range and may cause an unpredictable behavior of the software. Do you wish to continue?	Refer to the warning message text.
EID-1043	Error writing to file: {0}. This might be caused by a directory permission, quota or disk volume full issue.	Check for possible causes and try again.
WID-1044	Warning: there is a discrepancy in the build timestamp between the NE cached jar file ({0}) and the NE ({1}). Your CTC jar cache should be emptied.	Refer to the warning message text.
EID-1046	Selected CTC version ({0}) must be greater than or equal{to the login NE version ({1}).	The CTC software version must be greater than or equal to the software version on the node being managed.
EID-1047	No additional Pseudo IOS windows may be opened at this time. The maximum number of Pseudo IOS windows are open.	Refer to the error message text.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-1048	This Pseudo IOS connection has been terminated. Terminations are caused when the session has timed out, the node resets, or when the exit command has been invoked. This may also occur when the maximum number of concurrent Pseudo IOS connections has been reached.	Refer to the error message text.
EID-1049	A Pseudo IOS connection cannot be opened right now on this node. Please try again later.	Refer to the error message text.
EID-2001	No rolls were selected. {0}	No rolls were selected for the bridge and roll.
EID-2002	The roll must be completed or canceled before it can be deleted.	You cannot delete the roll unless it has been completed or cancelled.
EID-2003	An error occurred while deleting the roll. {0}	There was an error when CTC tried to delete the roll.
EID-2004	No Cisco IOS slot was selected.	You did not select a Cisco IOS slot.
EID-2005	CTC cannot find the online help files for {0}. The files might have been moved, deleted, or not installed. To install online help, run the setup program on the software 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 CD.
EID-2006	An error occurred while editing the circuit(s). {0} {1}.	An error occurred when CTC tried to open the circuit for editing.
EID-2007	The preferences could not be saved.	CTC cannot save the preferences.
EID-2008	The circuit preferences could not be saved: {0}	CTC cannot find the file needed to save the circuit preferences.
EID-2009	CTC was unable to download the package: {0}	Refer to the error message text.
EID-2010	An error occurred while deleting the destination.	CTC could not delete the destination.
EID-2011	The circuit could not be destroyed.	CTC could not destroy the circuit.
EID-2012	The reverse circuit could not be destroyed.	CTC could not reverse the circuit destroy.
EID-2013	The circuit creation failed. The circuit creation cannot proceed due to changes in the network which affected the circuit(s) being created. The dialog box will close. Please try again.	Refer to the error message text.
EID-2014	No circuit(s) were selected. {0}	You must select a circuit to complete this function.
EID-2015	The circuit {0} cannot be deleted because it has one or more rolls.	You must delete the rolls in the circuit before deleting the circuit itself.
EID-2016	The circuit deletion failed.	CTC could not delete the tunnel as there are circuits that use the tunnel.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-2017	An error occurred while mapping the circuit. {0}	There was an error mapping the circuit.
EID-2018	The circuit roll failed. The circuit must be in the DISCOVERED state in order to perform a roll.	There was a failure in circuit roll. Change the circuit state to DISCOVERED and proceed.
EID-2019	The circuit roll failed. Bridge and roll is not supported on DWDM circuits.	Refer to the error message text.
EID-2020	The circuit roll failed. The two circuits must have the same direction.	Refer to the error message text.
EID-2021	The circuit roll failed. The two circuits must have the same size.	Refer to the error message text.
EID-2022	The circuit roll failed. A maximum of two circuits can be selected for a bridge and roll operation.	Refer to the error message text.
EID-2023	CTC was unable to create a new user account.	Refer to the error message text.
EID-2024	An error occurred during node selection.	There was an error during node selection.
EID-2025	This feature cannot be used. Verify that each endpoint of this circuit is running software that supports this feature.	Refer to the error or warning message text. For example, this error is generated from the node view Provisioning > WDM-ANS tab to indicate that the selected ring type is not supported by the endpoints of the circuit. Another example is the Provisioning > VLAN tab in card view (Ethernet card only), where it indicates that the back-end Spanning Tree Protocol (STP) disabling is not supported.
EID-2026	The {0} request could not be applied. {1}	Error occurred while attempting to switch a subnetwork connection protection (SNCP) circuit away from a span.
EID-2027	An error occurred while deleting the circuit drop.	CTC could not delete the circuit drop.
EID-2028	An error occurred while removing the circuit node.	CTC could not remove the circuit node.
EID-2029	The requested operation is not supported.	The task you are trying to complete is not supported by CTC.
EID-2030	An error occurred during provisioning.	There was an error during provisioning.
EID-2031	An error occurred while adding the node.	There was an error while adding a node.
EID-2032	The circuit could not be renamed. {0}	CTC could not rename the circuit.
EID-2033	An error occurred during validation. {0}	There was an internal error while validating the user changes after the Apply button was pressed. This error can occur in the Edit Circuit dialog box or in the BLSR table in the shelf view (rare condition).

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-2034	Network circuits could not be added: {0}	Refer to the error message text.
EID-2035	The source and destination nodes are not connected.	Refer to the error message text.
EID-2036	The {0} cannot be deleted. LAN Access has been disabled on this node and this {0} is needed to access the node.	You cannot delete the DCC/GCC link as it is needed to access the node.
EID-2037	The attribute for {0} cannot be found.	CTC cannot find an attribute for the specified item.
EID-2038	The protection operation is invalid.	The protection operation you tried to execute is invalid.
EID-2040	Please select a node first.	You must select a node before performing the task.
EID-2041	No paths are available on this link. Please make another selection.	You must select a link that has paths available.
EID-2042	This span is not selectable. Only the green spans with an arrow may be selected.	Refer to the error message text.
EID-2043	This node is not selectable. Only the source node and nodes attached to included spans (blue) are selectable. Selecting a selectable node will enable its available outgoing spans.	Refer to the error message text.
EID-2044	This link may not be included in the required list. Constraints only apply to the primary path. Each node may have a maximum of one incoming signal and one outgoing link.	You must select only one link going in and out of a node. Selecting more than one link is contradictory to the path selection algorithm.
EID-2045	This link may not be included in the required list. Only one outgoing link may be included for each node.	Refer to the error message text.
EID-2047	Please enter a valid value for the slot number.	There was an error due to an invalid slot number.
EID-2048	Please enter a valid value for the port number.	There was an error due to an invalid port number.
EID-2050	The new circuit could not be destroyed.	CTC could not destroy the new circuit.
EID-2051	The circuit cannot be downgraded. {0}	The specified circuit cannot be downgraded.
EID-2052	An error occurred during circuit processing.	There was an error during the circuit processing.
EID-2054	An error occurred while selecting an endpoint.	There was an error during the endpoint selection.
EID-2055	No endpoints are available for this selection. Please make another selection.	This error occurs in the circuit creation dialog only during a race condition that has incorrectly allowed entities without endpoints to be displayed in the combination boxes.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-2056	A communication error occurred: {0}	An internal error occurred in Network Alarm tab while synchronizing alarms with the nodes.
EID-2059	An error occurred while deleting the node. {0}	There was an error during the node deletion.
EID-2060	No PCA circuits were found.	CTC could not find any protection channel access (PCA) circuits for this task.
EID-2061	An error occurred while provisioning the VLAN.	There was an error defining the VLAN.
EID-2062	An error occurred while deleting VLANs. No VLAN(s) were selected. Please select a VLAN.	Refer to the error message text.
EID-2063	The default VLAN cannot be deleted.	The selected VLAN is the default VLAN and cannot be deleted.
EID-2064	An error occurred while deleting VLANs. {0}	There was an error deleting the specified VLAN.
EID-2065	The profile cannot be imported. The profile "{0}" exists in the editor and the maximum number of copies (ten) exists in the editor. The import will be aborted. The profile has already been loaded eleven times.	Cannot import the profile because the profile has reached the maximum number of copies in the editor.
EID-2066	The profile could not be stored. An error occurred while writing to {0}.	CTC encountered an error while trying to store the profile.
EID-2067	An error occurred while writing to the file. {0}	CTC encountered an error while writing the specified file.
EID-2068	The alarm profile could not be loaded from the node.	CTC encountered an error trying to load the alarm profile from the node.
EID-2069	The file could not be found or an I/O exception occurred. {0}	Either the specified file was not found, or there was an input/output exception.
EID-2070	The profile could not be deleted. {0}	There was a failure in deleting the specified profile.
EID-2071	Only one column may be highlighted.	You cannot select more than one column during clone action.
EID-2072	Only one profile may be highlighted.	You cannot select more than one profile.
EID-2073	This column is permanent and cannot be removed.	You cannot delete a permanent column.
EID-2074	Select one or more profiles.	You have not selected any profile or column. Reset operation is done by right-clicking the selected column.
EID-2075	This column is permanent and cannot be reset.	A permanent column is non resettable.
EID-2077	This column is permanent and cannot be renamed.	You cannot rename a permanent column.
EID-2078	At least two columns must be highlighted.	You cannot compare two profiles unless you select two columns.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-2079	The alarm types cannot be loaded into table. There are no reachable nodes from which the list of alarm types can be loaded. Please wait until such a node is reachable and try again.	Refer to the error message text.
EID-2080	The node {0} has no profiles.	The specified node does not have any profiles.
EID-2081	An error occurred while removing profile {0} from the node {1}.	There was an error while removing the specified profile from the specified node.
EID-2082	The profile {0} does not exist on the node {1}.	CTC cannot find the specified profile from the specified node.
EID-2083	An error occurred while adding profile {0} to the node {1}.	There was an error adding the specified profile to the specified node.
EID-2085	The profile selection is invalid. No profiles were selected.	You tried to select an invalid profile. Select another profile.
EID-2086	The node selection is invalid. No nodes were selected.	You tried to select an invalid node. Select another node.
EID-2087	No profiles were selected. Please select at least one profile.	Refer to the error message text.
EID-2088	The profile name is invalid.	The profile name cannot be empty.
EID-2089	Too many copies of {0} exist. Please choose another name.	Select a unique name.
EID-2090	No nodes were selected. Please select the node(s) on which to store the profile(s).	You must select one or more nodes on which you can store the profile.
EID-2091	Unable to switch to the node {0}.	CTC is unable to switch to the specified node.
EID-2092	A general exception error occurred.	CTC encountered a general exception error while trying to complete the task.
EID-2093	The name is too short. It does not have enough characters. {0}	The name must have a minimum of six characters.
EID-2094	The password and confirmed password fields do not match.	You must make sure the two fields have the same password.
EID-2095	The password is invalid. {0}	The password you entered is not allowed.
EID-2096	The user must have a security level.	You must have an assigned security level to perform this task.
EID-2097	No user name was specified.	You did not specify a user name.
EID-2099	An error occurred while ring switching.	There was an error during the ring switch.
EID-2100	Please select at least one profile to delete.	You have not selected the profile to delete.
EID-2101	An error occurred while protection switching.	There was an error during the protection switching.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-2102	The forced switch could not be removed for some circuits. You must switch these circuits manually.	The forced switch could not be removed for some circuits. You must switch these circuits manually.
EID-2103	An error occurred while upgrading the span.	There was an error during the span upgrade.
EID-2104	The circuits cannot be switched back because one or both nodes are not reachable.	This error occurs during the SNCP span upgrade procedure.
EID-2106	The node name cannot be empty.	You must supply a name for the node.
EID-2107	An error occurred while adding {0}. The host is unknown.	There was an error adding the specified item.
EID-2108	{0} is already in the network.	The specified item exists in the network.
EID-2109	The node is already in the current login group.	The node you are trying to add is already present in the current login group.
EID-2110	Please enter a number between 0 and {0}.	You must enter a number in the range between 0 and the specified value.
EID-2111	This node ID is already in use. Please choose another.	Select a node ID that is not in use.
EID-2113	The extension byte for the ring cannot be set. {0}	CTC cannot set the MS-SPRing extension byte.
EID-2114	A card communication failure occurred during the operation.	This error can occur during an attempt to apply a MS-SPRing protection operation to a line.
EID-2115	An error occurred during the operation. {0}	There was an error in applying the specified operation.
EID-2116	The extension byte setting for the ring is invalid. {0}	The extension byte set for the specified ring is invalid.
EID-2118	The ring cannot be deleted. A protection operation is set. All protection operations must be clear for ring to be deleted.	Clear all the protection operations for the ring before deleting it.
EID-2119	{0} cannot be deleted because a protection switch is in effect. Please clear any protection operations, ensure that the reversion time is not "never" and allow any protection switches to clear before trying again.	Clear all protection operations or switches before deleting the ring.
EID-2120	The following nodes could not be unprovisioned {0} Therefore you will need to delete this {1} again later.	The specified nodes could not be unprovisioned. Try deleting this MS-SPRing later.
EID-2121	The ring cannot be upgraded. {0}	CTC cannot upgrade the specified ring.
EID-2122	The ring speed for is inadequate for the upgrade procedure. Only {0} (or higher) {1} can be upgraded to four-fiber.	You have selected an incorrect ring speed for upgrade. Only rings within the specified parameters can be upgraded to 4-fiber MS-SPRing.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-2123	Verify that the following nodes have at least two in-service ports with the same speed as the two-fiber {0}. The ports cannot serve as timing references, and they cannot have DCC terminations or overhead circuits. {1}	Nonupgradable nodes. Verify that the specified nodes have at least two Unlocked-enabled ports with the same speed as the 2-fiber MS-SPRing. The specified ports cannot serve as a timing reference, and they cannot have data communications channel (DCC) terminations or overhead circuits.
EID-2124	You cannot add this span because it is connected to a node that already has the east and west ports defined.	Refer to the error message text.
EID-2125	You cannot add this span as it would cause a single card to host both the east span and the west span. A card cannot protect itself.	Refer to the error message text.
EID-2126	An error occurred while provisioning the OSPF area. {0}	There is an Open Shortest Path First (OSPF) area error.
EID-2127	You cannot add this span. It would cause the following circuit(s) to occupy different {0} regions on different spans: {1} Either select a different span or delete the above circuit(s).	A circuit cannot occupy different STS regions on different spans. You may add a different span or delete the specified circuit.
EID-2128	The state is invalid.	An internal error occurred while trying to remove a span from a MS-SPRing. This alarm occurs in the network-level MS-SPRing creation dialog box.
EID-2129	You cannot use same slot for east and west protect ports.	Refer to the error message text.
EID-2130	The ring ID value, {0}, is not valid. Please enter a valid number between 0 and 9999.	Enter a ring ID value between 0 and 9999.
EID-2131	The reversion cannot be set to INCONSISTENT.	You must select another reversion type.
EID-2135	The overhead circuit preferences could not be stored: {0}	Input/Output error. Unable to store overhead circuit preferences.
EID-2137	An error occurred during the circuit merge. {0}	There was an error while merging the circuits.
EID-2138	Not all destinations could be deleted. Please try again.	Refer to the error message text.
EID-2139	An error occurred while updating the destinations.	There was an error in updating the circuit destinations.
EID-2143	No online help version was selected. The online help book cannot be deleted.	Select the version of online help, and proceed.
EID-2144	An error occurred while deleting the online help book(s). {0}	You cannot delete the specified online help.
EID-2145	No nodes appear to have a Cisco IOS card.	Refer to error message.
EID-2146	This is a security violation. You may only logout of your own account.	You cannot logout of an account other than your own.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-2147	This is a security violation. You may only change your own account.	You cannot change an account other than your own.
EID-2148	This is a security violation. You cannot delete the account under which you are currently logged in.	You cannot delete the account you are currently logged in.
WID-2149	There is no exportable content in this view.	Refer to the error message text.
WID-2150	The node {0} is not initialized. Please wait and try again.	Wait till the specified node is initialized and try again.
