Cisco ONS 15454 Troubleshooting Guide

Product and Documentation Release 6.0
Last Updated: September 2010

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

Text Part Number: 78-16891-01

Cisco ONS 15454 Troubleshooting Guide, Release 6.0

CONTENTS

FIGURES

About this Guide

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

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

This section provides the following information:

Revision History

Date	Notes
March 2007	Revision History Table added for the first time
April 2007	Added additional description for APSCM alarm in the “Alarm Troubleshooting” chapter.
August 2007	Replaced TX Power High column name with OPT-HIGH in the HI-TX Power section of the Alarm Troubleshooting chapter.

Date	Notes
September 2007	Updated the caution in the Side Switch the Active and Standby Cross-Connect Cards section of the "Alarm Troubleshooting" chapter. Added a note, caution, and rule in the Side Switch the Active and Standby Cross-Connect Cards section of the "Alarm Troublesooting" chapter.
June 2008	Updated FAILTOSW alarm in Alarm Troubleshooting chapter.
February 2009	Updated PORT-MISMATCH alarm details in Chapter 2, Alarm Troubleshooting.
June 2009	Updated PWR-FAIL-A, PWR-FAIL-B, PWR-FAIL-RET-A, and PWR-FAIL-RET-B alarm details in Chapter 2, Alarm Troubleshooting.
July 2009	• Updated the COMIOXC alarm details in Chapter 2, Alarm Troubleshooting. • Updated the description of GFP-LFD alarm in Chapter 2, Alarm Troubleshooting.
August 2009	Updated MEM-GONE alarm description in Chapter 2, Alarm Troubleshooting.
November 2009	Updated the card details for LCAS alarms in Chapter 2, Alarm Troubleshooting.
February 2010	Changed the BIEC parameter to BIT-EC in Chapter 5, "Performance Monitoring".
July 2010	Updated table in Chapter Error Messages.
September 2010	Updated the "Clear the COMIOXC Alarm" procedure in the chapter, "Alarm Troubleshooting".

Document Objectives

This guide gives general troubleshooting instructions, alarm troubleshooting instructions, equipment replacement instructions, and a list of error messages that apply to the ONS 15454. This information is contained in four chapters. Use this guide in conjunction with the appropriate publications listed in the Related Documentation section.

Audience

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

Document Organization

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

- Chapter 1, "General Troubleshooting," provides methods to discover hardware errors, such as failed ports, that adversely affect signal traffic; it also gives typical software problems that occur and their solutions.
- Chapter 2, "Alarm Troubleshooting," provides indexes, descriptions, and troubleshooting methods for all alarms and conditions generated by the ONS 15454.
- Chapter 3, "Transients Conditions," describes temporary (transient) conditions.

- Chapter 4, "Error Messages," provides a comprehensive list of all ONS 15454 error messages and their identification numbers.
- Chapter 5, "Performance Monitoring," defines performance monitoring parameters for all ONS 15454 cards.
- Chapter 6, "SNMP," describes simple network management protocol (SNMP) applications as they apply to the Cisco ONS 15454.

Related Documentation

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

- *Cisco ONS 15454 Procedure Guide*
  Provides procedures to install, turn up, test, and maintain an ONS 15454 node and network.
- *Cisco ONS 15454 Reference Manual*
  Provides installation, turn up, test, and maintenance procedures.
- *Cisco ONS SONET TL1 Command Guide*
  Provides a full TL1 command and autonomous message set including parameters, AIDs, conditions and modifiers for the Cisco ONS 15454, ONS 15327, ONS 15600 and ONS 15310-CL systems.
- *Cisco ONS SONET TL1 Reference Guide*
  Provides general information, procedures, and errors for TL1 in the Cisco ONS 15454, ONS 15327, ONS 15600 and ONS 15310-CL systems.
- *Ethernet Card Software Feature and Configuration G uide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*
  Provides software features for all Ethernet cards and configuration information for Cisco IOS on ML-Series cards.
- *Release Notes for the Cisco ONS 15454 Release 6.0*
  Provides caveats, closed issues, and new feature and functionality information.

Refer to the following standards documentation referenced in this publication:

- Telcordia GR-253 CORE

Document Conventions

This publication uses the following conventions:

Convention	Application
boldface	Commands and keywords in body text.
italic	Command input that is supplied by the user.
[ ]	Keywords or arguments that appear within square brackets are optional.
{ x | x | x }	A choice of keywords (represented by x) appears in braces separated by vertical bars. The user must select one.

Convention	Application
Ctrl	The control key. For example, where Ctrl + D is written, hold down the Control key while pressing the D key.
`screen font`	Examples of information displayed on the screen.
`boldface screen font`	Examples of information that the user must enter.
< >	Command parameters that must be replaced by module-specific codes.

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

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

Warning **IMPORTANT SAFETY INSTRUCTIONS**

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

SAVE THESE INSTRUCTIONS

Waarschuwing **BELANGRIJKE VEILIGHEIDSINSTRUCTIES**

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

BEWAAR DEZE INSTRUCTIES

Varoitus **TÄRKEITÄ TURVALLISUUSOHJEITA**

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

SÄILYTÄ NÄMÄ OHJEET

Attention **IMPORTANTES INFORMATIONS DE SÉCURITÉ**

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

CONSERVEZ CES INFORMATIONS

Warnung **WICHTIGE SICHERHEITSHINWEISE**

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

BEWAHREN SIE DIESE HINWEISE GUT AUF.

Avvertenza **IMPORTANTI ISTRUZIONI SULLA SICUREZZA**

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

CONSERVARE QUESTE ISTRUZIONI

Advarsel **VIKTIGE SIKKERHETSINSTRUKSJONER**

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

TA VARE PÅ DISSE INSTRUKSJONENE

Aviso **INSTRUÇÕES IMPORTANTES DE SEGURANÇA**

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

GUARDE ESTAS INSTRUÇÕES

¡Advertencia! **INSTRUCCIONES IMPORTANTES DE SEGURIDAD**

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

GUARDE ESTAS INSTRUCCIONES

Varning! **VIKTIGA SÄKERHETSANVISNINGAR**

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

SPARA DESSA ANVISNINGAR

FONTOS BIZTONSÁGI ELOÍRÁSOK

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

ORIZZE MEG EZEKET AZ UTASÍTÁSOKAT!

Предупреждение **ВАЖНЫЕ ИНСТРУКЦИИ ПО СОБЛЮДЕНИЮ ТЕХНИКИ БЕЗОПАСНОСТИ**

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

СОХРАНИТЕ ЭТИ ИНСТРУКЦИИ

警告 重要的安全性说明

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

请保存这些安全性说明

警告　安全上の重要な注意事項

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

これらの注意事項を保管しておいてください。

주의　중요 안전 지침

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

이 지시 사항을 보관하십시오.

Aviso　INSTRUÇÕES IMPORTANTES DE SEGURANÇA

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

GUARDE ESTAS INSTRUÇÕES

Advarsel　VIGTIGE SIKKERHEDSANVISNINGER

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

GEM DISSE ANVISNINGER

تحذير　إرشادات الأمان الهامة

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

Upozorenje

VAŽNE SIGURNOSNE NAPOMENE

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

SAČUVAJTE OVE UPUTE

Upozornění

DŮLEŽITÉ BEZPEČNOSTNÍ POKYNY

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

USCHOVEJTE TYTO POKYNY

Προειδοποίηση

ΣΗΜΑΝΤΙΚΕΣ ΟΔΗΓΙΕΣ ΑΣΦΑΛΕΙΑΣ

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

ΦΥΛΑΞΤΕ ΑΥΤΕΣ ΤΙΣ ΟΔΗΓΙΕΣ

אזהרה

הוראות בטיחות חשובות

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

שמור הוראות אלה

Opomena

ВАЖНИ БЕЗБЕДНОСНИ НАПАТСТВИЈА

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

ЧУВАЈТЕ ГИ ОВИЕ НАПАТСТВИЈА

Ostrzeżenie **WAŻNE INSTRUKCJE DOTYCZĄCE BEZPIECZEŃSTWA**

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

NINIEJSZE INSTRUKCJE NALEŻY ZACHOWAĆ

Upozornenie **DÔLEŽITÉ BEZPEČNOSTNÉ POKYNY**

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

USCHOVAJTE SI TENTO NÁVOD

Obtaining Optical Networking Information

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

Where to Find Safety and Warning Information

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

Cisco Optical Networking Product Documentation CD-ROM

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

Obtaining Documentation and Submitting a Service Request

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

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

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

General Troubleshooting

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

This chapter provides procedures for troubleshooting the most common problems encountered when operating a Cisco ONS 15454. To troubleshoot specific ONS 15454 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).