WID-2152	Spanning tree protection is being disabled for this circuit.	Refer to the warning message text.
WID-2153	Adding this drop will make the circuit a PCA circuit.	Refer to the warning message text.
WID-2154	Monitor circuits cannot be created on a port grouping circuit.	Refer to the warning message text.
WID-2155	Switch counts might not be fully supported on some nodes. {0}	The specified nodes do not support switch counts completely.
WID-2156	The manual roll mode is recommended for dual rolls. For auto dual rolls, please verify that roll to facilities are in service and error-free.	Refer to the warning message text.
WID-2157	The roll(s) cannot be completed. {0}	CTC could not complete the roll because the roll is destroyed, in an incomplete state, in a TL1_roll state, is cancelled, or is not ready to complete.
EID-2158	The roll mode is invalid. {0}	There are two roll modes: auto and manual. For a one-way circuit source roll, the roll mode must be auto and for a one-way circuit destination roll, the roll mode must be manual.
EID-2159	The roll is not ready for completion. {0}	The roll is not ready for completion.
EID-2160	The roll is not connected. {0}	Refer to error message text.
EID-2161	The sibling roll is not complete. {0}	One of the rolls is not completed for the dual roll. If it is auto roll, it will be completed when a valid signal is detected. If it is a manual roll, you must complete the roll from CTC if Bridge and Roll is operated from CTC, or from TL1 if Bridge and Roll is operated from TL1.
EID-2162	An error occurred during roll acknowledgement. {0}	Refer to the error message text.
EID-2163	The roll cannot be canceled. {0}	CTC cannot cancel the roll.
EID-2164	An error occurred during the roll. {0}	CTC encountered a roll error.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
WID-2165	The MAC address of the node {0} has been changed. All circuits originating from or dropping at this node will need to be repaired.	Repair the circuits that originate from or drop at the specified node, with the new MAC address.
WID-2166	The node cannot be inserted into the domain because it is not initialized.	Initialize the node and proceed.
WID-2167	You have insufficient security privileges to perform this action.	You do not have the privilege to perform this action.
WID-2168	The following warnings surfaced while loading {0}. {1}	CTC encountered warnings while loading the alarm profile import file.
WID-2169	One or more of the profiles selected do not exist on one or more of the nodes selected.	The profile selected does not exist on the node. Select another profile.
WID-2170	The profile list on node {0} is full. Please delete one or more profiles if you wish to add the profile. {1}	The number of profile that can exist on a node has reached the limit. To add a profile, delete any of the existing profiles.
WID-2171	You have been logged out. Click OK to exit CTC.	Refer to the warning message text.
WID-2172	The CTC CORBA (IIOP) listener port setting of {0} will be applied on the next CTC restart.	The Internet Inter-ORB Protocol (IIOP) listener port setting for the CTC Common Object Request Broker Architecture (CORBA) will be applied on the next CTC restart.
EID-2173	The port is unavailable. The desired CTC CORBA ({0}) listener port, {1}, is already in use or you do not have permission to listen on it. Please select an alternate port.	Select an alternate port, as the current port is either in use or you do not have enough permission on it.
EID-2174	An invalid number was entered. Please check it and try again.	You entered an invalid firewall port number. Try again.
WID-2175	An extension byte mismatch occurred. {0}	There is a mismatch with the extension byte.
WID-2176	Not all spans have the same OSPF area ID. This will cause problems with protection switching. To determine the OSPF area for a given span, click on the span and the OSPF area will be displayed in the pane to the left of the network map.	Refer to the warning message text.
WID-2178	Only one edit pane can be opened at a time. The existing pane will be displayed.	Refer to the warning message text.
WID-2179	No update is available because the circuit has been deleted.	Refer to the warning message text.
EID-2180	The CTC initialization failed during step {0}.	CTC initialization has failed in the specified step.
EID-2181	This link cannot be included because it originates from the destination.	You must not include this link as it originates from destination of a circuit. It is against the path selection algorithm.
EID-2182	The value of {0} is invalid.	The value of the specified item is invalid.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-2183	The circuit roll failed. Bridge and roll is not supported on VCAT circuits.	Refer to the error message text.
EID-2184	Spanning Tree Protocol cannot be enabled on some ports because the ports have been assigned an incompatible list of VLANs. You can view the VLAN/Spanning Tree table or reassign the Ethernet port VLANs.	Refer to the error message text.
EID-2185	The VLANs on some ports cannot be assigned because they are incompatible with the Spanning Tree Protocol. You can view the VLAN/Spanning Tree table or reassign the VLANs.	Refer to the error message text.
EID-2186	The software download failed on node {0}.	The software could not be downloaded onto the specified node.
EID-2187	The ring name cannot exceed {0} characters. Please try again.	You must shorten the length of the ring name.
EID-2188	The nodes in this ring do not support alphanumeric IDs. Please use a ring ID between {0} and {1}.	The ring ID should not contain alphanumeric characters, and must be in the specified range.
EID-2189	The TL1 keyword "all" cannot be used as the ring name. Please provide another name.	Refer to the error message text.
EID-2190	Adding this span will cause the ring to contain more nodes than allowed.	You have reached the maximum number of nodes allowed.
EID-2191	The ring name must not be empty.	You must supply a ring name.
EID-2192	A valid route cannot be found for the circuit creation request.	CTC could not complete the circuit creation request either because there are no physical links, or the bandwidth of the available links are already reserved.
EID-2193	A valid route cannot be found for the circuit drop creation request.	Refer to the error message text.
EID-2194	A valid route cannot be found for the roll creation request.	Refer to the error message text.
EID-2195	The circuit VLAN list cannot be mapped to one spanning tree. You can view the VLAN/Spanning Tree table or reassign VLANs.	Refer to the error message text.
EID-2196	CTC cannot be relaunched. {0}	There is an error relaunching CTC.
EID-2197	A CORBA failure occurred. CTC cannot proceed.	There was a CORBA failure, and the task cannot proceed. Verify the Java version.
EID-2198	CTC is unable to switch to the {0} view.	CTC is unable to switch to the specified view.
EID-2199	Login failed on {0} {1}	The login failed on the specified tasks.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/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 the error message text.
EID-2202	An intra-node DRI circuit must have two sources.	Intranode circuit must have two sources to be a dual ring interconnect (DRI).
EID-2203	No member was selected.	You must select a member.
EID-2204	The number of circuits must be a positive integer.	The number of circuits cannot be zero or negative.
EID-2205	The circuit type must be selected.	You must select a circuit type.
EID-2206	The profile cannot be autoselected. Please select profile(s) to store and try again.	Refer to the error message text.
EID-2207	You cannot add this span. Either the ring name is too long (that is, ring name length is greater than {0}) or the endpoints do not support alphanumeric IDs.	Reduce the length of the ring name, or remove the alphanumeric characters from the endpoints.
EID-2208	This is an invalid or unsupported JRE.	The version of Java Runtime Environment (JRE) is either invalid or unsupported.
EID-2209	The user name must be at least {0} characters long.	The user name must be at least of the specified character length.
EID-2210	No package name was selected.	You must select a package name.
EID-2211	No node was selected for upgrade.	You must select a node for the upgrade.
EID-2212	A protected line is not provisionable.	The protected line cannot be provisioned. Choose another line.
WID-2213	The current type or state of some drops does not allow the new circuit state of {0} to be applied to them indirectly.	The circuit state, specified by {0} cannot be applied to the selected drops.
EID-2214	The node is disconnected. Please wait until the node reconnects.	Refer to the error message text.
EID-2215	An error occurred while leaving the {0} page.	There was an error while leaving the specified page.
EID-2216	An error occurred while entering the {0} page.	There was an error while entering the specified page.
EID-2217	Some conditions could not be retrieved from the network view	Refer to the error message text.
EID-2218	The bandwidth must be between {0} and {1} percent.	The bandwidth must be within the specified parameters.
EID-2219	The protection operation failed. An XC loopback was applied on the cross-connection.	As the protection operation failed, a cross-connect (XC) loopback will be applied on cross-connection.
EID-2220	The tunnel status is PARTIAL. CTC is not able to change it. Please try again later.	Refer to the error message text.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-2221	A valid route cannot be found for the unprotected to {0} upgrade request.	Refer to the error message text.
EID-2222	One or more of the following nodes are currently part of a four-fiber {0}. Only a single four-fiber {0} is supported per node. {1}	The nodes, specified by {1}, are already part of a 4-fiber MS-SPRing type (specified by {0}).
EID-2223	Only one circuit can be upgraded at a time.	Refer to the error message text.
EID-2224	This link may not be included because it terminates on the source.	Refer to the error message text.
EID-2225	A valid signal could not be detected while trying to complete the roll. {0}	Roll can be completed only when a valid signal is detected. If not, the roll completion may result in an error.
EID-2226	The circuit roll failed. {0}	Refer to the error message text.
EID-2320	This VCAT circuit does not support deletion of its member circuits.	You can not delete a circuit that is a member of VCAT circuit.
EID-2321	An error occurred while deleting member circuits. {0}	Refer to the error message text.
WID-2322	Not all cross-connects from selected circuits could be merged into the current circuit. They might appear as partial circuits.	Refer to the warning message text.
EID-2323	The circuit roll failed. Bridge and roll is not supported on monitor circuits.	A monitor circuit does not support Bridge and Roll.
EID-2324	An error occurred during the circuit upgrade. {0}	Refer to the error message text.
EID-2325	You have failed {0} times to unlock this session. CTC will exit after you click OK or close this dialog box.	The maximum amount of attempts to unlock this session has been reached.
WID-2326	Currently, CTC does not support bridge and roll on circuits that are entirely created by TL1. To continue with bridge and roll in CTC, the selected circuits must be upgraded. Is it OK to upgrade the selected circuits and continue the bridge and roll operation?	Refer to the warning message text.
WID-2327	Currently, CTC does not support bridge and roll on circuits that are partially created by TL1. To continue with bridge and roll in CTC, the selected circuits must be upgraded. Is it OK to upgrade the selected circuits and continue the bridge and roll operation?	Refer to the warning message text.
EID-2328	An error occurred during the circuit reconfiguration. {0}	The attempt to reconfigure the specified circuit has failed.
EID-2329	{0} of {1} circuits could not be successfully created.	A few circuits could not be created.
EID-2330	An error occurred during circuit verification. The selected {0} is invalid! {1}	The selected item, specified by {0}, is invalid as per the details, specified in {1}.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-2331	Deleting {0} might be service affecting.	Deleting the item can affect the service of CTC.
EID-2332	A validation error occurred in row {0}. {1} hold-off timer for {2} must be between {3}-10,000 ms, in steps of 100 ms.	Refer to the error message text.
EID-2333	The SSLIOP port cannot have the same port value as IIOP port. Please change it and apply again.	Refer to the error message text.
EID-3001	An Ethernet RMON threshold with the same parameters already exists. Please change one or more of the parameters and try again.	Change a few parameters in an Ethernet remote monitoring (RMON) threshold and try again.
EID-3002	An error occurred while retrieving defaults from the node: {0}	There was an error while retrieving the defaults from the specified node.
EID-3003	The file {0} cannot be loaded.	CTC cannot load the specified file.
EID-3004	Properties cannot be loaded from the node.	Refer to the error message text.
EID-3005	NE update properties cannot be saved to the file {0}.	CTC cannot save the network element (NE) update values to the specified file.
EID-3006	NE update properties cannot be loaded from the node.	Refer to the error message text.
EID-3007	An error occurred while provisioning the {0}.	There was a provisioning error for the specified item.
EID-3008	This is not a valid card.	You cannot perform DWDM automatic node setup (ANS) from the card view. Please navigate to the node view and try again.
EID-3009	No {0} was selected.	Select the specified item, for example, VLAN, port, slot, etc.
EID-3010	A bidirectional optical link could not be created.	Refer to the error message text.
EID-3016	The subnet address is invalid.	Refer to the error message text.
EID-3017	The subnet address already exists.	Refer to the error message text.
EID-3019	The internal subnet address is incomplete.	Enter the complete internal subnet address.
EID-3020	The subnet address cannot be the same for both TSC cards. The requested action is not allowed.	A node's internal subnet must be different from one another as each TSC is on separate ethernet buses, isolated by broadcast domains.
EID-3021	An error occurred while retrieving the diagnostics: {0}	Refer to the error message text.
EID-3022	The requested action is not allowed.	The requested action is not allowed.
EID-3023	The low order cross-connect mode could not be retrieved.	Refer to the error message text.
EID-3024	The {0} cross-connect mode could not be switched. Please verify that the type and/or number of circuits provisioned does not exceed the criterion for switching modes.	CTC cannot switch the cross-connect mode for the specified item, as the type or the number of circuits does not match with the criterion for switching modes.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-3025	An error occurred while retrieving thresholds.	There was an error retrieving the thresholds.
EID-3026	The send DoNotUse attribute cannot be modified.	You cannot modify the Send DoNotUse field.
EID-3027	The SyncMsg attribute cannot be modified.	You cannot modify the SyncMsg field.
EID-3028	The port type cannot be changed.	You cannot change the port type.
EID-3029	Unable to switch to the byte because an overhead change is present on this byte of the port.	Refer to the error message text.
EID-3031	An error occurred while hard-resetting the card.	There was an error while resetting card hardware.
EID-3032	An error occurred while resetting the card.	There was an error while resetting the card.
EID-3033	The lamp test is not supported on this shelf.	Refer to the error message text.
EID-3035	The cross-connect diagnostics cannot be performed	Refer to the error message text.
EID-3036	The cross-connect diagnostics test is not supported on this shelf.	The cross-connect diagnostics test is not supported on this shelf.
EID-3039	An error occurred while changing the card type.	There was an error while changing the card.
EID-3040	The card type is invalid.	The selected card type is invalid.
EID-3041	An error occurred while applying changes.	CTC is unable to create a protection group. Check if the protect port supports circuits, a timing reference, SONET RS-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 the error message text.
EID-3046	The flow control watermark value must be between {0} and {1}, inclusive.	The flow control watermark value must be between the two specified values.
EID-3047	The file {0} could not be read. Please verify the name and try again.	Refer to the error message text.
EID-3048	There is no Cisco IOS startup configuration file available to download.	CTC could not find the configuration file for Cisco IOS startup.
EID-3049	The download cannot be done at this time because an update in progress.	Refer to the error message text.
EID-3050	An error occurred while trying to save the file to your local file system.	Check whether the file already exists and cannot be over written, or there is a space constraint in the file system.
EID-3051	The configuration file has a maximum size of {0} bytes.	The size of the configuration file should not exceed the specified number of bytes.
EID-3052	An error occurred while saving the configuration file to the TCC2/TCC2P.	Refer to the 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.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-3054	The provisioned input/output ports cannot be removed or another user is updating the card. Please try to remove these ports later.	Another user may be updating the card. You can try again later.
EID-3055	The soak maintenance pane cannot be created.	Refer to the error message text.
EID-3056	Defaults cannot be saved to the file {0}.	CTC cannot save the defaults to the specified file.
EID-3057	Default properties cannot be loaded from the node.	Refer to the error message text.
EID-3058	The file {0} does not exist.	Refer to the error message text.
EID-3059	An error occurred while refreshing.	There was an error while refreshing.
EID-3060	The ALS recovery pulse interval must be between {0} seconds and {1} seconds.	The automatic laser shutdown (ALS) Recovery Interval must be between the specified range of seconds.
EID-3061	The ALS recovery pulse duration must be between {0} seconds and {1} seconds.	The ALS Recovery Duration must be between the specified range of seconds.
EID-3062	An error occurred while setting values in the table.	Refer to the error message text.
EID-3064	This is not a G1000 card.	This card is not a G1000-4 card.
EID-3065	An error occurred while attempting to create this RMON threshold: {0}	You must wait some time before you try again.
EID-3066	The sample period must be between 10 and {0}.	Refer to the error message text.
EID-3067	The rising threshold must be between 1 and {0}.	This is an invalid rising threshold entry. The valid range is from 1 to the specified value.
EID-3068	The falling threshold must be between 1 and {0}.	This is an invalid falling threshold entry. The valid range is from 1 to the specified value.
EID-3069	The rising threshold must be greater than or equal to the falling threshold.	Refer to the error message text.
EID-3070	Error in data for ports {0} Exactly one VLAN must be marked untagged for each port. These changes will not be applied.	CTC encountered data error for the specified ports. Only one VLAN should be marked untagged for each port.
EID-3071	An error occurred while retrieving the learned address list.	Unable to retrieve the learned MAC address from the NE.
EID-3072	An error occurred while clearing the learned address.	Failure attempting to clear the learned MAC address from a specific card or Ether group.
EID-3073	An error occurred while clearing the selected rows.	Failure attempting to clear the learned MAC address from a specific card or Ether group.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-3074	An error occurred while clearing the learned address list by {0}.	Error encountered trying to clear the learned MAC address from either a VLAN or a port.
EID-3075	At least one row in the parameter column must be selected.	Refer to the error message text.
EID-3076	CTC lost its connection with this node. The NE Setup Wizard will exit.	Refer to the error message text.
EID-3077	No optical link was selected.	Refer to the error message text.
EID-3078	An optical link could not be created.	Refer to the error message text.
EID-3079	Defaults cannot be applied to the node. {0}	CTC cannot apply the defaults to the specified node.
EID-3080	CTC cannot navigate to the target tab. {0}	CTC cannot go to the specified target tab.
EID-3081	The port type cannot be changed.	Refer to the error message text.
EID-3082	The {0} extension byte cannot be changed.	You cannot modify the specified extension byte.
EID-3084	An error occurred while retrieving laser parameters for {0}.	There is no card, or there was an internal communications error when attempting to get the laser parameters for the card.
EID-3085	No OSC Terminations were selected	Select an OSC termination and proceed.
EID-3086	One or more Osc terminations could not be created.	Refer to the error message text.
EID-3087	The OSC termination could not be edited.	Refer to the error message text.
EID-3088	No {0} card is present to switch.	No card of the specified type is available to switch.
EID-3089	The {0} state cannot be used or changed when the {1} has failed or is missing.	You cannot use or change the specified state when the card is failed or missing.
EID-3090	The operation cannot be performed because the {0} is {1}LOCKED_ON/LOCKED_OUT.	You cannot perform operation.
EID-3091	The operation cannot be performed because the protect card is active.	Refer to the error message text.
EID-3092	The requested action cannot be applied because the service state is invalid.	Select another service state and proceed.
EID-3093	The operation cannot be performed because the duplex pair is {0}locked.	Refer to the error message text.
EID-3094	The operation cannot be performed because no cross-connect redundancy is available.	You cannot perform the requested operation on the cross connect card without having a backup cross connect card.
EID-3095	The deletion failed because the circuit is in use	Refer to the error message text.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
WID-3096	An internal communication error was encountered while retrieving laser parameters. This can happen when equipment is not present or when equipment is resetting. Check the equipment state and try to refresh the values again.	Refer to the warning message text.
EID-3097	The ring termination is in use.	The ring termination you are trying to access is in use. Try after sometime.
EID-3098	No ring terminations were selected.	Select one of the ring terminations.
EID-3099	The entered key does not match the existing authentication key.	Check the authentication key and reenter.
EID-3100	An error occurred during authentication.	There was an error in authentication. Verify that the key does not exceed the character limit.
EID-3101	The DCC metric must be between 1 and 65535.	The DCC metric should be in the range of 1 to 65535.
EID-3102	The DCC metric is invalid.	There was an invalid DCC metric.
EID-3103	The IP address {0} is invalid}.	The IP address is invalid.
EID-3104	The router priority must be between 0 and 255.	The router priority should be in the range of 0 to 255.
EID-3105	The router priority is invalid.	The router priority is invalid.
EID-3106	The hello interval must be between 1 and 65535.	The hello interval should be in the range of 1 to 65535.
EID-3107	The hello interval is invalid.	The hello interval is invalid.
EID-3109	The dead interval must be between 1 and 2147483647.	The dead interval value must be between 1 and 2147483647.
EID-3110	The dead interval must be larger than the hello interval.	Refer to the error message text.
EID-3111	The LAN transmit delay must be between 1 and 3600 seconds.	The LAN transit delay should be in the range of 1 to 3600 seconds.
EID-3112	The transmit delay is invalid.	The transmit delay is invalid.
EID-3113	The retransmit interval must be between 1 and 3600 seconds.	The retransmit interval should be in the range of 1 to 3600 seconds.
EID-3114	The retransmit interval is invalid.	The retransmit interval is invalid.
EID-3115	The LAN metric must be between 1 and 65535.	The LAN metric should be in the range of 1 to 65535.
EID-3116	The LAN metric is invalid.	The LAN metric is invalid.
EID-3117	If OSPF is active on the LAN, no DCC area IDs may be 0.0.0.0. Please change all DCC area IDs to non-0.0.0.0 values before enabling OSPF on the LAN.	Refer to the error message text.
EID-3118	If OSPF is active on the LAN, the LAN area ID cannot be the same as the DCC area ID.	LAN must be part of a different OSPF area other than the DCC network.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-3119	An error occurred during validation.	CTC was unable to validate the values entered by the user. This error message is common to several different provisioning tabs within CTC (examples include the SNMP provisioning tab, the General > Network provisioning tab, the Security > Configuration provisioning tab, etc.).
EID-3120	No object of type {0} was selected for deletion.	Choose an object of the specified type to delete.
EID-3121	An error occurred while deleting {0}.	There is an error deleting the item.
EID-3122	No object of type {0} was selected to edit.	Choose an object of the specified type to edit.
EID-3123	An error occurred while editing {0}.	There was an error editing the item.
EID-3124	The {0} termination is in use. Delete the associated OSPF range table entry and try again.	Refer to the error message text.
EID-3125	No {0} terminations were selected.	No specified terminations are selected.
EID-3126	The {0} termination could not be edited.	CTC could not edit the specified termination.
EID-3127	Orderwire cannot be provisioned because the E2 byte is in use by {0}.	Refer to the error message text.
EID-3128	The authentication key cannot exceed {0} characters.	The authentication key cannot exceed the specified number of characters.
EID-3129	The authentication keys do not match!	Refer to the error message text.
EID-3130	An error occurred while creating the OSPF area virtual link.	CTC encountered an error while creating the area virtual link.
EID-3131	An error occurred while creating the OSPF virtual link.	CTC encountered an error creating the virtual link.
EID-3132	An error occurred while setting the OSPF area range: {0}, {1}, false.	CTC encountered an error while setting the area range for the specified values.
EID-3133	The maximum number of OSPF area ranges has been exceeded.	OSPF area ranges exceeded the maximum number.
EID-3134	The area ID is invalid. Use the DCC OSPF area ID, LAN port area ID, or 0.0.0.0.	Refer to the error message text.
EID-3135	The mask is invalid.	Refer to the error message text.
EID-3136	The range address is invalid.	The range address is invalid. Try again.
EID-3137	Your request has been denied because the timing source information was updated while your changes were still pending. Please retry.	Refer to the error message text.
EID-3138	The clock source for switching is invalid.	You have selected an invalid clock source. Choose another clock.
EID-3139	A switch cannot be made to a reference of inferior quality.	Refer to the error message text.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-3140	A higher priority switch is already active.	You cannot switch the timing source manually when a higher priority switch is already active.
EID-3141	An attempt was made to access a bad reference.	Refer to the error message text.
EID-3142	No switch is active.	None of the switches are active.
EID-3143	An error occurred while creating the static route entry.	CTC encountered an error while a creating static route entry.
EID-3144	The maximum number of static routes has been exceeded.	The number of static routes has exceeded its limit.
EID-3145	The RIP metric must be between 1 and 15.	The Routing Information Protocol (RIP) metric should be in the range of 1 to 15.
EID-3146	The RIP metric is invalid.	Refer to the error message text.
EID-3147	An error occurred while creating the summary address.	There was an error while creating the summary address.
EID-3148	No Layer 2 domain has been provisioned.	You must provision any one of the Layer 2 domain.
EID-3149	The MAC addresses could not be retrieved.	Refer to the error message text.
EID-3150	The target file {0} is not a normal file.	The specified target file is not a normal file.
EID-3151	The target file {0} is not writable.	The target file is not writeable. Specify another file.
EID-3152	An error occurred while creating the protection group.	CTC encountered an error creating Protection Group.
EID-3153	The card cannot be deleted because it is in use.	Refer to the error message text.
EID-3154	An error occurred while provisioning the card: CTC cannot {0} the card.	CTC cannot perform the task on the card.
EID-3155	An error occurred while building the menu.	CTC encountered an error building the menu.
EID-3156	An error occurred while building the menu. Cards were not found for the {0} group.	CTC encountered an error while building the menu, as cards could not be found for the specified group).
EID-3157	The selected model could not be set because of an unexpected model class: {0}.	CTC encountered an unexpected model class while trying to complete the task.
EID-3158	Probable causes: - Unable to switch, because a similar or higher priority condition exists on a peer or far-end card. - A loopback is present on the working port.	Refer to the error message text.
EID-3159[1]	An error occurred while applying the operation.	CTC encountered an error while applying this operation.
EID-3160	An error occurred while provisioning the {0}.	CTC encountered the specified error.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-3161	An error occurred while upgrading the ring.	An error was encountered while attempting to upgrade the MS-SPRing. Refer to the details portion of the error dialog box for more information.
EID-3162	This protection operation cannot be set because the protection operation on the other side has been changed but not yet applied.	Refer to the error message text.
EID-3163	The data in row {0} cannot be validated.	CTC cannot validate the data for the specified row.
EID-3164	The new node ID ({0}) for ring ID {1} duplicates the ID of node {2}.	The new specified node ID for the specified ring ID is the same as another node ID.
EID-3165	The ring ID provided is already in use. Ring IDs must be unique.	Refer to the error message text.
EID-3166	An error occurred while refreshing the {0} table.	CTC encountered an error while refreshing the specified table.
EID-3167	The slot is already in use.	Refer to the error message text.
EID-3168	An error occurred while provisioning.	An error was encountered while attempting the specified provisioning operation. Refer to the details portion of the error dialog box for more information.
EID-3169	An error occurred while adding the card.	CTC encountered an error while adding the card.
EID-3170	You cannot delete this card: {0}.	Refer to the error message text.
EID-3171	An error occurred while creating the trap destination.	CTC encountered an error creating the trap destination.
EID-3172	No RMON thresholds were selected.	Select an RMON threshold.
EID-3173	The contact "{0}" cannot exceed {1} characters.	The specified contact exceeds the specified character limit.
EID-3174	The description "{0}" cannot exceed {1} characters.	The specified location exceeds the specified character limit.
EID-3175	The operator identifier "{0}" cannot exceed {1} characters.	The specified operator identifier exceeds the specified character limit.
EID-3176	The operator specific information "{0}" cannot exceed {1} characters.	The specified operator specific information exceeds the specified character limit.
EID-3177	The node name cannot be empty.	The specified name is empty.
EID-3178	The node name "{0}" cannot exceed {1} characters.	The specified name exceeds the specified character limit.
EID-3179	The protect card is in use.	Refer to the error message text.
EID-3180	The 1+1 protection group does not exist.	Create a 1+1 protection group.
EID-3181	The Y-cable protection group does not exist.	Refer to the error message text.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-3182	The topology element is in use and cannot be deleted as requested.	You cannot delete the topology element which is in use.
EID-3183	An error occurred while deleting the protection group.	CTC encountered an error while deleting the protection group.
EID-3184	No {0} was selected.	You must select an item before completing this task.
EID-3185	This ring has an active protection switch operation and cannot be deleted at this time.	Refer to the error message text.
EID-3186	The node is busy: {0} is {1} and cannot be deleted as requested.	The request cannot be completed.
EID-3187	An error occurred while deleting the trap destination.	CTC encountered an error deleting the trap destination.
EID-3188	An error occurred during authentication. The password entered is invalid.	The password you entered is invalid. Enter the password again.
EID-3189	The sum of the {0} must be between {1} and {2}.	Refer to the error message text.
EID-3214	The number of high order circuits for the line could not be retrieved.	The number of High Orders (STS/STM) for the line is not available.
EID-3215	An error occurred while refreshing.	Used frequently in pane classes to indicate a general error condition when trying to refresh from the model.
EID-3216	The proxy port is invalid.	Refer to the error message text.
EID-3217	The statistics could not be refreshed.	CTC could not refresh statistics values.
EID-3218	The automatic node setup could not be launched.	Refer to the error message text.
EID-3219	The automatic node setup information could not be refreshed.	Failure trying to retrieve automatic node setup information.
EID-3220	An error occurred while refreshing row {0}.	Error refreshing the specified row.
EID-3222	The statistics could not be cleared.	Refer to the error message text.
EID-3225	An error occurred while refreshing the pane.	Used frequently in pane classes to indicate a general error condition when trying to refresh from the model.
EID-3226	The {0} termination(s) could not be deleted. {1}	Refer to the error message text.
EID-3227	A baseline could not be recorded. Performance metrics will remain unchanged.	CTC failed to set the baseline values while provisioning NE. Previous values remain unchanged.
EID-3228	The {0} termination(s) could not be created. {1}	Refer to the error message text.
EID-3229	RIP is active on the LAN. Please disable RIP before enabling OSPF.	Turn off RIP on the LAN, before enabling OSPF.
EID-3230	OSPF is active on the LAN. Please disable OSPF before enabling RIP.	Turn off the OSPF on the LAN before enabling RIP.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-3231	An error occurred while setting the OPR.	An error was encountered while attempting to provision the optical power received (OPR).
WID-3232	The port state cannot be indirectly transitioned because the port is still providing services. If the port state should be changed, edit it directly through port provisioning.	Edit the port state while provisioning the port.
EID-3233	The current loopback provisioning does not allow this state transition.	Refer to the error message text.
EID-3234	The current synchronization provisioning does not allow this state transition.	You cannot transition the port state to the target date while in the current synchronization state.
EID-3235	The requested state transition cannot be performed on this software version.	Refer to the error message text.
EID-3236	The database restore failed. {0}	CTC failed to restore the specified database.
EID-3237	The database backup failed. {0}	CTC failed to backup the specified database.
EID-3238	The send PDIP setting on {0} is inconsistent with the setting on the control node {1}.	The send payload defect indicator path (PDI-P) setting on the specified item should be consistent with that of the specified control node.
EID-3239	The overhead termination is invalid	Refer to the error message text.
EID-3240	The maximum number of overhead terminations has been exceeded.	Overhead terminations have exceeded the limit.
EID-3241	The {0} termination port is in use.	The specified termination port is in use. Select another port.
EID-3242	An {1} exists on the selected ports. Therefore, you must create the {0}s one by one.	The specified DCC already exists on the selected port. You can create a DCC of another type.
WID-3243	The port you have chosen as an {0} endpoint already supports an {1}. The port cannot support both DCCs. After the {0} is created, verify that no EOC alarms are present and then delete the {1} to complete the downgrade.	The same port can not be used by multiple DCCs.
EID-3244	An {0} exists on the selected ports. Therefore, you must create the {1}s one by one.	The specified DCC already exists on the selected port. You can create a DCC of another type.