This chapter includes the following sections on network problems:

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

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

- 1.2 Troubleshooting Electrical Circuit Paths With Loopbacks, page 1-9—Explains how to use loopback tests described in "1.1 Troubleshooting Non-DWDM Circuit Paths with Loopbacks" to isolate trouble on DS-1, DS-3, or EC-1 electrical circuits.
- 1.3 Troubleshooting DS3XM-6 or DS3XM-12 Card Electrical Paths With FEAC Loopbacks, page 1-46—Describes how DS3XM-6 and DS3XM-12 card far-end alarm and control (FEAC) functions.
- 1.4 Troubleshooting DS1-E1-56 Card with Far End Loopcodes, page 1-47
- 1.5 Troubleshooting Optical Circuit Paths With Loopbacks, page 1-48—Explains how to use loopback tests described in "1.1 Troubleshooting Non-DWDM Circuit Paths with Loopbacks" to isolate trouble on OC-N optical circuits.
- 1.6 Troubleshooting Ethernet Circuit Paths With Loopbacks, page 1-71—Explains how to use loopback tests described in "1.1 Troubleshooting Non-DWDM Circuit Paths with Loopbacks" to isolate trouble on G-Series or CE-Series Ethernet circuits.
- 1.7 Troubleshooting MXP, TXP, or FC_MR-4 Circuit Paths With Loopbacks, page 1-90—Explains how to use loopbacks tests described in "1.1 Troubleshooting Non-DWDM Circuit Paths with Loopbacks" to isolate trouble on muxponder (MXP), transponder (TXP), or Fibre Channel (FC_MR) circuits.

- 1.8 Troubleshooting DWDM Circuit Paths With ITU-T G.709 Monitoring, page 1-105—Explains how to utilize performance monitoring (PM) and threshold crossing alerts (TCA) to locate signal degrades on DWDM circuit paths.

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

- 1.9 Using CTC Diagnostics, page 1-113—Explains how to perform card LED tests, download a diagnostic file for Cisco Technical Support, and create a bidirectional diagnostic VT circuit.
- 1.10 Restoring the Database and Default Settings, page 1-119—Provides procedures for restoring software data and restoring the node to the default setup.
- 1.11 PC Connectivity Troubleshooting, page 1-119—Provides troubleshooting procedures for PC and network connectivity to the ONS 15454.
- 1.12 CTC Operation Troubleshooting, page 1-125—Provides troubleshooting procedures for Cisco Transport Controller (CTC) login or operation problems.
- 1.13 Circuits and Timing, page 1-140—Provides troubleshooting procedures for circuit creation and error reporting as well as timing reference errors and alarms.
- 1.14 Fiber and Cabling, page 1-145—Provides troubleshooting procedures for fiber and cabling connectivity errors.
- 1.15 Power Supply Problems, page 1-155—Provides troubleshooting procedures for power supply problems.

1.1 Troubleshooting Non-DWDM Circuit Paths with Loopbacks

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

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

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

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

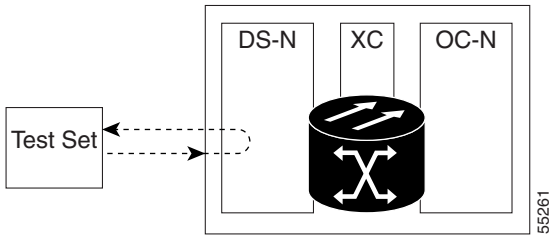
1.1.1 Facility Loopbacks

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

1.1.1.1 General Behavior

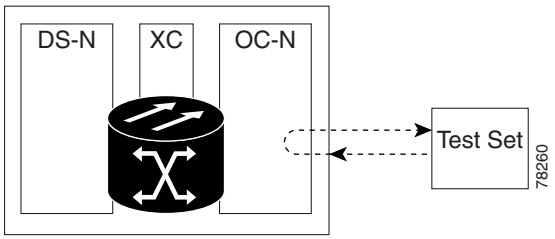
A facility (line) loopback tests the line interface unit (LIU) of a card, the electrical interface assembly (EIA), and related cabling. After applying a facility loopback on a port, use a test set to run traffic over the loopback. A successful facility loopback isolates the LIU, the EIA, or the cabling plant as the potential cause of a network problem. Figure 1-1 shows a facility loopback on a DS-N electrical card.

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



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

Figure 1-2 Facility (Line) Loopback Path on a Near-End OC-N Card



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

Figure 1-3 OC-N Facility Loopback Indicator

Caution Before performing a facility (line) loopback on an OC-N card, be sure the card contains at least two data communications channel (DCC) paths to the node where the card is installed. A second DCC provides a nonlooped path to log into the node after the loopback is applied, enabling you to remove the facility loopback. Ensuring a second DCC is not necessary if you are directly connected to the ONS 15454 containing the loopback OC-N card.

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

1.1.1.2 ONS 15454 Card Behavior

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

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

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

Table 1-1 ONS 15454 Card Facility Loopback Behavior

Card/Port	Facility Loopback Signal
DS-1	Terminated
DS-3	Terminated
DS3XM-6 or DS3XM-12	Terminated
All OC-N cards	Terminated
EC-1	Terminated
G-Series Ethernet	Terminated[1]
MXP, MXPP trunk ports	Bridged
MXP, MXPP client ports	Terminated
TXP, MXPP trunk ports	Bridged
TXP, MXPP client ports	Terminated

1. G-Series facility loopback is terminated and no AIS is sent downstream. However, the Cisco Link Integrity signal continues to be sent downstream.

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

- If an electrical or optical port is in the Out-of-Service and Management, Disabled (OOS-MA,DSBLD) service state, it injects an AIS signal upstream and downstream.
- When an electrical or optical port is placed in the OOS-MA,MT 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 in the *Cisco ONS 15454 Procedure Guide*.

MXP, TXP, and FC_MR-4 card facility loopbacks behave differently from other ONS 15454 cards. With a client-side facility loopback, the client port service state is OOS-MA,LPBK & MT; however the remaining client and trunk ports can be in any other service state. For cards in a trunk-side facility loopback, the trunk port service state is OOS-MA,LPBK & MT service state and the remaining client and trunk ports can be in any other service state.

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

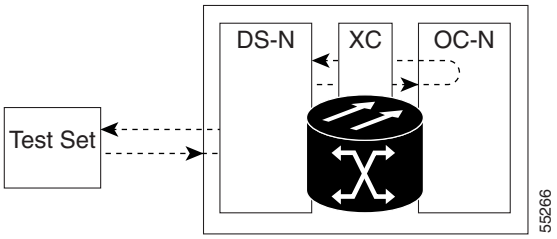
1.1.2 Terminal Loopbacks

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

1.1.2.1 General Behavior

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

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

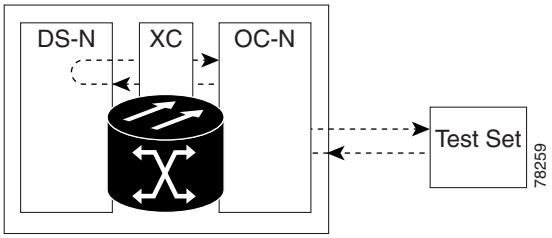


In CTC, OC-N cards with terminal loopbacks show an icon (Figure 1-5). Loopback icons are not shown on other cards in this release.

Figure 1-5 Terminal Loopback Indicator

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

Figure 1-6 Terminal Loopback Path on a DS-N Card



1.1.2.2 ONS 15454 Card Behavior

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

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

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

Table 1-2 ONS 15454 Card Terminal Loopback Behavior

Card/Port	Terminal Loopback Signal
DS-1	Terminated
DS-3	Bridged
DS3XM-6 or DS3XM-12	Bridged
All OC-N cards	Bridged
EC-1	Bridged
G-Series Ethernet	Terminated[1]
MXP, MXPP trunk ports	Bridged
MXP, MXPP client ports	Terminated
TXP, MXPP trunk ports	Bridged
TXP, MXPP client ports	Terminated

1. G-Series Ethernet terminal loopback is terminated and Ethernet transmission is disabled. No AIS is inserted for Ethernet, but a TPTFAIL alarm is raised on the far-end Ethernet port.

Bridged DS-N and OC-N terminal loopback examples are shown in Figure 1-7 and Figure 1-8.

Figure 1-7 Terminal Loopback on a DS-N Card with Bridged Signal

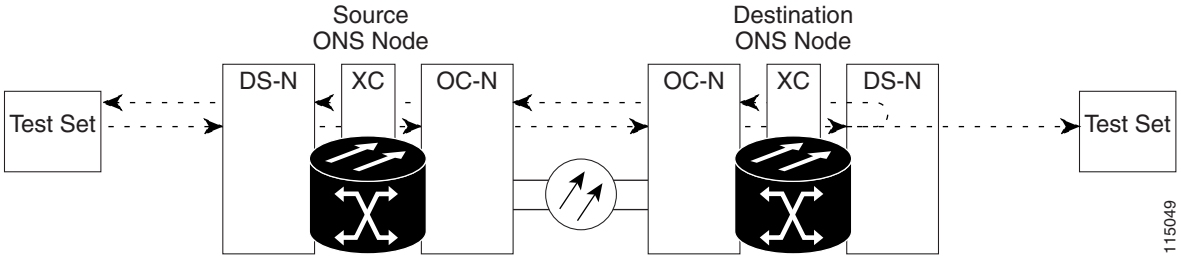
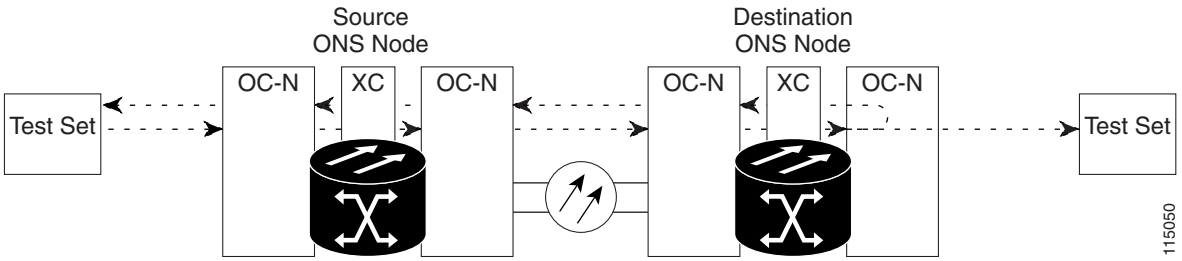


Figure 1-8 Terminal Loopback on an OC-N Card with Bridged Signal



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

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

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

MXP and TXP trunk and client ports have different service state behaviors and requirements from other ONS 15454 cards. The cards can simultaneously maintain different service states.