WID-3245	The port you have chosen as an {1} endpoint already supports an {0}. The port cannot support both DCCs. After the {1} is created, verify that no EOC alarms are present and then delete the {0} to complete the upgrade.	The port selected as a DCC endpoint already supports another DCC. Refer to the warning message text.
EID-3246	The wizard was not able to validate the data. {0}	CTC encountered an error.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-3247	An ordering error occurred. The absolute value should be {0}.	The absolute value entered was wrong.
EID-3248	The value for the parameter {0} is invalid.	CTC changed the incorrect parameter.
EID-3249	The voltage increment value is invalid.	Refer to the error message text.
EID-3250	The power monitor range is invalid.	Refer to the error message text.
EID-3251	The requested action could not be completed. {0}	CTC could not complete the specified action.
EID-3252	No download has been initiated from this CTC session.	Refer to the error message text.
EID-3253	The reboot operation failed. {0}	Refer to the error message text.
EID-3254	An error occurred during validation. {0}	The CTC was unable to validate the values entered by the user, specified by {0}. This error message is common to several different provisioning tabs within the CTC.
EID-3255	You cannot change the timing configuration because a Manual/Force operation is in effect.	Refer to the error message text.
WID-3256	The timing reference(s) could not be assigned because one or more of the timing reference(s): - is already used and/or - has been selected twice and/or - is attempting to use the same slot twice. Please verify the settings.	Refer to the warning message text.
EID-3257	Duplicate DCC numbers are not permitted. {0}.	CTC detected more than one occurrence of the a DCC number. Remove one of them.
EID-3258	A software error occurred while attempting to download the file. Please try again later.	Refer to the error message text.
EID-3259	An error occurred while creating the FC-MR threshold.	You must create a Fibre Channel Multirate (FC_MR) card threshold.
EID-3260	An error occurred while provisioning the internal subnet: {0}	The specified internal subnet could not be provisioned.
EID-3261	The port rate provisioning cannot be changed while circuits exist on this port.	Refer to the error message text.
EID-3262	The port provisioning cannot be changed when the port status is {0}.	You must provision the ports only when the port is Out of Service.
WID-3263	You are using Java version {0}. CTC should run with Java version {1}. It can be obtained from the installation CD or http://java.sun.com/j2se/	CTC is being launched with the wrong version of the JRE {0}. This version of CTC requires a particular version of the JRE {1}. The CTC and browser must be closed and restarted to allow the correct Java version to be loaded.
EID-3265	An error occurred while modifying the protection group.	The protection group could not be modified.
EID-3266	Conditions could not be retrieved from the shelf or card view.	Refer to the error message text.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
WID-3267	The XTC protection group cannot be modified.	Refer to the warning message text.
WID-3268	The filter entry is invalid. {0}	The specified entry is invalid.
WID-3269	The {0} operation was successfully initiated for {1} but its completion status could not be obtained from the node. When the node is accessible, check its software version to verify if the {0} succeeded.	Refer to the error message text.
WID-3270	The file {0} does not exist.	The specified file does not exist.
WID-3271	The value entered must be greater than {0}.	The value entered must be greater than the specified value.
WID-3272	An entry is required.	An entry is required to complete this task.
WID-3273	{0} already exists in the list.	The specified item already exists in the list.
WID-3274	A software upgrade is in progress. Network configuration changes that result in a node reboot cannot take place during a software upgrade. Please try again after the software upgrade is done.	Refer to the warning message text.
WID-3275	Ensure that the remote interface ID and the local interface ID on the two sides match. (The local interface ID on this node should equal the remote interface ID on the neighbor node and vice-versa).	Refer to the warning message text.
WID-3276	Both {0} and {1} exist on the same selected port. {2}	The specified port has both MS-DCC and RS-DCC.
WID-3277	The description cannot exceed {0} characters. Your input will be truncated.	The input exceeds the character limit. The value will be truncated to the maximum character limit.
WID-3279	This card has been deleted. CTC will return to the shelf view.	CTC returns to node view.
WID-3280	ALS will not engage until both the protected trunk ports detect LOS.	Refer to the warning message text.
WID-3282	Performing a software upgrade while TSC 5 is active could result in a service disruption. It is recommended that you make TSC 10 the active TSC by performing a soft reset of TSC 5. The following ONS 15600s are currently unsafe to upgrade...	Refer to the warning message text.
WID-3283	Before activating a new version, ensure that you have a database backup from the current version.	Refer to the warning message text.
WID-3284	Reverting to an older version.	CTC is being reverted to an older version of application.
WID-3285	Applying FORCE or LOCKOUT operations might result in traffic loss.	Refer to the warning message text.
WID-3286	The ring status is INCOMPLETE. CTC cannot determine if there are existing protection operations or switches in other parts of the ring. Applying a protection operation at this time could cause a traffic outage. Please confirm that no other protection operations or switches exist before continuing.	Refer to the warning message text.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
WID-3287	There is a protection operation or protection switch present on the ring. Applying this protection operation now will probably cause a traffic outage.	Refer to the warning message text.
WID-3288	The status of this ring is INCOMPLETE. CTC will not be able to apply this change to all of the nodes in the {0}.	Change the ring status to apply the change to all nodes in the ring type.
EID-3290	The specified provisionable patchcord(s) could not be deleted.	Refer to the error message text.
EID-3291	The revertive behavior cannot be changed because a protection switch is active.	Protection switch should not be active to change the revertive behavior.
EID-3292	An error occurred while resetting the shelf.	CTC encountered an error while resetting the node.
EID-3293	No such provisionable patchcords exists.	You are attempting to delete a provisionable patchcord that does not exist. This happens when multiple instances of CTC are running and attempting to delete the same provisionable patchcord concurrently.
EID-3294	No RMON thresholds are available for the selected port.	Refer to the error message text.
EID-3295	This card does not support RMON thresholds.	Refer to the error message text.
EID-3296	Buffer-to-buffer credit is only supported for Fibre Channel (FC) and FICON.	Refer to the error message text.
EID-3298	This interfaces does not support ALS auto restart.	Refer to the error message text.
EID-3300	Duplicate OSPF area IDs are not permitted.	OSPF area IDs should be unique.
EID-3301	The LAN metric cannot be zero.	Refer to the error message text.
EID-3302	The standby {0} is not ready.	Standby controller card is not ready.
EID-3303	The DCC area ID and {0} conflict. {1}	DCC Area ID and ring type, specified by {0}, conflict each other due to the details specified by {1}.
EID-3304	The DCC number is out of range.	Enter a DCC number that is within the range.
EID-3305	OSPF cannot be active on the LAN interface when the backbone area is set on a DCC interface.	You cannot have the default OSPF area on a DCC while OSPF is enabled on the LAN.
EID-3306	Ethernet circuits must be bidirectional.	Refer to the error message text.
EID-3307	An error occurred while creating a connection object at {0}.	CTC encountered an error at the specified connection while creating the connection.
EID-3308	DWDM links can be used only for optical channel circuits.	Refer to the error message text.
EID-3309	The link was excluded because it was in the wrong direction.	The optical channel (circuit) does not allow the specified link to be included because it is in the wrong optical direction.
EID-3310	The DWDM link does not have wavelengths available.	Refer to the error message text.
EID-3311	The laser is already on.	Refer to the error message text.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-3312	The power setpoint cannot be changed. {0} {1}	CTC cannot change the power setpoint. The new setpoint would either make the thresholds inconsistent or set the fail threshold outside the range.
EID-3313	The offset cannot be modified because the service state of the port is IS.	Refer to the error message text.
EID-3314	The requested action is not allowed. The state value is invalid.	Refer to the error message text.
EID-3315	This operation cannot be performed.	CTC is unable to perform operation.
EID-3316	The node side is invalid.	This task was applied to the wrong node side.
EID-3317	The ring name is too long.	Reduce the number of characters in the name.
EID-3318	The ring name is invalid.	The name you entered is illegal.
EID-3319	The wrong line was selected.	Select another line.
EID-3320	The optical link could not be deleted.	CTC cannot delete the optical link.
EID-3321	This feature is unsupported by this version of software.	Refer to the error message text.
EID-3322	The equipment is not plugged in.	Plug in the equipment and proceed.
EID-3323	The APC system is busy.	Automatic power control (APC) system is busy.
EID-3324	There is no path to regulate.	There is no circuit path to regulate.
EID-3325	The requested action is not allowed.	Generic DWDM provisioning failure message.
EID-3326	The input was invalid.	The input value is incorrect.
EID-3327	An error occurred while retrieving thresholds.	There was an error retrieving the thresholds. This message is displayed only for the OSCM/OSC-CSM line thresholds.
EID-3328	An error occurred while applying changes to row {0}. The value is out of range.	There was an error applying the changes to the specified row. The value is out of range.
EID-3330	Unable to switch to the byte because an overhead channel is present on this byte of the port.	Refer to the error message text.
EID-3331	An error occurred while applying changes to the row.	Refer to the error message text.
EID-3334	Timing parameters on the protect port cannot be changed.	You cannot change timing parameters on protect port.
EID-3335	The port type cannot be changed because the SDH validation check failed. Check if this port is part of a circuit, protection group, SONET DCC, orderwire, or UNI-C interface.	Refer to the error message text.
EID-3336	An error occurred while reading a control mode value.	The Control Mode must be retrieved.
EID-3337	An error occurred while setting a set point gain value.	The Gain Set Point must be set.
EID-3338	An error occurred while reading a set-point gain value.	The Gain Set Point must be retrieved.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-3339	An error occurred while setting a tilt calibration value.	The tilt calibration must be set.
EID-3340	An error occurred while setting expected wavelength.	The expected wavelength must be set.
EID-3341	An error occurred while reading expected wavelength.	The expected wavelength must be retrieved.
EID-3342	An error occurred while reading actual wavelength.	The actual wavelength must be retrieved.
EID-3343	An error occurred while reading actual band.	The actual band must be retrieved.
EID-3344	An error occurred while reading expected band.	The expected band must be retrieved.
EID-3345	An error occurred while setting expected band.	The expected band must be set.
EID-3346	An error occurred while retrieving defaults from the node: {0}.	There was an error retrieving defaults from the specified node.
EID-3347	The file {0} cannot be loaded.	CTC cannot load the specified file.
EID-3348	Properties cannot be loaded from the node.	Refer to the error message text.
EID-3349	NE update properties cannot be saved to a file.	Check your file system for space constraint or any other problem.
EID-3350	NE update properties cannot be loaded from the node.	Refer to the error message text.
EID-3351	The file {0} does not exist.	The specified file does not exist.
EID-3352	An error occurred while setting a value at {0}.	There was an error while setting the value at the specified location.
EID-3353	No such interface is available.	The interface specified is not present in CTC.
EID-3354	The specified endpoint is in use.	Select another endpoint that is not in use.
EID-3355	The specified endpoint is incompatible.	Refer to the error message text.
EID-3357	The connections could not be calculated.	Refer to the error message text.
EID-3358	An optical link model does not exist for the specified interface.	Create an optical link model for the interface, and proceed.
EID-3359	Optical parameters could not be set for the node.	Refer to the error message text.
EID-3360	ANS cannot be performed. Please check {0} parameter value.	Refer to the error message text.
EID-3361	The ring termination is in use. An error occurred while deleting the ring termination.	You cannot delete a ring in use.
EID-3362	An error occurred while deleting the ring termination.	There was an error while deleting ring termination.
EID-3363	No ring terminations were selected.	You must select a ring termination.
EID-3364	An error occurred while creating the ring ID.	There was an error while creating the ring ID.
EID-3365	The OSC termination is in use.	Select another optical service channel (OSC) which is not in use.
EID-3366	The OSC termination could not be deleted.	There was an error deleting the OSC termination.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-3370	No optical link was selected.	You must select an optical link.
EID-3371	An error occurred while calculating the automatic optical link list.	Refer to the error message text.
EID-3372	CTC attempted to access an OCHNC connection that has been destroyed.	CTC destroyed an external attempt to access an optical channel network connection.
EID-3375	The expected span loss must be set.	Refer to the error message text.
EID-3376	The measured span loss could not be retrieved.	Refer to the error message text.
EID-3377	The wrong interface was used.	The interface used for the card is wrong.
EID-3378	This is a duplicate origination patchcord identifier.	The provisionable patchcord identifier to the patchcord you are attempting to provision is already in use by another patchcord on the origination node.
EID-3379	This is a duplicate termination patchcord identifier.	The provisionable patchcord identifier to the patchcord you are attempting to provision is already in use by another patchcord on the remote node.
EID-3380	The host cannot be found.	Refer to the error message text.
EID-3381	The maximum frame size must be between {0} and {1} and may be increased in increments of {2}.	The frame size must be in the specified range. This can be incremented by the specified value.
EID-3382	The number of credits must be between {0} and {1}.	The number of credits must be between the specified values.
EID-3383	The GFP buffers available must be between {0} and {1} and may be increased in increments of {2}.	The GFP buffers must be in the specified range. This can 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. Is it OK to continue?	Refer to the warning message text.
EID-3385	{0}. Delete the circuits and try again.	Refer to the error message text.
EID-3386	The transponder mode could not be provisioned: {0}	The specified transponder mode cannot be provisioned.
EID-3387	You must change port(s) {0} to an out-of-service state before changing card parameters. Click "Reset" to revert the changes.	All the card ports should be changed to out-of-service before changing the parameters.
EID-3388	The card mode cannot be changed because the card has circuits.	Refer to the error message text.
EID-3389	An error occurred while changing the card mode.	Refer to the error message text.
EID-3390	The port is in use.	Refer to the error message text.
EID-3391	The port rate cannot be changed because the port has been deleted.	You cannot change the port rate of a card that has been deleted.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
WID-3392	The timing reference(s) could not be assigned because with external timing, only a single protected, or two unprotected timing references per BITS Out can be selected. Please use the "Reset" button and verify the settings.	Refer to the warning message text.
WID-3393	The timing reference(s) could not be assigned because with line or mixed timing, only a single unprotected timing reference per BITS Out can be selected. Please use the "Reset" button and verify the settings.	Refer to the warning message text.
EID-3394	An error occurred while refreshing the power monitoring values.	Refer to the error message text.
EID-3395	The configuration is invalid. {0}	CTC encountered an error in IP address, net mask length, or default router, or a restricted IIOP port was selected.
EID-3396	The configuration is invalid. The standby controller card is not a TCC2P card.	The standby controller card should be a TCC2P card.
EID-3397	The file {0} is the wrong version.	The specified file is of wrong version.
EID-3398	The PPM cannot be deleted.	Refer to the error message text.
EID-3399	The PPM cannot be deleted because it has port(s) in use.	Remove the ports connected to the Pluggable Port Module before it can be deleted.
EID-3400	Unable to switch. A force to the primary facility is not allowed.	Refer to the error message text.
EID-3401	{0} cannot be provisioned for the port while {1} is enabled.	The relationship between parameters {0} and {1} are such that enabling either one, prevents the provisioning of the other.
EID-3402	The switch request could not be completed. The {0} card is not present or is not responding. Try again after ensuring that the {0} card is present and is not resetting.	Refer to the error message text.
EID-3403	The administrative state transition has not been attempted on the monitored port.	Refer to the error message text.

EID-3404	The far end IP address could not be set on the {0} termination. The IP address cannot be:
	loopback (127.0.0.0/8)
	class D (224.0.0.0/4)
	class E (240.0.0.0/4)
	broadcast (255.255.255.255/32)
	internal {1}
		Refer to the error message text.

EID-3405	You cannot change card parameters with port {0} in {1} state. Click "Reset" to revert the changes.	Refer to the error message text.
EID-4000	The {0} ring name cannot be changed now because a {0} switch is active.	You cannot change the ring name because a switch of the same ring type is active.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-4001	The {0} node ID cannot be changed now because a {0} switch is active.	You cannot change the ring ID because a switch of the same ring type is active.