- For TXP and TXPP cards with a client-side terminal loopback, the client port is in the OOS-MA,LPBK & MT service state and trunk port must be in IS-NR service state.
- For MXP and MXPP cards with a client-side terminal loopback, the client port is in the OOS-MA,LPBK & MT service state and the remaining client and trunk ports can be in any service state.

- In MXP or TXP trunk-side terminal loopbacks, the trunk port is in the OOS-MA,LPBK & MT service state and the client ports must be in IS-NR service state for complete loopback functionality. A terminal loopback affects all client ports because it is performed on the aggregate signal.

The loopback itself is listed in the Conditions window. For example, the window would list the LPBKTERMINAL condition or LPBKFACILITY condition for a tested port. (The Alarms window would show 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:

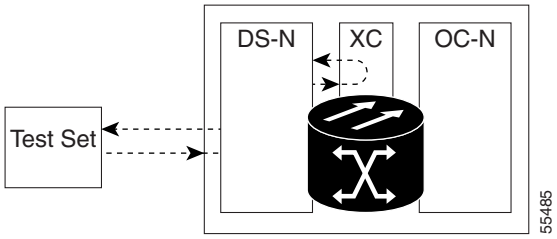
- If an electrical or optical port is in the OOS-MA,DSBLD service state, it injects an AIS signal upstream and downstream.
- When an electrical or optical port is placed in the OOS-MA,MT service state before loopback testing, the port clears the AIS signal upstream and downstream unless there is a service-affecting 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 15454 Procedure Guide*.

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

1.1.3 Hairpin Circuits

A hairpin circuit sends traffic in and out an electrical port rather than sending the traffic onto the OC-N card. A hairpin loops back only the specific synchronous transport signal (STS) or virtual tributary (VT) circuit and does not cause an entire OC-N port to loop back, preventing all traffic on the OC-N port from dropping. The hairpin allows you to test a specific STS or VT circuit on nodes running live traffic. Figure 1-9 shows the hairpin circuit path on a DS-N card.

Figure 1-9 Hairpin Circuit Path on a DS-N Card



1.1.4 Cross-Connect Loopbacks

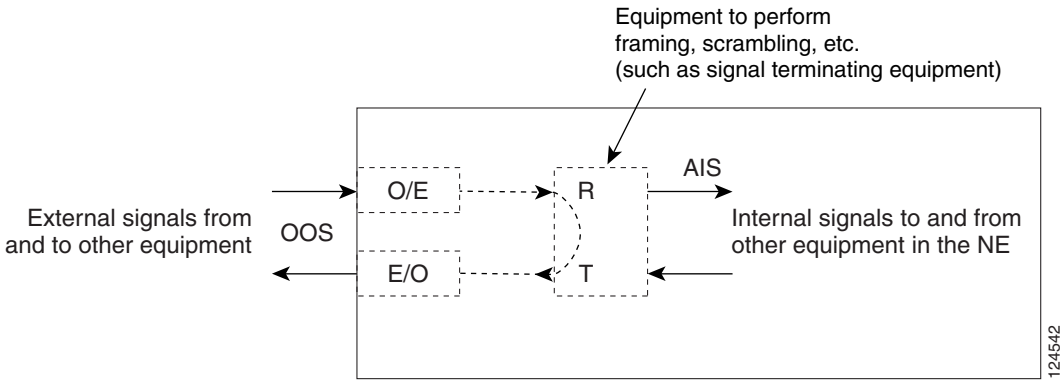
A cross-connect (XC) loopback tests an OC-N circuit path as it passes through the cross-connect card and loops back to the port being tested without affecting other traffic on the optical port. Cross-connect loopbacks are less invasive than terminal or facility loopbacks. Facility and terminal loopback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

allows you to create a loopback on any embedded channel at supported payloads of STS-1 granularity and higher. For example, you can place a loopback on a single STS-1, STS-3c, STS-6c, etc. on an optical facility (line) without interrupting the other STS circuits.

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

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

Figure 1-10 Network Element with SONET Cross-Connect Loopback Function



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

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

1.2 Troubleshooting Electrical Circuit Paths With Loopbacks

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

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

Note These procedures apply to DS-1, DS-3, and EC-1 cards. The test sequence for your circuits will differ according to the type of circuit and network topology.

West-to-east direction (left to right):

1. A facility (line) loopback on the source-node electrical port (DS-N or EC-N)
2. A hairpin on the source-node electrical port

3. An XC loopback on the destination-node OC-N STS (carrying the electrical circuit)
4. A terminal (inward) loopback on the destination-node electrical port

East-to-west direction (right to left):

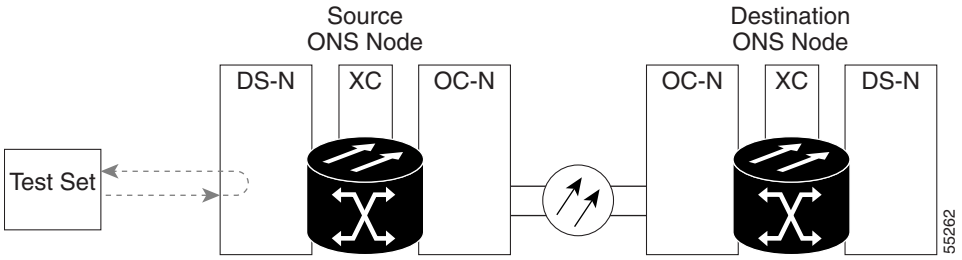
1. A facility (line) loopback on the destination-node electrical port
2. A hairpin on the destination-node electrical port
3. An XC loopback on the source-node OC-N STS (carrying the electrical circuit)
4. A terminal (inward) loopback on the source-node electrical port

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

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

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

Figure 1-11 Facility (Line) Loopback on a Circuit Source DS-N Port



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

Note Facility loopbacks require on-site personnel.

Note ONS 15454 DS-3 terminal (inward) loopbacks do not transmit an AIS in the direction away from the loopback. Instead of AIS, a continuance of the signal transmitted into the loopback is provided. A DS3/EC1-48 card can be provisioned to transmit AIS for a terminal loopback if desired.

Depending upon your card type, complete the "Create the Facility (Line) Loopback on the Source DS-1, DS-3, DS3N-12, DS3i-N-12, or EC1 Port" procedure on page 1-11 or the "Create the Facility (Line) Loopback on the Source DS3E or DS3XM Port" procedure on page 1-12, then test and clear the loopbacks as instructed.

Create the Facility (Line) Loopback on the Source DS-1, DS-3, DS3N-12, DS3i-N-12, or EC1 Port

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

Use appropriate cabling to attach the Tx and Rx terminals of the electrical test set to the EIA connectors or DSx panel for the port you are testing. The Tx and Rx terminals connect to the same port.

Step 2 Adjust the test set accordingly. (For specific procedures to use the test set equipment, consult the manufacturer.)

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

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

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

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

Step 7 Click **Apply**.

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

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

Step 9 Complete the "Test and Clear the DS-3, DS3N-12, DS3i-N-12, or EC1 Port Facility Loopback Circuit" procedure on page 1-11.

Test and Clear the DS-3, DS3N-12, DS3i-N-12, or EC1 Port Facility Loopback Circuit

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

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

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

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

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

Step 6 Choose the appropriate state (**IS**; **OOS,DSBLD**; **OOS,MT**; **IS,AINS**) from the Admin State column for the port being tested.

Step 7 Click **Apply**.

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

Step 9 Complete the "Test the Electrical Cabling" procedure on page 1-13.

Create the Facility (Line) Loopback on the Source DS3E or DS3XM Port

This procedure applies to DS3E, DS3XM-6, and DS3XM-12 cards. It does not utilize the DS3XM card FEAC loopback functions. For this information, refer to the "1.3 Troubleshooting DS3XM-6 or DS3XM-12 Card Electrical Paths With FEAC Loopbacks" section on page 1-46.

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

Use appropriate cabling to attach the Tx and Rx terminals of the electrical test set to the EIA connectors or DSx panel for the port you are testing. The Tx and Rx terminals connect to the same port.

Step 2 Adjust the test set accordingly. (For specific procedures to use the test set equipment, consult the manufacturer.)

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

Step 4 For any of these cards, click the **Maintenance > DS3** tabs.

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

Step 5 For the DS3 tab, choose **OOS,MT** from the Admin State column for the port being tested. If this is a multiport card, select the appropriate row for the port being tested. For the DS1 tab, no state selection is necessary unless the DS-1 has been placed in service. The loopback/send code cannot be selected for a DS-1 if the derived state is OOS,DSBLD.

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

Step 7 Click **Apply**.

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

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

Step 9 Complete the "Test and Clear the DS3E or DS3XM Port Facility Loopback Circuit" procedure on page 1-12.

Test and Clear the DS3E or DS3XM Port Facility Loopback Circuit

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

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

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

Step 4 For any of these cards, click the **Maintenance > DS3** tabs.

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

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

Step 6 Choose the appropriate state (**IS**; **OOS,DSBLD**; **OOS,MT**; **IS,AINS**) from the Admin State column for the port being tested.

Step 7 Click **Apply**.

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

Step 9 Complete the "Test the Electrical Cabling" procedure on page 1-13.

Test the Electrical Cabling

Step 1 Replace the suspected bad cabling (the cables from the test set to the DSx panel or the EIA ports) with a known-good cable. For instructions, refer to the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15454 Procedure Guide*.

If a known-good cable is not available, test the suspected bad cable with a test set. Remove the suspected bad cable from the DSx panel or the EIA and connect the cable to the Tx and Rx terminals of the test set. Run traffic to determine whether the cable is good or defective.

Step 2 Resend test traffic on the loopback circuit with a known-good cable installed. If the test set indicates a good circuit, the problem was probably the defective cable.

Step 3 Replace the defective cable.

Step 4 In card view for the electrical card, depending upon the type, click the **Maintenance > Loopback** tab, **Maintenance > DS1** tab, or **Maintenance > DS3** tab.

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

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

Step 6 Choose the appropriate state (**IS**; **OOS,DSBLD**; **OOS,MT**; **IS,AINS**) from the Admin State column for the port being tested.

Step 7 Click **Apply**.

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

Step 9 Complete the "Test the Electrical Card" procedure on page 1-13.

Test the Electrical Card

Step 1 Complete the "Physically Replace a Traffic Card" procedure on page 2-243 for the suspected bad card and replace it with a known-good one.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. refer to the procedures in the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-231. For more information, refer to the "Maintain the Node" chapter in the *Cisco ONS 15454 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 Return Materials Authorization (RMA) process. Contact Cisco Technical Support (1 800 553-2447).

Step 4 Complete the "Physically Replace a Traffic Card" procedure on page 2-243 for the faulty card.

Step 5 In card view for the electrical card, depending upon the type, click the **Maintenance > Loopback** tab, **Maintenance > DS1** tab, or **Maintenance > DS3** tab.

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

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

Step 7 Choose the appropriate state (**IS**; **OOS,DSBLD**; **OOS,MT**; **IS,AINS**) from the Admin State column for the port being tested.

Step 8 Click **Apply**.

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

Step 10 Complete the "Test the EIA" procedure on page 1-14.

Test the EIA

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

- **a.** Remove the lower backplane cover. Loosen the five screws that secure it to the ONS 15454 and pull it away from the shelf assembly.
- **b.** Loosen the nine perimeter screws that hold the EIA panel in place.
- **c.** Lift the EIA panel by the bottom to remove it from the shelf assembly.
- **d.** Follow the installation procedure for the appropriate EIA. Refer to the "Install the Shelf and Backplane Cable" procedure in the *Cisco ONS 15454 Procedure Guide* for instructions.

Step 2 Resend test traffic on the loopback circuit with known-good cabling, a known-good card, and the reinstalled EIA. If the test set indicates a good circuit, the problem was probably an improperly seated EIA, and you can proceed to Step 16. If the problem persists and the EIA is not shown to be improperly seated, proceed to Step 3.

Step 3 In card view for the electrical card, depending upon the type, click the **Maintenance > Loopback** tab, **Maintenance > DS1** tab, or **Maintenance > DS3** tab.

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

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

Step 5 Choose the appropriate state (**IS**; **OOS,DSBLD**; **OOS,MT**; **IS,AINS**) from the Admin State column for the port being tested.

Step 6 Click **Apply**.

Step 7 Click **Yes** in the confirmation dialog box. Proceed to Step 16.

Step 8 If the test set indicates a faulty circuit, the problem is probably a defective EIA. Return the defective EIA to Cisco through the RMA process. Contact Cisco Technical Support (1 800 553-2447).

Step 9 Replace the faulty EIA by completing the "Replace the Electrical Interface Assembly" procedure on page 2-250.

Step 10 Resend test traffic on the loopback circuit with known-good cabling, a known-good card, and the replacement EIA. If the test set indicates a faulty circuit, repeat all of the facility loopback procedures.

Step 11 If the test set indicates a good circuit, the problem was probably the defective EIA. Clear the facility (line) loopback by clicking the **Maintenance > Loopback** tab, **Maintenance > DS1** tab, or **Maintenance > DS3** tab.

Step 12 Choose **None** from the Loopback Type column for the port being tested.

Step 13 Choose the appropriate state (**IS**; **OOS,DSBLD**; **OOS,MT**; **IS,AINS**) from the Admin State column for the port being tested.

Step 14 Click **Apply**.

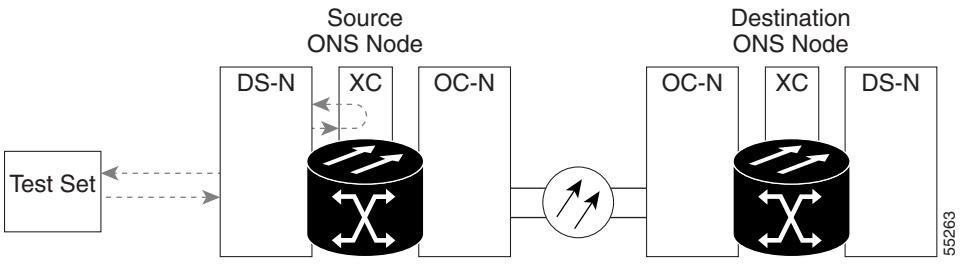
Step 15 Click **Yes** in the confirmation dialog box.

Step 16 Complete the "1.2.2 Perform a Hairpin Test on a Source-Node Electrical Port (West to East)" procedure on page 1-15.

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

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

Figure 1-12 Hairpin on a Source-Node Port



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

Note Hairpin loopbacks require on-site personnel.

Complete the "Create the Hairpin Circuit on the Source-Node Electrical Port" procedure on page 1-16.

Create the Hairpin Circuit on the Source-Node Electrical Port

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

a. If you just completed the "1.2.1 Perform a Facility (Line) Loopback on a Source Electrical Port (West to East)" procedure on page 1-10, leave the electrical test set hooked up to the electrical port in the source node.

b. If you are starting the current procedure without the electrical test set hooked up to the DS-N port, use appropriate cabling to attach the Tx and Rx terminals of the electrical test set to the DSx panel or the EIA connectors for 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 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 STS, and number, such as 1.

c. Click **Next**.

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

e. Choose the Size, such as STS-1.

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

g. Click **Next**.

h. In the Circuit Creation source dialog box, select the same Node, card Slot, Port, and STS (or VT) where the test set is connected. Leave Use Secondary Source unchecked.

i. Click **Next**.

j. In the Circuit Creation destination dialog box, use the same Node, card Slot, Port, and STS (or VT) used for the source dialog box. Leave Use Secondary Destination unchecked.

k. Click **Next**.

l. 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 and that the Dir column describes it as a one-way circuit.

Step 5 Complete the "Test and Delete the Electrical Port Hairpin Circuit" procedure on page 1-16.

Test and Delete the Electrical Port Hairpin Circuit

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

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

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

a. Click the **Circuits** tab.

b. Choose the hairpin circuit being tested.

c. Click **Delete**.

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

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

Step 4 Complete the "Test the Standby Cross-Connect Card" procedure on page 1-17.

Test the Standby Cross-Connect Card

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

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

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

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

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

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

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

Caution Cross-connect side switches, with the exception of side switches using XC-VXC-10G cards, are service-affecting. Any live traffic on any card in the node endures a hit of up to 50 ms. XC-VXC-10G side switches are errorless.

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

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

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

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

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

Step 3 Resend test traffic on the loopback circuit.

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

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

a. Click the **Circuits** tab.

b. Choose the hairpin circuit being tested.

c. Click **Delete**.

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

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

Step 5 To confirm a defective original cross-connect card, complete the "Retest the Original Cross-Connect Card" procedure on page 1-18.

Retest the Original Cross-Connect Card

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

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

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

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

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

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

Step 2 Resend test traffic on the loopback circuit.

Step 3 If the test set indicates a faulty circuit, the problem is probably the defective card. Return the defective card to Cisco through the RMA process. Contact Cisco Technical Support (1 800 553-2447) and proceed to Step 4. If the test does not indicate a faulty circuit, proceed to Step 5.

Step 4 Complete the "Physically Replace an In-Service Cross-Connect Card" procedure on page 2-243 for the defective card.

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 hairpin circuit:

a. Click the **Circuits** tab.

b. Choose the hairpin circuit being tested.

c. Click **Delete**.

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

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

Step 6 Complete the "1.2.3 Perform an XC Loopback on a Destination-Node OC-N STS (West to East) Carrying an Electrical Signal" procedure on page 1-19.