WID-4002	CAUTION: Reverting to an earlier software release may result in TRAFFIC LOSS and loss of connectivity to the node. It may require onsite provisioning to recover.
	If the node was running {0} before, reverting will restore the {0} provisioning, losing any later provisioning. If the node was running some other version, reverting will LOSE ALL PROVISIONING.
	{1}
	{2}
		Refer to the warning message text.

EID-4003	The Cisco IOS console is disabled for the card in Slot {0}.	The card might not be a Cisco IOS-based card or it may be rebooting.
EID-4004	An error occurred while canceling the software upgrade.	CTC encountered an error while canceling the software upgrade.
EID-4005	{0} encountered while performing a database backup.	CTC encountered the specified error during database backup.
EID-4006	The file {0} does not exist or cannot be read.	Refer to error message.
EID-4007	The size of the file {0} is zero.	The size of the file that is being backed up or restored is zero.
WID-4008	A software upgrade is in progress. {0} cannot proceed during a software upgrade. Please try again after the software upgrade has completed.	The specified action cannot be performed during a software upgrade. You must try after the upgrade process is completed.
EID-4009	{0} encountered while restoring the database.	CTC encountered the specified error while restoring the database.
EID-4010	The operation was terminated because: {0}	Refer to the error message text.
EID-4011	An error occurred during provisioning: {0}	Refer to the error message text.
WID-4012	Node management for {0} is not provided.	Refer to the warning message text.

EID-4013	CAUTION: Reverting to an earlier software release may result in TRAFFIC LOSS and loss of connectivity to the node. It may require onsite provisioning to recover.
	If the node was running {0} before, reverting will restore the {0} provisioning, losing any later provisioning. If the node was running some other version, reverting will LOSE ALL PROVISIONING.
	{1}
	{2}
	{3}
		Refer to the error message text.

EID-4014	The manual path trace mode for this equipment does not support an expected string consisting of all null characters. Please change the expected string or the path trace mode.	The path trace mode does not support strings that consist of null characters. You must either change the expected string or the path trace mode.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-4015	Software activation is in progress. Provisioning is not allowed.	Refer to the error message text.
EID-4016	Software activation is in progress. {0} is not allowed.	Refer to the error message text.
EID-4017	Path Trace mode cannot be set at this endpoint. The circuit is one-way.	Refer to the error message text.
WID-4018	{0} already exists. Do you want to replace it?	Refer to the warning message text.
EID-4019	Profile cannot be mapped because the UNI Port is not in transparent mode.	Refer to the error message text.
EID-4020	Profile cannot be mapped because the transparent mode UNI Port tagged VLAN is not {0}.	Refer to the error message text.
EID-4021	Profile cannot be mapped because SVLAN {0} is not enabled for the NNI Port.	Refer to the error message text.
EID-4022	The user already exists.	Refer to the error message text.
EID-4023	Access control already exists for the group selected.	Refer to the error message text.
EID-4024	The View already exists.	Refer to the error message text.
EID-4025	Invalid Mask entry, cant be more then {0} the length of OID.	Refer to the error message text.
EID-4026	CTC was unable to create a new view.	Refer to the error message text.
EID-4027	Name and Subtree OID cant be empty.	Refer to the error message text.
EID-4028	Password will be sent as plain text.	Refer to the error message text.
EID-4029	The passwords must be at least {0} characters long.	Refer to the error message text.
EID-4030	The admitted SVLAN values must be in the range [1-4093].	Refer to the error message text.
EID-4031	On {0} interface the Recover from Fiber Cut Fails.	Refer to the error message text.
EID-4032	Link Integrity and L2 1+1 protection cannot operate on the same interface.	Refer to the error message text.
WID-4033	No files were specified. Please enter a valid file name.	Refer to the error message text.
EID-4034	WDMANS parameter already present.	Refer to the error message text.
EID-4035	WDMANS parameter is not valid.	Refer to the error message text.
EID-4036	WDMANS parameter cannot be removed. This may be in use by the system.	Refer to the error message text.
EID-4037	This operation is not supported on the protect entity of a protection group.	Refer to the error message text.
EID-5000	A valid route cannot be found for the tunnel change request.	Refer to the error message text.
EID-5001	The tunnel could not be changed.	Refer to the error message text.
EID-5002	The tunnel could not be restored and must be recreated manually.	Refer to the error message text.
EID-5003	The circuit roll failed. {0}	Refer to the error message text.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-5004	There is already one four-fiber {0} provisioned on the set of nodes involved in {1}. The maximum number of four-fiber {0} rings has been reached for that node.	There is already one 4-fiber MS-SPRing provisioned on the set of nodes involved in the ring. The maximum number of 4-fiber MS-SPRing rings has been reached for that node.
WID-5005	A non-zero hold-off time can violate switching time standards, and should only be used for a circuit with multiple path selectors.	Refer to the warning message text.
WID-5006	Warning: A different secondary {0} node should only be used for DRI or open-ended path protected circuits.	You should use different secondary end point only for DRI or open-ended path protected circuits.
WID-5007	If you change the scope of this view, the contents of this profile editor will be lost.	Refer to the warning message text.
WID-5008	Please ensure that all the protection groups are in proper states after the cancellation.	Refer to the warning message text.
WID-5009	The circuit {0} is not upgradable. No {1} capable {2}s are available at the node {3}.	No VT-capable STSs are available at the node.
EID-5010	The domain name already exists.	Refer to the error message text.
EID-5011	The domain name cannot exceed {0} characters.	You may have reached the maximum number of characters.
WID-5012	The software load on {0} does not support the addition of a node to a 1+1 protection group.	Refer to the warning message text.
EID-5013	{0} does not support the bridge and roll feature. Please select a different port.	The specified port does not support Bridge and Roll.
EID-5014	An automatic network layout is already in progress. Please wait for it to complete before running it again.	You must for the automatic network layout to complete before running it again.
WID-5015	{0} cannot be applied to {1}.	You cannot apply the admin state operation, specified by {0}, to port count, specified by {1}.
EID-5016	An error occurred while attempting to provision the {0}. {1}	CTC encountered an error while provisioning the card.
EID-5017	Provisioning could not be rolled back. The {0} might be left in an INCOMPLETE state and should be manually removed.	You may have to remove the MS-SPRing manually as it was left incomplete.
EID-5018	{0} is a(n) {1} node and cannot be added to a(n) {2} network.	You cannot add the node {0} of type {1} to the host node of type {2}. This prevents you from hosting both SONET and SDH nodes in the same session.
EID-5019	The manual path trace mode for this equipment does not support an expected string consisting of all null characters. Please change the expected string or the path trace mode.	The path trace mode does not support strings that consist of null characters. You must either change the expected string or the path trace mode.
EID-5020	Software activation is in progress. Provisioning is not allowed.	Refer to the warning message text.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-5021	Software activation is in progress. {0} is not allowed.	Refer to the error message text.
WID-5022	Warning: Ethergroup circuits are stateless (that is, always in service). The current state selection of {0} will be ignored.	Refer to the warning message text.
EID-5023	CTC cannot communicate with the node. The operation failed.	CTC encountered a network communication error. Connectivity between CTC and the NE was disrupted, either transiently or permanently.
EID-5024	The overhead circuit will not be upgraded.	Refer to the error message text.
WID-5025	The path targeted for this switch request is already active. The switch request can be applied, but traffic will not switch at this time.	Refer to the warning message text.
EID-5026	An ONS 15600 cannot serve as the primary or secondary node in a four-fiber {0} circuit. Please change your ring and/or node selections so that an ONS 15600 is not chosen as the primary or secondary node in this four-fiber {1} circuit.	Refer to the error message text.
WID-5027	The {0} Edit dialog box for the ring {1} has been closed due to significant provisioning changes. These changes might only be transitory, so you can reopen the {0} Edit dialog box to view the updated state.	Reopen the MS-SPRing edit window to view the updated state of the ring.
WID-5028	Warning: This operation should only be used to clean up rolls that are stuck. It might also affect completeness of the circuit. Is it OK to continue with the deletion?	Refer to the warning message text.
EID-5029	A software downgrade cannot be performed to the selected version while an SSXC card is inserted in this shelf. Please follow the steps to replace the SSXC with a CXC card before continuing the software downgrade.	Refer to the error message text.
EID-5030	A software downgrade cannot be performed at the present time.	Try the software downgrade later.
WID-5031	Canceling a software upgrade during a standby TSC clock acquisition might result in a traffic outage.	Refer to the warning message text.
EID-5032	An error occurred while accepting the load.	Refer to the error message text.
EID-5033	The profile could not be loaded. An error occurred while decoding the characters.	CTC detected an error while decoding characters and could not load the profile.
EID-5034	The profile could not be loaded. An error occurred while trying to recognize the file format.	CTC detected an error and could not load the profile.
EID-5035	The profile could not be loaded. An error occurred while reading the file.	CTC could not read the file and is therefore unable to load the profile.
EID-5036	The GNE hostname {0} is invalid.	The specified host name is invalid. CTC could not resolve the host name to any valid IP address.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-5037	Provisionable patchcords cannot be created between transponder trunk ports and multiplexer/demultiplexer ports on the same node.	You must create provisionable patchcords between transponder trunk ports and multiplexer/demultiplexer ports that are on different nodes.
EID-5038	Provisionable patchcords created between transponder trunk ports and multiplexer/demultiplexer ports must use the same wavelength: {0} is not equal to {1}.	Wavelengths used by provisionable patchcords for transponder trunk ports and multiplexer/demultiplexer ports must be the same.
EID-5039	Provisionable patchcords created between transponder trunk ports and multiplexer/demultiplexer ports must use the same wavelength: {0} is not equal to {1}. Please provision the {2} wavelength on {3}.	Transmitter and receiver port wavelengths are not equal. Provision the receiver and transmitter wavelengths on transmitter and receiver ports respectively.
EID-5040	Provisionable patchcords created between OC3/OC12 ports and multiplexer/demultiplexer ports are not supported.	Refer to the error message text.
EID-5041	Provisionable patchcords created between gray OC-N trunk ports and multiplexer/demultiplexer ports are not supported.	Refer to the error message text.
EID-5042	Provisionable patchcords created between OC-N trunk ports and multiplexer/demultiplexer ports must use the same wavelength: {0} is not equal to {1}.	Wavelengths used by provisionable patchcords for STM-N trunk ports and multiplexer/demultiplexer ports must be the same.
WID-5043	Warning: Only the line card was provisioned. The wavelength compatibility check was skipped.	Refer to the warning message text.
EID-5044	Virtual links can be used only for OCH-Trail circuits.	Refer to the error message text.
EID-5045	The virtual link does not have wavelengths available.	Set wavelengths for the virtual link and proceed.
WID-5046	Warning: if you select "Use OCHNC Direction," your circuit will be limited to nodes prior to release 07.00.	Refer to the warning message text.
EID-5047	Provisionable patchcords created between OC3/OC12 ports are not supported.	Refer to the error message text.
EID-5048	Provisionable patchcords created between gray OC-N trunk ports are not supported.	Refer to the error message text.
EID-5049	Provisionable patchcords created between gray OC-N trunk ports and multiplexer/demultiplexer ports are not supported.	Refer to the error message text.
EID-5050	The element model could not be found. {0}	The specified element model cannot be located.
WID-5051	The port state cannot be indirectly transitioned because the port aggregates OCHCC circuits: if the port state needs to be changed, edit it directly through port provisioning.	Refer to the warning message text.
EID-5052	The operation is not valid for the connection type.	You might have selected the incorrect switch.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-5053	The operation cannot be performed because the connection is under test access.	Refer to the error message text.
EID-5054	The TL1 tunnel could not be opened. {0}	Refer to the error message text.
EID-5055	Some patchcords were not deleted. Patchcords cannot be deleted if they are incomplete or support any circuits, or if the nodes supporting them are not connected.	Refer to the error message text.
EID-5056	This PPC cannot be deleted because one or more circuits are provisioned over it.	Remove the circuits provisioned over the provisionable patchcord before trying to delete it.
EID-5057	The addition of the last node has not yet finished. Please wait before trying to add a new node.	Refer to the error message text.
EID-5058	An OCHNC upgrade is applicable only to bidirectional circuits.	Refer to the error message text.
EID-5059	The OCHNC upgrade failed. One or more communication failures occurred during the operation.	CTC encountered a complete failure while upgrading optical channel network connection.
EID-5060	The OCHNC upgrade partially failed. One or more communication failures occurred during the operation. Create the OCHCC manually.	CTC encountered a partial failure while upgrading an optical channel network connection.
EID-5061	The overhead circuit source and destination must reside on the same shelf.	Refer to the error message text.
EID-5062	A four-fiber {0} cannot be created using three cards.	A four-fiber MS-SPRing needs four cards.
WID-5063	The profile "{0}" includes a change to the OPEN-SLOT alarm severity. This change is disallowed for the ONS 15600. "{1}" will continue to use the OPEN-SLOT severity of MN that is included in the default configuration. Other changes from the "{2}" profile were successfully applied to {3}".	Refer to the warning message text.

EID-5064	{0}
	{1}
		This indicates the status of SNCP switching.

WID-5065	If you apply routing constraints to more than {0} nodes, performance might be affected and the operation might require more time than expected. Select Yes if you intend to proceed in spite of this risk, or No if you prefer to review your selection.	Refer to the warning message text.
WID-5066	The routing constraints will be lost. Are you sure you want to reset your changes?	Refer to the warning message text.
WID-5067	The routing constraints will be lost. Are you sure you want to leave this panel?	Refer to the warning message text.
EID-5068	The routing constraints could not be applied.	Refer to the error message text.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-5069	A source node cannot be added to either of these lists.	Select a node other than the source node to add to the route.
EID-5070	A destination node cannot be added to either of these lists.	Select a node other than the destination node to add to the route.
EID-5071	This node already belongs to one of these lists.	The node is already selected either in include or exclude list in the OCH circuit.
EID-5072	An OCH-Trail tunnel link was found but without any associated circuit.	Create an OCH-Trail circuit associated with the link.
EID-5073	You are creating an unprotected link from a protected port. Do you want to continue?	Refer to the error message.
EID-5074	Deleting OCH DCN circuits will cause a loss of connectivity to nodes in the circuit path that do not have other DCN connections. Do you want to continue?	Refer to the error message.
EID-5075	The VLAN ID must be a number between 1 and 4093.	Enter a number between 1 and 4093.
EID-5076	An error occurred while provisioning the VLAN ID. The VLAN ID is already present in the current profile	Select a VLAN ID that is not present in the current profile.
EID-5077	An error occurred while provisioning the VLAN database profile. {0}	CTC could not save the VLAN profile to the file name mentioned.
EID-5078	The VLAN merge is not complete. You forgot to fill {0} record(s).	Fill in the number of records specified and then proceed.
EID-5079	An error occurred while validating the provisionable patchcord.	Refer to the error message text.
EID-5080	No rolls are available.	You cannot delete a roll without selecting a roll.
EID-5081	An error occurred while tracing the RPR ring: {0}	The circuit reference is invalid.
EID-5082	{0} does not support: - Low-order circuits that have both {1}-protected and {2}-protected spans and that cross a node that does not have low-order cross-connect capability. - High-order circuits that carry low-order circuits with the parameters described above.	Refer to the error message text.
EID-5083	This circuit is not the same size as the existing circuit {0}. This circuit has size {1} and the existing circuit has size {2}.	During an RPR circuit creation on an ML-Series card, the new circuit size and the existing circuit size must be the same.
EID-5084	The Trunk model could not be found. {0}	The trunk specified is not found.