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

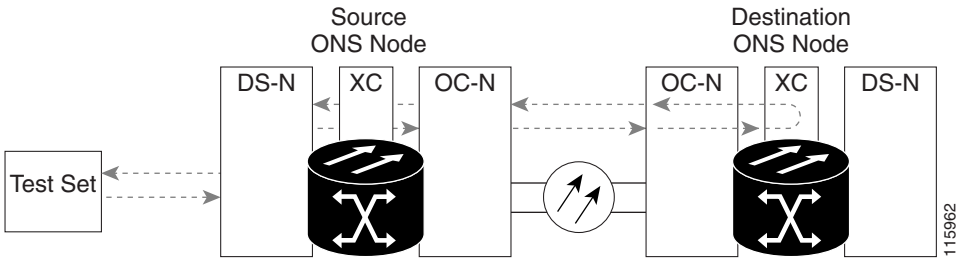
The XC loopback tests whether any problem exists on the circuit's OC-N span, isolating this span from others present on the card. The loopback occurs on the cross-connect card in a network circuit. Figure 1-13 shows an example of an XC loopback on a destination OC-N port. The traffic pattern looks similar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

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

Note XC loopbacks do not require on-site personnel.

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

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



Create the XC Loopback on a Destination-Node OCN STS

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

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

a. If you just completed the "1.2.2 Perform a Hairpin Test on a Source-Node Electrical Port (West to East)" procedure on page 1-15, leave the optical test set hooked up to the destination-node port.

b. If you are starting the current procedure without the optical test set hooked up to the destination port, use appropriate cabling to attach the 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 **OOS,MT** 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 OC-N card to display the card view.
b. Click the **Maintenance > Loopback > SONET STS** tab.
c. Click the check box in the **XC Loopback** column for the port being tested.
d. Check **Apply**.
e. Click **Yes** in the confirmation dialog box.

Step 5 Complete the "Test and Clear the XC Loopback Circuit" procedure on page 1-20.

Test and Clear the XC Loopback Circuit

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

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

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

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

a. In card view, click the **Maintenance > Loopback > SONET STS** tab.
b. Uncheck the check box in the **XC Loopback** column for the circuit being tested.
c. Click **Apply**.
d. Click **Yes** in the confirmation dialog box.

Step 4 Complete the "Test the Standby Cross-Connect Card" procedure on page 1-20.

Test the Standby Cross-Connect Card

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

a. Determine the standby cross-connect card. On both the physical node and the CTC node view window, the standby cross-connect ACT/SBY LED is amber and the active card ACT/SBY LED is green.
b. Position the cursor over the standby cross-connect card.
c. Right-click and choose **RESET CARD**.

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

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

Caution Cross-connect side switches, with the exception of side switches using XC-VXC-10G cards, are service-affecting. Any live traffic on any card in the node endures a hit of up to 50 ms. XC-VXC-10G side switches are errorless.

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

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

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

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

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

Step 3 Resend test traffic on the loopback circuit.

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

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

a. Click the **Circuits** tab.

b. Choose the XC loopback circuit being tested.

c. Click **Delete**.

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

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

Step 5 To confirm a defective original cross-connect card, complete the "Retest the Original Cross-Connect Card" procedure on page 1-21.

Retest the Original Cross-Connect Card

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

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

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

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

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

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

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

Step 2 Resend test traffic on the loopback circuit.

Step 3 If the test set indicates a faulty circuit, the problem is probably the defective card. Return the defective card to Cisco through the RMA process. 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 "Physically Replace an In-Service Cross-Connect Card" procedure on page 2-243 for the defective cross-connect card and 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**.

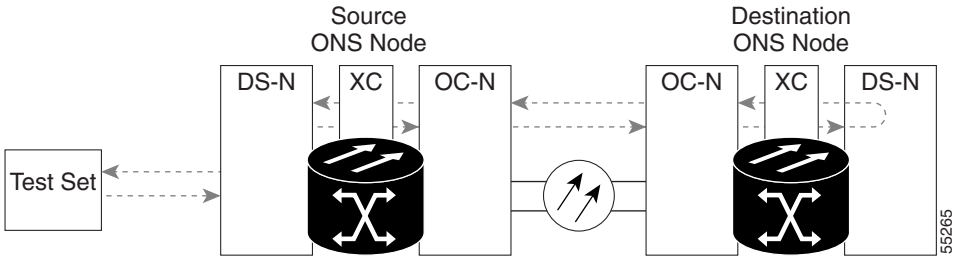
d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

Step 6 If the tests indicate further problems, go to the "1.2.4 Perform a Terminal (Inward) Loopback on a Destination Electrical Port Port (West to East)" procedure on page 1-22.

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

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

Figure 1-14 Terminal (Inward) Loopback to a Destination DS-N Port



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

Note Terminal loopbacks require on-site personnel.

Note ONS 15454 DS-3 terminal (inward) loopbacks do not transmit an AIS in the direction away from the loopback. Instead of AIS, a continuance of the signal transmitted into the loopback is provided. A DS3/EC1-48 card can be provisioned to transmit AIS for a terminal loopback if desired.

Depending upon your card type, complete the "Create the Terminal (Inward) Loopback on a Destination DS-3, DS3N-12, DS3i-N-12, or EC1 Port" procedure on page 1-23 or the"Create the Terminal (Inward) Loopback on a Destination DS-3E or DS3XM Port" procedure on page 1-25. Then test and clear the loopback as instructed.

Create the Terminal (Inward) Loopback on a Destination DS-3, DS3N-12, DS3i-N-12, or EC1 Port

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

- **a.** If you just completed the "1.2.3 Perform an XC Loopback on a Destination-Node OC-N STS (West to East) Carrying an Electrical Signal" procedure on page 1-19, leave the electrical test set hooked up to the source-node port.
- **b.** If you are starting the current procedure without the electrical test set hooked up to the electrical port, use appropriate cabling to attach the Tx and Rx terminals of the electrical test set to the DSx panel or the EIA connectors for the port you are testing. Both Tx and Rx connect to the same port.

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

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

Step 4 In the Circuit Creation dialog box, choose the type, such as STS, and number, such as 1.

Step 5 Click **Next**

Step 6 In the next Circuit Creation dialog box, give the circuit an easily identifiable name such as DS1toDS2.

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

Step 8 Click **Next**.

Step 9 In the Circuit Creation source dialog box, select the **Node**, card **Slot**, **Port**, and **STS (or VT)** where the test set is connected.

Step 10 Click **Next**.

Step 11 In the Circuit Creation destination dialog box, use the same Node, card Slot, Port, and STS (or VT) used for the source dialog box.

Step 12 Click **Next**.

Step 13 In the Circuit Creation circuit routing preferences dialog box, leave all defaults. Click **Finish**.

Step 14 Confirm that the newly created circuit appears in the Dir column as a two-way circuit.

Note It is normal for the "LPBKTERMINAL (DS1, DS3)" condition on page 2-157 to appear during a loopback setup. The condition clears when you remove the loopback.

Note ONS 15454 DS-3 terminal (inward) loopbacks do not transmit an AIS in the direction away from the loopback. Instead of AIS, a continuance of the signal transmitted into the loopback is provided. A DS3/EC1-48 card can be provisioned to transmit AIS for a terminal loopback if desired.

Step 15 Create the terminal (inward) loopback on the destination port being tested:

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

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

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

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

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

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

f. Click **Apply**.

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

Step 16 Complete the "Test and Clear the DS-3, DS3N-12, DS3i-N-12, or EC1 Destination Port Terminal Loopback Circuit" procedure on page 1-24.

Test and Clear the DS-3, DS3N-12, DS3i-N-12, or EC1 Destination Port Terminal Loopback Circuit

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

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

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

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

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

Step 6 Select the appropriate state (**IS**; **OOS,DSBLD**; **OOS,MT**; **IS,AINS**) in the Admin State column for the port being tested.

Step 7 Click **Apply**.

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

Step 9 Clear the terminal loopback:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

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

Step 10 Complete the "Test the Destination Electrical Card" procedure on page 1-27.

Create the Terminal (Inward) Loopback on a Destination DS-3E or DS3XM Port

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

a. If you just completed the "1.2.3 Perform an XC Loopback on a Destination-Node OC-N STS (West to East) Carrying an Electrical Signal" procedure on page 1-19, leave the electrical test set hooked up to the electrical port in the source node.

b. If you are starting the current procedure without the electrical test set hooked up to the electrical port, use appropriate cabling to attach the Tx and Rx terminals of the electrical test set to the DSx panel or the EIA connectors for 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 In CTC node view, click the **Circuits** tab and click **Create**.

Step 3 In the Circuit Creation dialog box, choose the type, such as STS, and number, such as 1.

Step 4 Click **Next**.

Step 5 In the next Circuit Creation dialog box, give the circuit an easily identifiable name such as DS1toDS3.

Step 6 Leave the **Bidirectional** check box checked.

Step 7 Click **Next**.

Step 8 In the Circuit Creation source dialog box, select the **Node**, card **Slot**, **Port**, and **STS (or VT)** where the test set is connected.

Step 9 Click **Next**.

Step 10 In the Circuit Creation destination dialog box, use the same Node, card Slot, Port, and STS (or VT) used for the source dialog box.

Step 11 Click **Next**.

Step 12 In the Circuit Creation circuit routing preferences dialog box, leave all defaults. Click **Finish**.

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

Note It is normal for the "LPBKTERMINAL (DS1, DS3)" condition on page 2-157 to appear during a loopback setup. The condition clears when you remove the loopback.

Note ONS 15454 DS-3 terminal (inward) loopbacks do not transmit an AIS in the direction away from the loopback. Instead of AIS, a continuance of the signal transmitted into the loopback is provided. A DS3/EC1-48 card can be provisioned to transmit AIS for a terminal loopback if desired.

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

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

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

c. Click the **Maintenance > DS3** tabs.

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

d. For the DS3 tab, choose **OOS,MT** from the Admin State column for the port being tested. If this is a multiport card, select the appropriate row for the port being tested. For the DS1 tab, no state selection is necessary unless the DS-1 has been placed in service. The loopback/send code cannot be selected for a DS-1 if the derived state is OOS,DSBLD.

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

f. Click **Apply**.

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

Step 15 Complete the "Test and Clear the DS-3E or DS3XM Destination Port Terminal Loopback Circuit" procedure on page 1-26.

Test and Clear the DS-3E or DS3XM Destination Port Terminal Loopback Circuit

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

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

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

Step 4 Click the **Maintenance > DS3** tabs.

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

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

Step 6 Select the appropriate state (**IS**; **OOS,DSBLD**; **OOS,MT**; **IS,AINS**) in the Admin State column for the port being tested.

Step 7 Click **Apply**.

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

Step 9 Clear the terminal loopback:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

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

Step 10 Complete the "Test the Destination Electrical Card" procedure on page 1-27.

Test the Destination Electrical Card

Step 1 Complete the "Physically Replace a Traffic Card" procedure on page 2-243 for the suspected bad card and replace it with a known-good one.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Refer to the procedures in the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-231. For more information, refer to the "Maintain the Node" chapter in the *Cisco ONS 15454 Procedure Guide*.

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 (1 800 553-2447).

Step 4 Complete the "Physically Replace a Traffic Card" procedure on page 2-243 for the defective electrical card.

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

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

b. Depending upon the card type, click the **Maintenance > Loopback** tab, **Maintenance > DS1** tab, or **Maintenance > DS3** tab.

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

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

d. Select the appropriate state (**IS**; **OOS,DSBLD**; **OOS,MT**; **IS,AINS**) in the Admin State column for the port being tested.

e. Click **Apply**.

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

Step 6 Delete the terminal (inward) loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

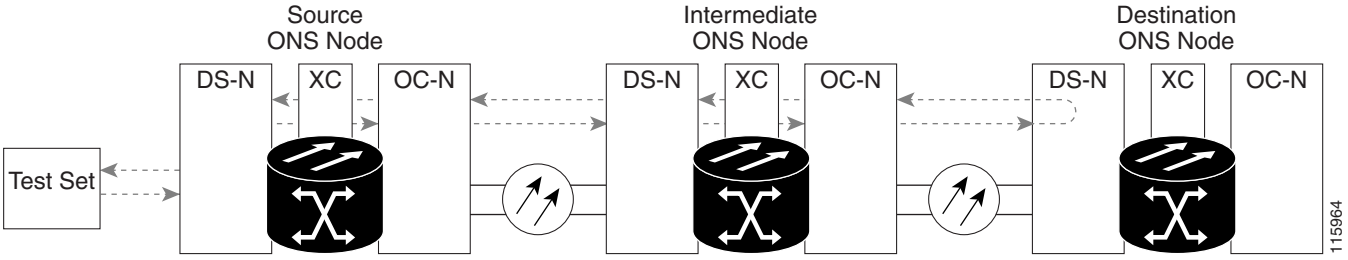
d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

Step 7 Complete the "1.2.5 Perform a Facility (Line) Loopback on a Destination-Node Electrical Port (East to West)" procedure on page 1-28.

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

The facility (line) loopback test is performed on the destination-node electrical port in the network circuit. Completing a successful facility (line) loopback on this port isolates the cabling, the electrical card, and the EIA as possible failure points. Figure 1-15 shows an example of a facility loopback on a destination DS-N port.

Figure 1-15 Facility (Line) Loopback on a Circuit Destination DS-N Port



Caution Performing a loopback on an in-service circuit is service-affecting. To protect traffic, apply a lockout or Force switch to the target loopback port. For basic instructions, refer to the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-231. For more information about these operations, refer to the "Maintain the Node" chapter in the *Cisco ONS 15454 Procedure Guide*.

Note Facility loopbacks require on-site personnel.

Note ONS 15454 DS-3 terminal (inward) loopbacks do not transmit an AIS in the direction away from the loopback. Instead of AIS, a continuance of the signal transmitted into the loopback is provided. A DS3/EC1-48 card can be provisioned to transmit AIS for a terminal loopback if desired.

Depending upon your card type, complete the "Create the Facility (Line) Loopback on the Destination DS-1, DS-3, DS3N-12, DS3i-N-12, or EC1 Port" procedure on page 1-29 or the "Create the Facility (Line) Loopback on the Source DS3E or DS3XM Port" procedure on page 1-30. Then test and clear the loopback as instructed.

Create the Facility (Line) Loopback on the Destination DS-1, DS-3, DS3N-12, DS3i-N-12, or EC1 Port

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

a. If you just completed the "1.2.4 Perform a Terminal (Inward) Loopback on a Destination Electrical Port Port (West to East)" procedure on page 1-22, leave the electrical test set hooked up to the destination-node port.

b. Use appropriate cabling to attach the Tx and Rx terminals of the electrical test set to the EIA connectors or DSx panel for the port you are testing. The Tx and Rx terminals connect to the same port.

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

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

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

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

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

Step 7 Click **Apply**.

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

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

Step 9 Complete the "Test and Clear the DS-3, DS3N-12, DS3i-N-12, or EC1 Port Facility Loopback Circuit" procedure on page 1-29.

Test and Clear the DS-3, DS3N-12, DS3i-N-12, or EC1 Port Facility Loopback Circuit

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

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

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

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

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

Step 6 Choose the appropriate state (**IS**; **OOS,DSBLD**; **OOS,MT**; **IS,AINS**) from the Admin State column for the port being tested.

Step 7 Click **Apply**.

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

Step 9 Complete the "Test the Electrical Cabling" procedure on page 1-31.

Create the Facility (Line) Loopback on the Source DS3E or DS3XM Port

This procedure applies to DS3E, DS3XM-6, and DS3XM-12 cards. It does not utilize the DS3XM card FEAC loopback functions. For this information, refer to the "1.3 Troubleshooting DS3XM-6 or DS3XM-12 Card Electrical Paths With FEAC Loopbacks" section on page 1-46.

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

Use appropriate cabling to attach the Tx and Rx terminals of the electrical test set to the EIA connectors or DSx panel for 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 For any of these cards, click the **Maintenance > DS3** tabs.

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

Step 4 For the DS3 tab, choose **OOS,MT** from the Admin State column for the port being tested. If this is a multiport card, select the appropriate row for the port being tested. For the DS1 tab, no state selection is necessary unless the DS-1 has been placed in service. The loopback/send code cannot be selected for a DS-1 if the derived state is OOS,DSBLD.

Step 5 Choose **Facility (Line)** from the Loopback Type column for the port being tested. If this is a multiport card, select the appropriate row for the port being tested.

Step 6 Click **Apply**.

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

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

Step 8 Complete the "Test and Clear the DS3E or DS3XM Port Facility Loopback Circuit" procedure on page 1-30.

Test and Clear the DS3E or DS3XM Port Facility Loopback Circuit

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

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

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

Step 4 For any of these cards, click the **Maintenance > DS3** tabs.

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

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

Step 6 Choose the appropriate state (**IS**; **OOS,DSBLD**; **OOS,MT**; **IS,AINS**) from the Admin State column for the port being tested.

Step 7 Click **Apply**.

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

Step 9 Complete the "Test the Electrical Cabling" procedure on page 1-31.

Test the Electrical Cabling

Step 1 Replace the suspected bad cabling (from the test set to the DSx panel or the EIA ports) with known-good cable. For instructions, refer to the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15454 Procedure Guide*.

If a known-good cable is not available, test the suspected bad cable with a test set. (Refer to manufacturer instructions for test-set use.) Remove the suspected bad cable from the DSx panel or the EIA and connect the cable to the Tx and Rx terminals of the test set. Run traffic to determine whether the cable is good or defective.

Step 2 Resend test traffic on the loopback circuit with a known-good cable installed. If the test set indicates a good circuit, the problem was probably the defective cable.

Step 3 Replace the defective cable.

Step 4 In card view for the electrical card, depending upon the type, click the **Maintenance > Loopback** tab, **Maintenance > DS1** tab, or **Maintenance > DS3** tab.

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

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

Step 6 Choose the appropriate state (**IS**; **OOS,DSBLD**; **OOS,MT**; **IS,AINS**) from the Admin State column for the port being tested.

Step 7 Click **Apply**.

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

Step 9 Complete the "Test the Electrical Card" procedure on page 1-31.

Test the Electrical Card

Step 1 Complete the "Physically Replace a Traffic Card" procedure on page 2-243 for the suspected bad card and replace it with a known-good one.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Refer to the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-231 for basic procedures. For more information, refer to the "Maintain the Node" chapter in the *Cisco ONS 15454 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 "Physically Replace a Traffic Card" procedure on page 2-243 for the faulty card.

Step 5 In card view for the electrical card, depending upon the type, click the **Maintenance > Loopback** tab, **Maintenance > DS1** tab, or **Maintenance > DS3** tab.

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

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

Step 7 Choose the appropriate state (**IS**; **OOS,DSBLD**; **OOS,MT**; **IS,AINS**) from the Admin State column for the port being tested.

Step 8 Click **Apply**.

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

Step 10 Complete the "Test the EIA" procedure on page 1-32.