EID-5085	The maximum number of VLAN DB profiles is {0}.	Refer to the error message.
EID-5086	The circuit roll failed. You cannot bridge and roll the selected circuit because it has a monitor circuit.	Refer to the error message.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-5087	You cannot use same slot for east working and west protect ports.	Refer to the error message text.
EID-5088	You cannot use same slot for east working and west protect ports.	Refer to the error message text.
WID-5089	The maximum number of circuits that can be deleted at a time is 200. Do you want to delete the first 200 circuits selected?	Refer to the error message text
EID-5090	This operation cannot be completed. The selected circuits have different state models; please select circuits of the same type.	Refer to the error message text
EID-5091	Some PPC terminations were not repaired.	Refer to the error message text
WID-5092	The TL1 encoding mode for the tunnel is being changed. Do you want to modify the encoding?	Confirm if you really want to modify TL1 tunnel encoding.
EID-5094	Currently, CTC does not support bridge and roll on circuits having multiple cross-connects on a single node.	Refer to the error message text.
EID-5095	No path were selected. Please select at least one path starting from the {0} NE.	Refer to the error message text.
EID-5096	The first path must starts from the {0} NE.	Refer to the error message text.
EID-5097	The selected path should be linked with the last selected and keep the same direction.	Refer to the error message text.
EID-5098	The node is not selectable. Only the Span between the nodes are selectable.	Refer to the error message text.
EID-5099	Raman Command Error on {0}. {1}.	Refer to the error message text.
EID-5100	Raman Command in TimeOut. {0}.	Refer to the error message text.
EID-5101	Failed to get trunk ports for client. {0}.	Refer to the error message text.
EID-5102	Protected cards must have 2 trunk ports. (found {0}).	Refer to the error message text.
EID-5103	Failed to get collocated OCH ports for trunk: {0}.	Refer to the error message text.
EID-5104	Both OCHCC and OCHNC Protected are not allowed.	Refer to the error message text.
EID-5105	Cannot find entity model for endpoint: {0}.	Refer to the error message text.
EID-5106	Cannot find Out OTS line for selected endpoint: {0}.	Refer to the error message text.
EID-5107	Cannot find Protected Out OTS line for selected endpoint: {0}.	Refer to the error message text.
EID-5108	The demultiplexer associated with the selected endpoint :{0} is missing or not connected.	Refer to the error message text.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-5109	The demultiplexer associated with the protect path for the selected endpoint: {0} is missing or not connected.	Refer to the error message text.
EID-5110	The card selection is invalid. No cards were selected.	Refer to the error message text.
EID-5111	An error was occurred while configuring SNMPv3 proxy server.	Refer to the error message text.
EID-5112	No source of trap was selected.	Refer to the error message text.
EID-5113	Specify a valid value for target tag.	Refer to the error message text.
EID-5114	Specify a valid value for context engine ID.	Refer to the error message text.
EID-5115	No value was selected for proxy type.	Refer to the error message text.
EID-5116	No value was selected for local user.	Refer to the error message text.
EID-5117	No value was selected for proxy destination.	Refer to the error message text.
EID-5118	Specify a valid value for target IP.	Refer to the error message text.
EID-5119	The password for authentication should be at least 8 characters long.	Refer to the error message text.
EID-5120	The user name should be at least 6 characters long.	Refer to the error message text.
EID-5122	The node ({0}) does not support ML-MR POS port protection.	Refer to the error message text.
EID-5123	Primary ({0}) and secondary ({1}) nodes have to be the same for ML-MR POS port protection.	Refer to the error message text.
EID-5124	No nodes appear to support a Pseudo IOS connection.	Refer to the error message text.
EID-5125	No node was selected.	Refer to the error message text.
EID-5126	The Pseudo IOS console is disabled for the selected node.	Refer to the error message text.
EID-5127	The password for encryption should be at least 8 characters long.	Refer to the error message text.
EID-5128	{0} configuration already exists for the {1} {2} with the specified parameters.	Refer to the error message text.
WID-5129	Failed to retrieve the complete OSPF database as it is very large. Please contact Cisco Technical Support (http://www.cisco.com/techsupport) if you want to retrieve the complete OSPF database.	Refer to the warning message text.
EID-5130	Connection failed on node {0}	Refer to the error message text.
EID-5131	An error occurred while deleting the circuit end point.	Refer to the error message text.
WID-5132	Failed to retrieve the status of Proxy server on the node. Please contact Cisco Technical Support (http://www.cisco.com/techsupport) if you want to retrieve the Proxy status.	Refer to the warning message text.
EID-5133	SNMPv3 Proxy configuration already exists for the specified parameters.	Refer to the error message text.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-5134	On node {0} the calculated gain is much greater than expected. The wizard cannot operate under this condition. Please call TAC for support.	Refer to the error message text.
EID-5135	Added {0} network circuits to {1}. Circuits using the following wavelength(s) could not be updated as there is not a unique path through the added node: {2}	Refer to the error message text.
WID-5136	This operation will be applied to all drops of this circuit.	Refer to the error message text.
EID-5137	Please specify a valid SRLG value. SRLG value should be numeric.	Refer to the error message text.
EID-5138	Please specify a unique SRLG value. SRLG value already exists.	Refer to the error message text.
EID-5139	Unable to retrieve the node info.	The node name/node IP address could not be retrieved.
EID-5140	Unable to retrieve the link info.	The link source/link destination information could not be retrieved.
EID-5141	Error while initializing some instances.	Error in the backend process.
EID-5142	Unable to generate the SRLG Report.	The node name/node IP address or link source/link destination information could not be retrieved.
WID-5143	Are you sure you want to reset the unique SRLG for {0}	Refer to the error message text.
EID-5144	Unable to set the SRLG for {0}	Refer to the error message text.
EID-5145	Unable to launch view for {0}	The node/link is down.
EID-5146	Unknown Error occurred while updating the SRLG value on the Node/Link. {0}	Refer to the error message text.
WID-5147	Are you sure you want to reset the additional SRLG for {0}	Refer to the error message text.
EID-5148	Unable to set the SRLG for CRS node {0}	• Cisco CRS node connectivity is down. • XML interface on the Cisco CRS is not reachable. • Not enough memory on the Cisco CRS.
EID-5149	Unable to get the node model	Complete node information could not be retrieved.
EID-5150	Unable to get the side model	Complete side information could not be retrieved.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-5151	Unable to delete the SRLG for CRS node {0}	Refer to the error message text.
WID-5152	Some SRLGs cannot be synchronized. Network operation might be inconsistent.	Refer to the error message text.
EID-5153	Unable to perform SRLG synchronization operation.	• The node name/node IP address or link source/link destination information could not be retrieved. • Cisco CRS node connectivity is down. • XML interface on the Cisco CRS is not reachable. • Not enough memory on the Cisco CRS.
EID-5154	Specified value is out of range for SRLG. SRLG value should be specified between {0}-{1}	Refer to the error message text.
WID-5155	No. of SRLGs for circuit {0} are exceeding the limit. One circuit can have maximum {1} SRLGs defined. Trimming SRLG list to defined maximum size.	Refer to the error message text.
EID-5156	Maximum limit for defining additional SRLGs for Node/Link is reached. Maximum SRLGs that can be defined are {0}	Refer to the error message text.
WID-5157	No CRS based OCH Trail circuits detected	There are no Cisco CRS nodes associated with the circuit.
WID-5158	Some SRLGs cannot be deleted from CRS. Please use Synchronize IPoDWDM to synchronize SRLGs.	• Cisco CRS node connectivity is down. • XML interface on the Cisco CRS is not reachable. • Not enough memory on the Cisco CRS.
WID-5159	Some SRLGs cannot be set on CRS. Please use Synchronize IPoDWDM to synchronize.	• Cisco CRS node connectivity is down. • XML interface on the Cisco CRS is not reachable. • Not enough memory on the Cisco CRS.
EID-5160	Maintenance state cannot be set on CRS. Please use Synchronize IPoDWDM to synchronize.	• Cisco CRS node connectivity is down. • XML interface on the Cisco CRS is not reachable. • Not enough memory on the Cisco CRS.
EID-5161	Some of the effected routers could not be brought back into IS.	• Cisco CRS node connectivity is down. • XML interface on the Cisco CRS is not reachable. • Not enough memory on the Cisco CRS.
EID-5162	The circuit must be in the DISCOVERED state in order to start a PPT.	Refer to the error message text.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-5163	Unable to retrieve the Shelf info.	Complete node information could not be retrieved.
EID-5164	Requested operation cannot be completed.	Refer to the error message text.
EID-5165	Unable to perform Maintenance synchronization operation.	• The node name/node IP address or link source/link destination information could not be retrieved. • Cisco CRS node connectivity is down. • XML interface on the Cisco CRS is not reachable. • Not enough memory on the Cisco CRS.
EID-5166	Source is not fully specified.	The node, shelf, or slot is not selected.
EID-5167	Unable to set the Transport Admin State on the CRS {0}	• Cisco CRS node connectivity is down. • XML interface on the Cisco CRS is not reachable. • Not enough memory on the Cisco CRS.
EID-5168	Unable to set the Maintenance state for {0}	Complete node information could not be retrieved.
WID-5169	Some routers have responded not to start maintenance. Do you still want to go ahead with the maintenance activity?	Refer to the error message text.
WID-5170	Some Transport Admin States cannot be synchronized. Network operation might be inconsistent.	Refer to the error message text.
WID-5171	Some routers have not responded with Embargo status. Continuing maintenance activity may be traffic affecting. Are you sure you want to continue?	Refer to the error message text.
EID-5172	Provisionable patchcords can not be created between incompatible ports.	Refer to the error message text.
EID-5173	Some Server Trail terminations were not repaired.	Refer to the error message text.
WID-5174	Routing constraints has been specified only for protected path. Can be evaluated to move some constraints on working path since these are treated with priority. Please consider that some good constraint on protected part may not be evaluated correctly since that constraint may be already applied to working path by auto-routing. Do you want to continue anyway?	Refer to the error message text.
EID-5175	Unknown Error occurred while updating the SRLG value on the CRS node(s). {0}	Refer to the error message text.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
WID-5176	One or more SVLANs are invalid. Please remove them before continuing.	Refer to the error message text.
EID-6000	This platform does not support power monitoring thresholds.	Refer to the error message text.
EID-6001	One of the XC cards has failures or is missing.	Check whether all the cross-connect cards are installed and working.
EID-6002	One of the XC cards is locked.	Unlock the cross-connect card.
EID-6003	The OSC termination could not be created. This ring ID is already assigned.	Enter a new ID for the ring.
EID-6004	A system reset cannot be performed while a BLSR ring is provisioned on the node.	Remove the MS-SPRing from the node and continue with the reset procedure.
EID-6005	The timing references could not be assigned. - Only two DS1 or BITS interfaces can be specified. - DS1 interfaces cannot be retimed and used as a reference. - BITS-2 is not supported on this platform.	Refer to the error message text.
EID-6006	The timing references could not be assigned. - An NE reference can only be used if the timing mode is LINE. - A BITS reference can only be used if the timing mode is not LINE. - A Line reference can only be used if the timing mode is not EXTERNAL.	Refer to the error message text.
EID-6008	SF BER and SD BER are not provisionable on the protect line of a protection group.	Refer to the error message text.
WID-6009	If auto adjust GFP buffers is disabled, GFP buffers available must be set to an appropriate value based on the distance between the circuit endpoints.	Refer to the warning message text.
WID-6010	If auto detection of credits is disabled, credits available must be set to a value less than or equal to the number of receive credits on the connected FC endpoint.	Refer to the warning message text.
WID-6011	Ingress idle filtering should be turned off only when required to operate with non-Cisco Fibre Channel/FICON-over-SONET equipment.	Refer to the warning message text.
EID-6012	The retiming configuration could not be changed because there are circuits on this port.	You cannot change the timing configuration on this port unless the circuits on this port are deleted.
EID-6013	The NTP/SNTP server could not be changed. {1}	Refer to the error message text.
EID-6014	The operation failed because the reference state is OOS.	Change the Unlocked state to Active.
EID-6015	The distance extension cannot be disabled if the port media type is FICON 1Gbps ISL or FICON 2Gbps ISL.	Refer to the error message text.
EID-6016	The card mode cannot be changed to Fibre Channel Line Rate if the port media type is FICON 1Gbps ISL or FICON 2Gbps ISL.	Refer to the error message text.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-6017	The destination of a {0} route cannot be a node IP address.	A node IP address cannot be the destination for a static route.
EID-6018	The destination of a {0} route cannot be the same as the subnet used by the node.	Refer to the error message text.
EID-6019	The destination of a static route cannot be 255.255.255.255	The network address such as 255.255.255.255 is not valid. Enter a valid address.
EID-6020	The destination of a static route cannot be the loopback network (127.0.0.0/8).	Refer to the error message text.
EID-6021	The subnet mask length for a non default route must be between 8 and 32.	Length of subnet mask must be within the specified range.
EID-6022	The subnet mask length for a default route must be 0.	Refer to the error message text.
EID-6023	The destination of a {0} route cannot be an internal network{1}.	The destination of a static route must not be an internal network.
EID-6024	The destination of a {0} route cannot be a class D (224.0.0.0/4) or class E (240.0.0.0/4) address.	The destination of a static route must not be a Class D or Class E address.
EID-6025	The destination of a {0} route cannot be a class A broadcast address (x.255.255.255/8).	The destination of a static route must not be a Class A broadcast address. It should be (xxx.0.0.0).
EID-6026	The destination of a {0} route cannot be a class B broadcast address (x.x.255.255/16).	The destination of a static route must not be a Class B broadcast address.
EID-6027	The destination of a {0} route cannot be a class C broadcast address (x.x.x.255/24).	The destination of a static route must not be a Class C broadcast address.
EID-6028	The destination of a {0} route cannot be the subnet broadcast address associated with a node IP address.	The destination of a static route must not be a subnet broadcast address of a node IP.
EID-6029	The next hop of a static route cannot be the same as the destination of the route or an internal network{0}.	Static route must have the default route as the next hop, and not destination of the route or internal network.
EID-6030	The next hop of a static default route must be the provisioned default router.	The default route is selected for networks that do not have a specific route.
EID-6031	No more static routes can be created.	You have reached the maximum number of static routes.
EID-6032	This static route already exists.	Refer to the error message text.
EID-6033	A previous operation is still in progress.	Another operation is in progress. You must try after sometime.
EID-6035	The parent entity does not exist.	Refer to the error message text.
EID-6036	The parent PPM entity does not exist.	Create a parent entity for the PPM.
EID-6037	This equipment type is not supported.	CTC does not support this equipment.
EID-6038	The PPM port is invalid.	Refer to the error message text.
EID-6039	The card is part of a regeneration group.	Select another card.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-6040	Out of memory.	Refer to the error message text.
EID-6041	The port is already present.	Refer to the error message text.
EID-6042	The port is used as timing source.	Choose another port because the selected port is being used as a timing source.
EID-6043	A DCC or GCC is present.	Refer to the error message text.
EID-6044	The card or port is part of protection group.	Refer to the error message text.
EID-6045	The port has overhead circuit(s).	Refer to the error message text.
EID-6046	The ITU-T G.709 configuration is not compatible with the data rate.	Refer to the error message text.
EID-6047	The port cannot be deleted because its service state is OOS-MA,LPBK&MT.	To delete the port, you must change the port state to Locked,disabled.
EID-6048	{0} is {1}.	The trunk port is in the wrong state to carry out the action.
EID-6049	The card operating mode of {0} is not supported.	CTC does not support the mode of operation requested on the card.
EID-6050	Some {0} terminations were not {1}d. {2}	Refer to the error message text.
WID-6051	All {0} terminations were {1}d successfully. {2}	Refer to the warning message text.
EID-6052	The authentication key can not be blank.	Enter an authentication key.
EID-6053	No more SNMP trap destinations can be created.	You have reached the maximum number of SNMP trap destinations.
EID-6054	{0} is not a valid IP address for an SNMP trap destination.	The IP address specified is not a valid receiver of SNMP traps.
EID-6055	The IP address is already in use.	Refer to the error message text.
EID-6056	The SNMP trap destination is invalid. {0}	The specified SNMP trap destination is invalid. Choose another destination.
WID-6057	Changing the card mode will result in an automatic reset.	Refer to the warning message text.
EID-6058	The maximum number of IP-over-CLNS tunnels has been exceeded.	Refer to the error message text.
EID-6059	The specified IP-over-CLNS tunnel already exists!	Specify another IP-over-CLNS tunnel.
EID-6060	An error occurred while trying to {0} an IP-over-CLNS tunnel entry: {1}.	Refer to the error message text.
EID-6061	An error occurred while deleting the IP-over-CLNS tunnel entry.	CTC encountered an error while deleting the IP-over-CLNS tunnel entry.
EID-6062	The selected IP-over-CLNS tunnel does not exist.	Create a IP-over-CLNS tunnel.
EID-6063	The selected router does not exist.	Create a router.
EID-6064	The MAA address list is full.	Refer to the error message text.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-6065	The selected area address is duplicated.	Enter another area address.
EID-6066	The primary area address cannot be removed.	Refer to the error message text.
EID-6067	The selected area address does not exist.	Choose another area address.
EID-6068	The IP-over-CLNS NSEL cannot be modified while there are IP-over-CLNS tunnel routes provisioned.	You cannot change the NSEL address if tunnels are provisioned.
EID-6069	The node is currently in ES mode. Only Router 1 can be provisioned.	An end system needs only one provisioned router.
EID-6070	No router was selected.	Select a router.
EID-6071	The TARP data cache cannot be flushed.	You cannot flush the cache in the Target Identifier Address Resolution Protocol (TARP) state.
EID-6072	The TARP data cache entry cannot be added: {0}	You cannot add the specified cache entry.
WID-6073	A TARP request has been initiated. Try refreshing the TARP data cache later.	Refer to the warning message text.
EID-6074	End system mode only supports one subnet.	Refer to the error message text.
EID-6075	An error occurred while trying to remove a MAT entry. The entry does not exist.	CTC is removing the MAT entry.
EID-6076	An error occurred while trying to {0} a TARP manual adjacency entry: {1}	CTC cannot add the specified adjacency entry for reasons unknown.
EID-6077	The area address must be between 1 and 13 bytes long, inclusive.	The area address should not be more than 13 characters.
EID-6078	A TDC entry with this TID {0} does not exist in the table.	The specified target identifier does not exist.
EID-6079	A TDC entry with this TID {0} could not be removed. Please verify that TARP is enabled.	You must enable TARP 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 the warning message text.
EID-6081	The limit of 10 RADIUS server entries has been reached.	CTC does not allow more than 10 RADIUS servers.
EID-6082	{0} cannot be empty.	The Shared Secrets field should not be empty.
EID-6083	The entry you selected for editing has been altered by another user. The changes cannot be committed.	Refer to the error message text.
EID-6084	The RADIUS server entry already exists.	Specify another RADIUS server entry.
WID-6085	Disabling shell access will prevent Cisco TAC from connecting to the vxWorks shell to assist users.	Refer to the warning message text.
EID-6086	The card cannot be changed because card resources are in use.	The card you are trying to remove is being used. Cannot change the card.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-6087	The card cannot be changed because the card type is invalid or incompatible.	Refer to the error message text.
EID-6088	This line cannot be put into loopback while it is in use as a timing source.	Refer to the error message text.
EID-6089	The interface was not found. {0}	CTC cannot find the specified interface.
EID-6090	The interface type is not valid for this operation. {0}	Choose another interface.
EID-6091	The current state of the interface prohibits this operation. {0}	The port is in an invalid state to set a loopback.
EID-6092	This operation is prohibited for this interface. {0}	CTC does not allow this operation for the specified interface.
EID-6093	The maximum number of TARP data cache entries has been exceeded.	You have exceeded the number of characters permitted.
EID-6094	The maximum number of manual adjacency table entries has been exceeded.	Refer to the error message text.
EID-6095	The AIS/Squelch mode is invalid.	Refer to the error message text.
EID-6096	A default IP-over-CLNS tunnel route is only allowed on a node without a default static route and a default router of 0.0.0.0.	Refer to the error message text.
EID-6097	The authorization key does not comply with Cisco IOS password restrictions. {0}	Specify another authorization key.
EID-6098	A default static route is not allowed when a default IP-over-CLNS tunnel exists.	Refer to the error message text.
EID-6099	You cannot create a subnet on a disabled router.	Create the subnet on an active router.
WID-6100	Disabling a router that has a provisioned subnet is not recommended.	Refer to the warning message text.
EID-6101	The MAT entry already exists.	Refer to the error message text.
WID-6102	The new card has less bandwidth than the current card. Circuits of size VT15 and larger will be deleted.	Refer to the warning message text.
EID-6103	The TDC entry already exists.	Specify another entry for the TARP data cache.
EID-6104	APC ABORTED.	APC is aborted.
EID-6105	The 'Change Card' command is valid for MRC cards only when Port 1 is the sole provisioned port.	Refer to the error message text.
EID-6106	To delete all RADIUS server entries, RADIUS authentication must be disabled.	Disable RADIUS authentication and proceed.
EID-6107	The node failed to restart the TELNET service on the selected port. Try using another unreserved port that is not being used within the following ranges: 23, 1001-9999 (with the exception of 1080, 2001-2017, 2361, 3081-3083, 4001-4017, 4022, 4081, 4083, 5000, 5001, 7200, 9100, 9300, 9401).	Refer to the error message text.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-6108	That port is already in use.	Restart a Telnet session.
EID-6109	A section trace is active on the trunk port. The action cannot be completed.	Actions such as putting the port in an incomplete state are not permitted while a section trace is active.
EID-6110	The maximum number of TARP requests has been reached.	You have exceeded the maximum number of TARP requests.
EID-6111	The card in Slot {0} cannot be removed from the protection group while its traffic is switched.	Refer to the error message text.
EID-6112	An error occurred while adding a shelf: {0}	The shelf ID specified is invalid or already exists, the equipment does not support multishelf, the specified shelf position is out of range, or the specified shelf position is already in use.
EID-6113	An error occurred while deleting a shelf: {0}	One or more of the equipment modules (provisioned virtual links, provisioned server trails, provisioned protection groups, or provisioned DCCs) in the shelf is currently in use. Delete cards from all the slots and try again.
EID-6114	The maximum number of supported shelves has already been provisioned.	Refer to the error message text.
EID-6115	There are bad or duplicate shelf positions. Valid rack numbers are {0} to {1}. Valid rack positions are {2} to {3}.	Refer to the error message text.
EID-6116	CTC attempted to access an OCH-Trail connection that has been destroyed.	Software has prevented an attempt to access an OCH trail.
EID-6117	CTC attempted to access an OCH-Trail adit that has been destroyed.	The resource cannot be accessed because it is released or fully utilized.
WID-6118	The following slots are provisioned but do not have cards installed: {0} CTC will assume they are ITU-T interfaces.	Refer to the warning message text.
EID-6119	The shelves could not be rearranged. {0}	One of the following conditions is present: duplicate shelf positions, invalid shelf positions, or concurrent movement (two CTC sessions are attempting to rearrange the shelves at the same time.)
EID-6120	This equipment does not support multishelf.	Refer to the error message text.
WID-6121	This internal patchcord cannot be provisioned because the endpoints have no compatible wavelengths.	The endpoints of an internal patchcord should have compatible wavelengths.
EID-6122	The wizard could not be started. {0}	CTC was unable to initiate the wizard due to the specified reason.
EID-6123	The OSI request can not be completed successfully.	A communication failure occurred.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-6124	The ALS recovery pulse interval is invalid.	Refer to the error message text.
EID-6125	The ALS recovery pulse duration is invalid.	Refer to the error message text.
EID-6126	The current setting does not support the specified ALS mode.	Refer to the error message text.
EID-6127	All enabled routers are required to have the same area.	Refer to the error message text.
EID-6128	A software download is in progress. Configuration changes that result in a card reboot cannot take place during a software download. Please try again after the software download is done.	Refer to the error message text.
EID-6129	The payload configuration and card mode are incompatible.	Refer to the error message text.
EID-6135	A DCC is present.	A data communications channel (DCC) already exists.
EID-6136	An error occurred during provisioning: {0}	CTC was not able to provision the specified port or card.
EID-6137	Multishelf cannot be disabled. {0}	Multishelf is not supported on equipment, is already disabled, or modules on the shelf are currently in use.
EID-6138	The LAN configuration is invalid.	Verify the LAN configuration.
EID-6139	Invalid card(s) are present. Please remove all non-MSTP cards and try again.	Non-DWDM cards cannot be added to an a DWDM node. Remove the cards.
EID-6140	The shelf identifier for a subtended shelf cannot be provisioned through CTC. It must be changed using the LCD.	Refer to the error message text.
EID-6143	The DHCP server could not be changed.	Refer to the error message text.
EID-6144	The port provisioning cannot be changed when the port media is Undefined.	If the port is not preprovisioned with the type of media that is going to be inserted, you cannot access any of the existing values for the port.
WID-6145	OSPF on LAN should only be enabled when the LAN routers run OSPF. Otherwise, the node will not be reachable from outside its subnet. RIP implementation only advertise routes in one direction to connected routers. It does not learn or distribute routes advertised by other routers. Also note that enabling OSPF on the LAN will temporarily cause the current list of static routes to stop being advertised to remote nodes and only be used locally.	Refer to the warning message text.
WID-6146	Deleting the protection group while in a switched state might cause a loss of traffic. It is recommended that you verify switch states before proceeding.	Refer to the warning message text.
EID-6149	The LAPD MTU size must be greater than or equal to the {0} LSP buffer size {1}. Alternatively, you can decrease the {0} LSP buffer size to {2}.	Refer to the error message text.
EID-6150	The value is out of range.	Enter a value that is within the range.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-6151	The minimum span loss must be less than the maximum span loss.	Refer to the error message text.
EID-6152	The "Use NTP/SNTP Server" field is checked. Enter the NTP/SNTP server IP address or server name.	Enter the NTP/SNTP server name. To leave this field empty, uncheck the “Use NTP/SNTP Server" and proceed.
EID-6153	The maximum frame size is invalid.	Refer to the error message text.
EID-6154	To combine unidirectional two-port provisioning and autonegotiation on the same port, autonegotiation must be set first.	Refer to the error message text.
EID-6155	Transponder mode cannot be provisioned with circuits on the card.	Refer to the error message text.
EID-6156	The transponder configuration is invalid.	The transponder is not configured properly.
EID-6157	The watermark values are either out of range or inconsistent.	Enter valid watermark values.
EID-6179	The 1+1 protection group is not optimized.	Refer to the error message text.
EID-6196	The equipment has failed or is missing.	Operation is requested on a failed or missing equipment.
EID-6197	Attributes cannot be changed when the port administrative state is {0}.	You cannot change the attributes when the port is in the specified administrative state.
WID-6204	This action will cause the node to reboot. When provisioning in single-shelf mode, Shelf {0} of the node that you connect to must be properly preprovisioned or you will lose traffic. Use the LCD to return to single-shelf mode. CTC cannot be used for this. Changing from subtended shelf mode to single-shelf mode could be traffic-affecting.	Refer to the warning message text.
EID-6205	The interlink port is not provisioned.	The user creates an ADM peer group without interlink ports.
EID-6206	The ADM peer group has already been created on the peer card.	The user creates an ADM peer group involving an ADM card inserted in a peer group.
EID-6207	This card is not in the ADM peer group.	The selected ADM card is not involved in an ADM peer group.
EID-6208	The payload is not OTU2.	Refer to the error message text.
EID-6209	The side is already defined by the node.	During the creation of a side on node, a side is already defined.
EID-6210	No side was selected.	The user requests an operation on a side, but no side is selected.
EID-6211	The side was not deleted.	CTC could not delete the selected side successfully.
EID-6212	One of the ports is connected to a patchcord or virtual link.	An operation on a port was not performed because the port is connected to a patchcord or a virtual link.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-6213	It is not possible to associate the side to the two ports.	During the creation of a side it is not possible to associate the selected ports to the new side.
EID-6214	The port is already assigned to a side.	The selected port is already assigned to a side.
EID-6215	Error provisioning the CVLAN ID. Enter a valid number or range between 0 and 4094.	The entered CVLAN ID was out of the admitted range.
EID-6216	Changing card will reset the optical thresholds to the default setting and may affect the optical connection. The optical connection will work only if the optical performance is compatible with {0} card. Please check the network design.	Refer to the error message text.
EID-6217	You cannot delete the {0} {1}.	You cannot delete {0} {1} because it is part of an ADM peer group or one or more circuits are provisioned on it.
EID-6218	Invalid ethernet duplex value	the Ethernet duplex value is invalid. Enter again.
EID-6219	Invalid committed info rate	The committed info rate value is invalid. Enter again.
EID-6220	Invalid Ethernet speed value	The Ethernet speed value is invalid. Enter again.
EID-6221	Invalid mtu value	The MTU value is invalid. Enter again.
EID-6222	Invalid flow control value	The flow control value is invalid. Enter again.
EID-6223	Invalid Network Interface Mode	The network interface mode value is invalid. Enter again.
EID-6224	Invalid ingress COS value	The ingress cost of service (CoS) value is invalid. Enter again.
EID-6225	Invalid ethertype value	The Ethertype value is invalid. Enter again.
EID-6226	Invalid buffer size value	The Buffer size value is invalid. Enter again.
EID-6227	Invalid egress QOS value	The egress quality of service (QoS) value is invalid. Enter again.
EID-6228	Invalid QinQ working Mode	The QinQ working mode is invalid. Enter again.
EID-6229	Configured protection status Not Supported	The protection status is not supported
EID-6230	The number of provisioned entries exceeds the limit	Refer to the error message text.
EID-6231	This is not a valid VLAN ID.	Entered VLAN ID is not present in the database file.
EID-6232	The VLAN remapping ID is not allowed.	Refer to the error message text.
EID-6233	The CVLAN is duplicated.	You cannot have identical CVLAN IDs.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-6234	The VLAN ID is out of range.	The VLAN ID entered is out of range.
EID-6235	This is not a valid VLAN name.	The entered VLAN name exceeds the number of characters (32) allowed.
EID-6236	The protected VLAN number exceeds the maximum allowed.	The user enters more than 256 protected VLAN in the VLAN database.
EID-6237	The port is not in OOS disabled admin state	Refer to the error message text.
EID-6238	The VLAN ID is in use.	The entered VLAN ID is in use by a node.
EID-6239	APC wrong node side.	Refer to the error message text.
EID-6240	You cannot change the Admin State for an interlink port when it is part of an ADM peer group. This operation is not supported.	Refer to the error message text.
EID-6242	The protection slot is invalid.	You must select a valid protection slot.
EID-6243	The {0} address of {1} is invalid.	Refer to the error message text.
EID-6244	The mask of {0} is invalid.	The mask of the specified value is not valid.
EID-6245	The cost must be between 1 and 32767.	Refer to the error message text.
EID-6246	The {0} address cannot be {1}.	Refer to the error message text.
EID-6247	The authentication type is invalid.	Enter a valid authentication type.
EID-6248	The cost must between 1 and 15.	Refer to the error message text.
EID-6249	The port has a cross-connect.	Refer to the error message text.