Test the EIA

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

- **a.** Remove the lower backplane cover. Loosen the five screws that secure it to the ONS 15454 and pull it away from the shelf assembly.
- **b.** Loosen the nine perimeter screws that hold the EIA panel in place.
- **c.** Lift the EIA panel by the bottom to remove it from the shelf assembly.
- **d.** Follow the installation procedure for the appropriate EIA. Refer to the "Install the Shelf and Backplane Cable" chapter in the *Cisco ONS 15454 Procedure Guide* for instructions.

Step 2 Resend test traffic on the loopback circuit with known-good cabling, a known-good card, and the reinstalled EIA. If the test set indicates a good circuit, the problem was probably an improperly seated EIA, and you can proceed to Step 16. If the problem persists and the EIA is not shown to be improperly seated, proceed to Step 3.

Step 3 In card view for the electrical card, depending upon the type, click the **Maintenance > Loopback** tab, **Maintenance > DS1** tab, or **Maintenance > DS3** tab.

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

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

Step 5 Choose the appropriate state (**IS**; **OOS,DSBLD**; **OOS,MT**; **IS,AINS**) from the Admin State column for the port being tested.

Step 6 Click **Apply**.

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

Step 8 If the test set indicates a faulty circuit, the problem is probably a defective EIA. Return the defective EIA to Cisco through the RMA process. Contact Cisco Technical Support (1 800 553-2447).

Step 9 Replace the faulty EIA. Complete the "Replace the Electrical Interface Assembly" procedure on page 2-250.

Step 10 Resend test traffic on the loopback circuit with known-good cabling, a known-good card, and the replacement EIA. If the test set indicates a faulty circuit, repeat all of the facility loopback procedures.

Step 11 If the test set indicates a good circuit, the problem was probably the defective EIA. Clear the facility (line) loopback by clicking the **Maintenance > Loopback** tab, **Maintenance > DS1** tab, or **Maintenance > DS3** tab.

Step 12 Choose **None** from the Loopback Type column for the port being tested.

Step 13 Choose the appropriate state (**IS**; **OOS,DSBLD**; **OOS,MT**; **IS,AINS**) from the Admin State column for the port being tested.

Step 14 Click **Apply**.

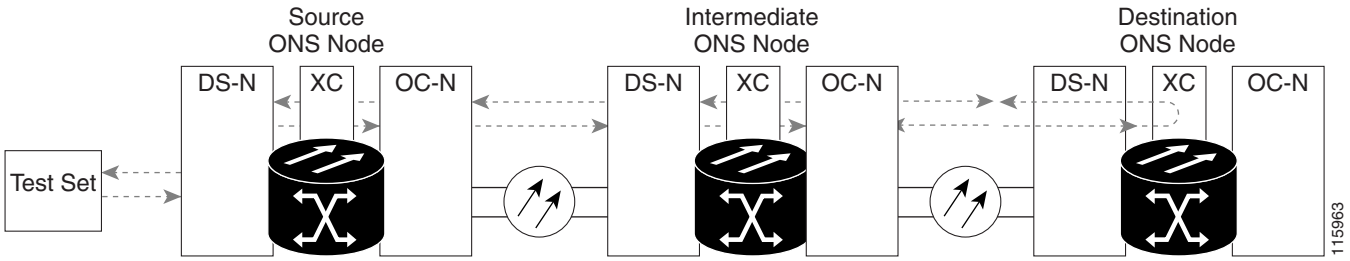
Step 15 Click **Yes** in the confirmation dialog box.

Step 16 Complete the "1.2.6 Perform a Hairpin Test on a Destination-Node Electrical Port (East to West)" procedure on page 1-33.

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

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

Figure 1-16 Hairpin on a Destination-Node DS-N Port



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

Note Hairpin loopbacks require on-site personnel.

Complete the "Create the Hairpin Circuit on the Destination-Node Port" procedure on page 1-34.

Create the Hairpin Circuit on the Destination-Node Port

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

- **a.** If you just completed the "1.2.5 Perform a Facility (Line) Loopback on a Destination-Node Electrical Port (East to West)" procedure on page 1-28, leave the electrical test set hooked up to the electrical port in the destination node.
- **b.** If you are starting the current procedure without the electrical test set hooked up to the electrical port, use appropriate cabling to attach the Tx and Rx terminals of the electrical test set to the DSx panel or the EIA connectors for 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 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 STS, and number, such as 1.
- **c.** Click **Next**.
- **d.** In the next Circuit Creation dialog box, give the circuit an easily identifiable name such as Hairpin1.
- **e.** Choose the Size, such as STS-1.
- **f.** Uncheck the **Bidirectional** check box. Leave the default values for State, SD Threshold, and SF Threshold.
- **g.** Click **Next**.
- **h.** In the Circuit Creation source dialog box, select the same Node, card Slot, Port, and STS (or VT) where the test set is connected. Leave Use Secondary Source unchecked.
- **i.** Click **Next**.
- **j.** In the Circuit Creation destination dialog box, use the same Node, card Slot, Port, and STS (or VT) used for the source dialog box. Leave Use Secondary Destination unchecked.
- **k.** Click **Next**.
- **l.** 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 and that the Dir column describes it as a one-way circuit.

Step 5 Complete the "Test and Delete the Electrical Hairpin Circuit" procedure on page 1-34.

Test and Delete the Electrical Hairpin Circuit

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

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

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

- **a.** Click the **Circuits** tab.
- **b.** Choose the hairpin circuit being tested.

c. Click **Delete**.

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

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

Step 4 Complete the "Test the Standby Cross-Connect Card" procedure on page 1-35.

Test the Standby Cross-Connect Card

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

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

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

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

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

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

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

Caution Cross-connect side switches, with the exception of side switches using XC-VXC-10G cards, are service-affecting. Any live traffic on any card in the node endures a hit of up to 50 ms. XC-VXC-10G side switches are errorless.

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

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

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

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

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

Step 3 Resend test traffic on the loopback circuit.

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

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

a. Click the **Circuits** tab.

b. Choose the hairpin circuit being tested.

c. Click **Delete**.

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

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

Step 5 To confirm a defective original cross-connect card, complete the "Retest the Original Cross-Connect Card" procedure on page 1-36.

Retest the Original Cross-Connect Card

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

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

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

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

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

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

Step 2 Resend test traffic on the loopback circuit.

Step 3 If the test set indicates a faulty circuit, the problem is probably the defective card. Return the defective card to Cisco through the RMA process. Contact Cisco Technical Support (1 800 553-2447) and proceed to Step 4. If the test does not indicate a faulty circuit, proceed to Step 5.

Step 4 Complete the "Physically Replace an In-Service Cross-Connect Card" procedure on page 2-243 for the defective cross-connect card.

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 hairpin circuit:

a. Click the **Circuits** tab.

b. Choose the hairpin circuit being tested.

c. Click **Delete**.

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

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

Step 6 Complete the "1.2.7 Perform an XC Loopback on a Source-Node OC-N STS (East to West) Carrying an Electrical Circuit" procedure on page 1-37.

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

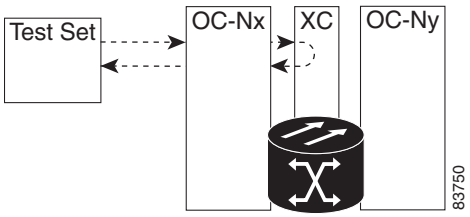
The XC loopback tests whether any problem exists on the circuit's OC-N span, isolating this span from others present on the card. It also eliminates the cross-connect card as the source of trouble for a faulty circuit. The loopback occurs on the cross-connect card in a network circuit. Figure 1-17 shows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

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

Note XC loopbacks do not require on-site personnel.

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

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



Complete the "Create the XC Loopback on the Source OC-N Port Carrying an Electrical Circuit" procedure on page 1-37.

Create the XC Loopback on the Source OC-N Port Carrying an Electrical Circuit

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

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

a. If you just completed the "1.2.6 Perform a Hairpin Test on a Destination-Node Electrical Port (East to West)" section on page 1-33, 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 **OOS,MT** 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 OC-N card to display the card view.
b. Click the **Maintenance > Loopback > SONET STS** tab.
c. Check the **XC Loopback** column check box for the port being tested.
d. Click **Apply**.
e. Click **Yes** in the confirmation dialog box.

Step 5 Complete the "Test and Clear the XC Loopback Circuit" procedure on page 1-38.

Test and Clear the XC Loopback Circuit

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

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

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

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

a. In card view, click the **Maintenance > Loopback > SONET STS** tab.
b. Uncheck the check box in the **XC Loopback** column for the circuit being tested.
c. Click **Apply**.
d. Click **Yes** in the confirmation dialog box.

Step 4 Complete the "Test the Standby Cross-Connect Card" procedure on page 1-38.

Test the Standby Cross-Connect Card

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

a. Determine the standby cross-connect card. On both the physical node and the CTC node view window, the standby cross-connect ACT/SBY LED is amber and the active card ACT/SBY LED is green.
b. Position the cursor over the standby cross-connect card.
c. Right-click and choose **RESET CARD**.

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

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

Caution Cross-connect side switches, with the exception of side switches using XC-VXC-10G cards, are service-affecting. Any live traffic on any card in the node endures a hit of up to 50 ms. XC-VXC-10G side switches are errorless.

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

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

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

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

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

Step 3 Resend test traffic on the loopback circuit.

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

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

a. Click the **Circuits** tab.

b. Choose the XC loopback circuit being tested.

c. Click **Delete**.

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

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

Step 5 To confirm a defective original cross-connect card, complete the "Retest the Original Cross-Connect Card" procedure on page 1-39.