EID-6250	The reversion time is invalid.	The reversion time is invalid. Enter again.
EID-6251	Invalid Margin For Span Aging. Value is not in the range 0 - 10.	Enter a value between 0 and 10.
EID-6252	The data cannot be retrieved because ANS parameters cannot be calculated on the node in its current configuration.	Refer to the error message text.
EID-6253	Invalid Margin For Span Aging.	Refer to the error message text.
EID-6254	SDH mode does not support timing references.	Timing reference is not supported by SDH mode.
EID-6255	Only DS1 interfaces with ESF line types support timing references.	Refer to the error message text.
EID-6256	sendDoNotUse and sendDoNotUseFF are mutually exclusive.	Refer to the error message text.
EID-6257	The termination is already in use.	Refer to the error message text.
EID-6258	The side is carrying services or traffic.	Refer to the error message text.
EID-6259	A pluggable module on Port 22 remains unmanaged.	Refer to the error message text.
EID-6260	You cannot delete this port. There was a severe architectural error related to the index of the pluggable trunk port object. Please contact technical support for assistance.	Refer to the error message text.
EID-6261	This is not a valid VLAN ID. The VLAN database is empty.	The user adds a row without a valid VLAN database loaded.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-6263	The equipment requires two slots.	The user provisions a double footprint card in a single slot.
EID-6264	The patchcord is duplicated.	Refer to the error message text.
EID-6265	The wavelength is in use by an OCH trail, a virtual link, or an internal patchcord.	Refer to the error message text.
EID-6266	The card cannot be changed because the port has not been provisioned.	Refer to the error message text.
EID-6267	Each port can have a maximum of 8 MAC addresses.	Refer to the error message text.
EID-6268	This server trail does not have a valid start or end.	Refer to the error message text.
EID-6269	The maximum number of server trails is 3743.	Refer to the error message text.
EID-6270	A unique server trail ID could not be allocated.	Refer to the error message text.
EID-6271	The server trail already exists.	Refer to the error message text.
EID-6272	The server trail size must not exceed the port bandwidth.	Refer to the error message text.
EID-6273	An OCH Trail circuit is active on the trunk port. To modify the ITU-T G.709 parameter, the circuit must be out of service.	Refer to the error message text.
EID-6274	Unable to restore this database: The software version cannot be obtained from the node. Please try again.	The user tries to restore a database on a node, but its not possible to get the software version from it.
EID-6275	You cannot change this parameter. The port is part of an active circuit.	Certain parameters like Port Rate and Admin State cannot be changed when the port is part is part of an active circuit. Delete all the circuits on the port before changing admin state of the port.
EID-6276	APC is disabled. APC Correction Skipped. Override cannot be performed.	Refer to the error message text.
EID-6277	There are no alarm conditions available to run APC Correction Skipped Override.	Refer to the error message text.
EID-6278	APC Correction Skipped Override is not supported for this card.	Refer to the error message text.
EID-6279	Protection cannot be disabled when the FPAS alarm is active.	Refer to the error message text.
WID-6280	Any configuration change will be lost and the operation is traffic affecting.	Refer to the error message text.
EID-6281	The port is involved in a protection group. The protected port is not in the {0} administrative state	Change the port state to administrative.
WID-6282	Forcing FPGA update will be traffic-affecting.	Refer to the error message text.
WID-6283	Enabling ALS on a DWDM trunk port that is connected to a channel filter will result in a conflict with the ALS on the amplifier card or with the VOA startup process. Is it OK to continue?	Refer to the error message text.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
WID-6284	Changing the timing standard will re-initialize the shelf timing and might affect traffic. OK to continue?	Refer to the error message text.
WID-6285	Since you are changing the IP address of one node containing some PPC terminations, you are also requested to run the PPC Repair tool in order to fix the IP addresses stored in the nodes connected by these PPCs	Refer to the error message text.
EID-6286	The port type cannot be changed because the port has been deleted.	Refer to the error message text.
EID-6287	You cannot edit the {0} {1}.	Port rate of Optical and Electrical ports cannot be changed while circuits are provisioned on them.
EID-6288	The BERT configuration is invalid.	Refer to the error message text.
EID-6289	The BERT mode is not yet configured	Refer to the error message text.
WID-6290	The BERT mode is configured in unframed format	Refer to the error message text.
WID-6291	Port has circuits; configuring the BERT mode will disrupt normal traffic.	Refer to the error message text.
EID-6292	The alarm type name cannot exceed 20 characters	Refer to the error message text.
EID-6294	The alarm type name contains invalid characters. Only the following characters are valid: 0-9, A-z, a-z and "-".	Refer to the error message text.
EID-6295	The alarm type is in use and cannot be deleted.	Refer to the error message text.
EID-6296	Maximum number of alarm types that can be added cannot exceed 50.	Refer to the error message text.
EID-6297	Hard coded alarm types cannot be deleted.	Refer to the error message text.
EID-6298	The alarm type already exists.	Refer to the error message text.
EID-6299	The alarm type does not exist.	Refer to the error message text.
EID-6300	Selective auto negotiation is allowed only when selected speed and duplex modes are non-auto. Click "Reset" to revert the changes.	Refer to the error message text.
WID-6301	Selective auto negotiation applies only to copper SFPs.	Refer to the error message text.
EID-6302	Users are not allowed to perform this operation.	When logged in as a maintenance user provisioning operation is not allowed.
EID-6303	The ITU-T G.709 configuration cannot be disabled when Fast Protection is enabled.	Refer to the error message text.
EID-6304	Users are not allowed to perform this operation.	Refer to the error message text.
EID-6305	The view could not be deleted.	Refer to the error message text.
EID-6306	The ITU-T G.709 configuration cannot be disabled when Fast Protection is enabled.	Refer to the error message text.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
WID-6307	You have only selected one trunk-to-trunk patchcord. For complete deletion, you must select both patchcords that are attached to the 10GE_XP/GE_XP cards. Do you want to continue?	Refer to the warning message text.
WID-6308	You have only selected one trunk-to-OCH patchcord. For complete deletion, you must select both patchcords that are attached to the TXP/MXP card. Do you want to continue?	Refer to the warning message text.
EID-6309	OCHNC circuits, OSC terminations, synchronization sources and protection groups must be removed before you can remove this patchcord.	Refer to the error message text.
EID-6310	The Committed Info Rate value must be in range [0-100].	Refer to the error message text.
EID-6311	The MTU value must be in range [64-9700].	Refer to the error message text.
EID-6312	The multicast IP address must be in range [224.0.0.0 - 239.255.255.255] Excluding the following IP address subranges [(224-239).(0/128).0.(0-255)]	Refer to the error message text.
EID-6313	The multicast IP address count must be in range [1-256]	Refer to the error message text.
EID-6314	Could not retrieve TTY session for the chosen CRS.	Refer to the error message text.
EID-6315	CRS provisioning failed. {0}	Refer to the error message text.
EID-6316	The chosen node is not a CRS-1.	Refer to the error message text.
EID-6317	The value specified for IPv6 Address or IPv6 Default Router is invalid.	Refer to the error message text.
EID-6318	The value specified for Prefix Length is invalid. Valid range of values is 0 to 128.	Refer to the error message text.
EID-6319	IPv6 mode can be enabled only if SOCKS and firewall are enabled on the node.	Refer to the error message text.
EID-6320	IPv6 mode cannot be enabled on a node if RIP is enabled.	Refer to the error message text.
EID-6321	IPv6 mode cannot be enabled on a node if 'OSPF on LAN' is enabled.	Refer to the error message text.
EID-6322	IPv6 Address cannot be specified for {0} when IPv6 mode is not enabled on the node.	Refer to the error message text.
EID-6323	CTC was unable to delete SnmpV3 Target.	Refer to the error message text.
EID-6324	The card mode is invalid in this configuration.	Refer to the error message text.
EID-6325	SW version mismatch on node {0}: found {1}, expected {2}.	Refer to the error message text.
EID-6326	The CRS node {0} version[{1}] is greater than the supported version[{2}]. The creation of ochtrail circuits between CRS nodes will not be disabled, but there could be unexpected behaviors.	Refer to the error message text.
EID-6327	The end point of patchcord have an incompatible wavelength.	Refer to the error message text.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-6329	Protection/AIS action cannot be both set to squelch.	Refer to the error message text.
EID-6330	The node failed to restart the Pseudo IOS CLI service on the selected port. Try using another unreserved port that is not being used within the 1024 - 65535 range.	Refer to the error message text.
EID-6331	That port is already in use. Also note that the Pseudo IOS port may not be changed if any Pseudo IOS connections are currently open.	Refer to the error message text.
WID-6332	All previously configured IPv6 destinations will become unreachable if IPv6 mode is disabled. It is recommended that you remove all IPv6 related provisioning before disabling IPv6 mode. Do you want to continue?	Refer to the warning message text.
WID-6333	The NE default {0} not available in the selected NE Defaults Tree.	Refer to the warning message text.
WID-6334	Could not find the NE default {0}.	Refer to the warning message text.
WID-6335	CTC was unable to create a new Target account.	Refer to the warning message text.
WID-6336	Changing the card to EFEC mode will cause the ports 1 and 2 to be disabled. Do you want to continue?	Refer to the warning message text.
WID-6337	CE-MR-10/CE-MR-6 card does not validate the Ethernet FCS when traffic is received from optical side. This can result in errored frames from optical side being forwarded to the peer device via front ports. It would be left to the peer device to detect the errors and discard the frames. It is suggested to enable the FCS option on both ends of the circuit. The GFP FCS will be used to discard errored frames. The discarded frames will be accounted under the performance pane for the POS port.	Refer to the warning message text.
WID-6338	Ingress COS setting is not compatible with QinQ mode.	Refer to the warning message text.
WID-6339	Some circuits may become partial as part of this upgrade and would need to be reconfigured.	Refer to the warning message text.
WID-6340	One or more QinQ rules have not been deleted because they are not related to the current circuit.	Refer to the warning message text.
WID-6341	The Functional view on {0} is disabled.	Refer to the warning message text.
WID-6342	Changing the {0} settings might be traffic affecting. Do you want to continue?	Refer to the warning message text.
WID-6343	The selected file name is too long. File names (including the full path) must be less than 254 characters.Please enter a valid file name.	Refer to the warning message text.
EID-6344	It is detected a shelf mismatch condition.	Refer to the error message text.
EID-6345	The line termination is invalid.	Refer to the error message text.
EID-6346	The overhead is not supported.	Refer to the error message text.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-6347	A patchcord was expected for a successful operation.	Refer to the error message text.
EID-6348	A Virtual link already exists on the same path.	Refer to the error message text.
EID-6349	The overhead creation has failed.	Refer to the error message text.
EID-6350	The unprotected line is not present	Refer to the error message text.
EID-6351	The port status is active.	Refer to the error message text.
EID-6352	IPv4 access cannot be disabled when IPv6 mode is not enabled on the node.	Refer to the error message text.
EID-6353	IPv4 access cannot be disabled when the node is in Multishelf configuration.	Refer to the error message text.
EID-6354	Disabling IPv4 access may lead to loss of communication with the node. Make the change anyway?	Refer to the error message text.
EID-6355	IPv6 access cannot b disabled when IPv4 Access is disabled on the node.	Refer to the error message text.
EID-6356	Multishelf configuration cannot be enabled when IPv4 Access is disabled on the node.	Refer to the error message text.
EID-6357	The Multicast SVLAN field can be modified only when the MVR feature is disabled.	Refer to the error message text.
EID-6358	Too many TRANSLATE QinQ rules per port with MVR feature enabled.	Refer to the error message text.
EID-6359	The PLIM {0} is part of an OCH Trail circuit and its configuration cannot be changed.	Refer to the error message text.
EID-6360	The fiber cut restore operation did not succeeded on {1}. {0}	Refer to the error message text.
EID-6361	The resource is already in use, please retry later.	Refer to the error message text.
EID-6362	Request timed out, please retry.	Refer to the error message text.
EID-6363	An internal communication error was encountered while retrieving values. Please retry.	Refer to the error message text.
EID-6364	Could not perform the requested operation because of a CRS communication error.	Refer to the error message text.
EID-6365	Could not perform the requested operation on PLIM {0} because that port is already in an LMP data link with neighbor {1}.	Refer to the error message text.
EID-6366	The IP address {0} was not found in the CRS ARP table.	Refer to the error message text.
WID-6367	This operation will also change the CRS configuration. Is it OK to continue?	Refer to the error message text.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
WID-6368	This operation will also change the CRS configuration. Moreover, it requires the PLIM shutdown and may be SERVICE AFFECTING. Is it OK to continue?	Refer to the error message text.
EID-6369	The rollback operation has failed.	Refer to the error message text.
EID-6370	The requested operation is not authorized on {0}. Please check task privileges.	Refer to the error message text.
WID-6371	Since you have changed the IP address of one node containing Server Trail terminations, you should also fix the IP addresses stored in the nodes connected by these Server Trails. Run the Server Trail Repair tool to fix these IP addresses.	Refer to the error message text.
EID-6372	A Server Trail with the requested ID and old peer IP Address does not exist.	Refer to the error message text.
WID-6373	AIS Squelch action and Link Integrity attribute should not be simultaneously set on the same port in case of GR3/FAPS: Profile {0}, Port {1}, SVLAN {2}.	Refer to the error message text.
EID-6374	The selected SVLAN is already used for MVR.	Refer to the error message text.
EID-6375	Missing L2 internal patchcords between XP cards.	Refer to the error message text.
EID-6376	Profile cannot be mapped because the SVLAN is not enabled on the port.	Refer to the error message text.
EID-6377	The configuration must be applied on the working interface in case of protection group.	Refer to the error message text.
EID-6378	Squelch protection action and Auto mode are not compatible in case of L2 1+1.	Refer to the error message text.
EID-6379	The NTP/SNTP server and the Backup NTP/SNTP servers cannot be the same.	Refer to the error message text.
EID-6380	Multishelf VLAN range must be in range of {0} to {1}.	Refer to the error message text.
WID-6381	Changing the OTU2_XP card mode to “10GE LAN to WAN” will reboot the card. Do you want to continue?	Refer to the error message text.
WID-6382	Changing the OTU2_XP card mode from “10GE LAN to WAN” will reboot the card and delete the pluggable ports 1 and 3. Do you want to continue?	Refer to the error message text.
EID-6383	The board is busy. Please retry later.	Refer to the error message text.
EID-6384	The value "{0}" must be between {1} and {2}.	Refer to the error message text.
EID-6385	The value "{0}" has too many decimal points [xx.0 .. xx.9].	Refer to the error message text.
EID-6386	The value "{0}" must be a float between {1} and {2}.	Refer to the error message text.

Table 4-1 Error Messages (continued)

Error/Warning ID	Error/Warning Message	Description
EID-6387	The value "{0}" must be a integer between {1} and {2}.	Refer to the error message text.
EID-6388	"{0}" is not a valid enumerated value.	Refer to the error message text.
EID-6389	Power fail low TCA is greater than high TCA.	Refer to the error message text.
EID-6390	Error while setting DISABLE FEC on {0}.	Refer to the error message text.
EID-6391	Error while setting STANDARD FEC on {0}.	Refer to the error message text.
EID-6392	Error while setting ENHANCED FEC on {0}.	Refer to the error message text.
EID-6393	Error while setting SD BER on {0}.	Refer to the error message text.
EID-6394	The maximum number of CVLAN ranges cannot exceed 48 in selective QinQ mode.	Refer to the error message text.
EID-6397	Unable to update the FPGA as the STANBY CTX is not ready.	Please retry later.
EID-6398	Unable to update the FPGA as the database is busy saving recent modifications.	Please retry later.

[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.

INDEX