Retest the Original Cross-Connect Card

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

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

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

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

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

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

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

Step 2 Resend test traffic on the loopback circuit.

Step 3 If the test set indicates a faulty circuit, the problem is probably the defective card. Return the defective card to Cisco through the RMA process. 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 "Physically Replace an In-Service Cross-Connect Card" procedure on page 2-243 for the defective cross-connect 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**.

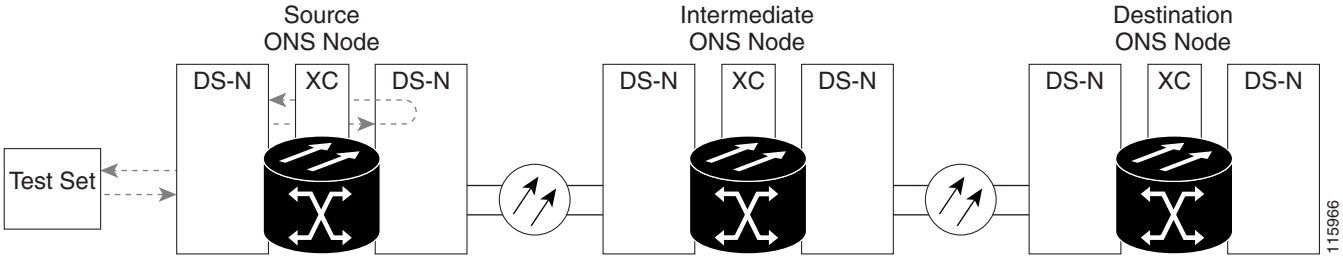
d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

e. If the problem is not resolved, go to the "1.2.8 Perform a Terminal (Inward) Loopback on a Source-Node Electrical Port (East to West)" section on page 1-40.

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

The terminal (inward) loopback test is performed on the source-node electrical port in the circuit, such as a source-node electrical port. You first create a bidirectional circuit that starts on the destination-node electrical port and loops back on the source-node electrical port. Then you proceed with the terminal loopback test. Completing a successful terminal loopback to a source-node electrical port verifies that the circuit is good to the source electrical port. Figure 1-18 shows an example of a terminal loopback on a source DS-N port.

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



Caution Performing a loopback on an in-service circuit is service-affecting. To protect traffic, apply a lockout or Force switch to the target loopback port. Refer to the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-231 for basic instructions. For more information about these operations, refer to the "Maintain the Node" chapter in the *Cisco ONS 15454 Procedure Guide*.

Note Terminal loopbacks require on-site personnel.

Note ONS 15454 DS-3 terminal (inward) loopbacks do not transmit an AIS in the direction away from the loopback. Instead of AIS, a continuance of the signal transmitted into the loopback is provided. A DS3/EC1-48 card can be provisioned to transmit AIS for a terminal loopback if desired.

Depending upon your card type, complete the "Create the Terminal (Inward) Loopback on a Source DS-1, DS-3, DS3N-12, DS3i-N-12, or EC1 Port" procedure on page 1-41 or the "Create the Terminal (Inward) Loopback on a Source DS3E or DS3XM Port" procedure on page 1-43. Then test and clear the loopback as instructed.

Create the Terminal (Inward) Loopback on a Source DS-1, DS-3, DS3N-12, DS3i-N-12, or EC1 Port

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

- **a.** If you just completed the "1.2.7 Perform an XC Loopback on a Source-Node OC-N STS (East to West) Carrying an Electrical Circuit" procedure on page 1-37, leave the electrical test set hooked up to the DS-N port in the source node.
- **b.** If you are starting the current procedure without the electrical test set hooked up to the DS-N port, use appropriate cabling to attach the Tx and Rx terminals of the electrical test set to the DSx panel or the EIA connectors for the port you are testing. Both Tx and Rx connect to the same port.

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

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

Step 4 In the Circuit Creation dialog box, choose the type, such as STS, and number, such as 1.

Step 5 Click **Next**.

Step 6 In the next Circuit Creation dialog box, give the circuit an easily identifiable name such as DS1toDS4.

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

Step 8 Click **Next**.

Step 9 In the Circuit Creation source dialog box, select the **Node**, card **Slot**, **Port**, and **STS** (or **VT**) where the test set is connected.

Step 10 Click **Next**.

Step 11 In the Circuit Creation destination dialog box, use the same Node, card Slot, Port, and STS (or VT) used for the source dialog box.

c. Click **Next**.

d. In the Circuit Creation circuit routing preferences dialog box, leave all defaults. Click **Finish**.

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

Note It is normal for the "LPBKTERMINAL (DS1, DS3)" condition on page 2-157 to appear during a loopback setup. The condition clears when you remove the loopback.

Note ONS 15454 DS-3 terminal (inward) loopbacks do not transmit an AIS in the direction away from the loopback. Instead of AIS, a continuance of the signal transmitted into the loopback is provided. A DS3/EC1-48 card can be provisioned to transmit AIS for a terminal loopback if desired.

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

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

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

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

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

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

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

f. Click **Apply**.

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

Step 14 Complete the "Test and Clear the DS-3, DS3N-12, DS3i-N-12, or EC1 Port Terminal Loopback" procedure on page 1-42.

Test and Clear the DS-3, DS3N-12, DS3i-N-12, or EC1 Port Terminal Loopback

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

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

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

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

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

Step 6 Select the appropriate state (**IS**; **OOS,DSBLD**; **OOS,MT**; **IS,AINS**) in the Admin State column for the port being tested.

Step 7 Click **Apply**.

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

Step 9 Clear the terminal loopback:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

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

Step 10 Complete the "Test the Source Electrical Card" procedure on page 1-45.

Create the Terminal (Inward) Loopback on a Source DS3E or DS3XM Port

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

a. If you just completed the "1.2.7 Perform an XC Loopback on a Source-Node OC-N STS (East to West) Carrying an Electrical Circuit" procedure on page 1-37, leave the electrical test set hooked up to the DS-N port in the source node.

b. If you are starting the current procedure without the electrical test set hooked up to the DS-N port, use appropriate cabling to attach the Tx and Rx terminals of the electrical test set to the DSx panel or the EIA connectors for 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 In CTC node view, click the **Circuits** tab and click **Create**.

Step 3 In the Circuit Creation dialog box, choose the type, such as STS, and number, such as 1.

Step 4 Click **Next**.

Step 5 In the next Circuit Creation dialog box, give the circuit an easily identifiable name such as DS1toDS5.

Step 6 Leave the **Bidirectional** check box checked.

Step 7 Click **Next**.

Step 8 In the Circuit Creation source dialog box, select the **Node**, card **Slot**, **Port**, and **STS** (or **VT**) where the test set is connected.

Step 9 Click **Next**.

Step 10 In the Circuit Creation destination dialog box, use the same Node, card Slot, Port, and STS (or VT) used for the source dialog box.

d. Click **Next**.

e. In the Circuit Creation circuit routing preferences dialog box, leave all defaults. Click **Finish**.

Step 11 Confirm that the newly created circuit appears in the Dir column as a two-way circuit.

Note It is normal for the "LPBKTERMINAL (DS1, DS3)" condition on page 2-157 to appear during a loopback setup. The condition clears when you remove the loopback.

Note ONS 15454 DS-3 terminal (inward) loopbacks do not transmit an AIS in the direction away from the loopback. Instead of AIS, a continuance of the signal transmitted into the loopback is provided. A DS3/EC1-48 card can be provisioned to transmit AIS for a terminal loopback if desired.

Step 12 Create the terminal (inward) loopback on the destination port being tested:

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

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

c. Click the **Maintenance > DS3** tabs.

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

Step 13 For the DS3 tab, choose **OOS,MT** from the Admin State column for the port being tested. If this is a multiport card, select the appropriate row for the port being tested. For the DS1 tab, no state selection is necessary unless the DS-1 has been placed in service. The loopback/send code cannot be selected for a DS-1 if the derived state is OOS,DSBLD.

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

e. Click **Apply**.

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

Step 14 Complete the "Test and Clear the DS3E or DS3XM Port Terminal Loopback Circuit" procedure on page 1-44.

Test and Clear the DS3E or DS3XM Port Terminal Loopback Circuit

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

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

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

Step 4 Depending upon the card type, click the **Maintenance > Loopback** tab, **Maintenance > DS1** tab, or **Maintenance > DS3** tab.

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

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

Step 6 Select the appropriate state (**IS**; **OOS,DSBLD**; **OOS,MT**; **IS,AINS**) in the Admin State column for the port being tested.

Step 7 Click **Apply**.

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

Step 9 Clear the terminal loopback:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

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

Step 10 Complete the "Test the Source Electrical Card" procedure on page 1-45.

Test the Source Electrical Card

Step 1 Complete the "Physically Replace a Traffic Card" procedure on page 2-243 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 (1 800 553-2447).

Step 4 Complete the "Physically Replace a Traffic Card" procedure on page 2-243 for the defective electrical card.

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

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

b. Depending upon the card type, click the **Maintenance > Loopback** tab, **Maintenance > DS1** tab, or **Maintenance > DS3** tab.

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

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

d. Select the appropriate state (**IS**; **OOS,DSBLD**; **OOS,MT**; **IS,AINS**) in the Admin State column for the port being tested.

e. Click **Apply**.

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

Step 6 Delete the terminal (inward) loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

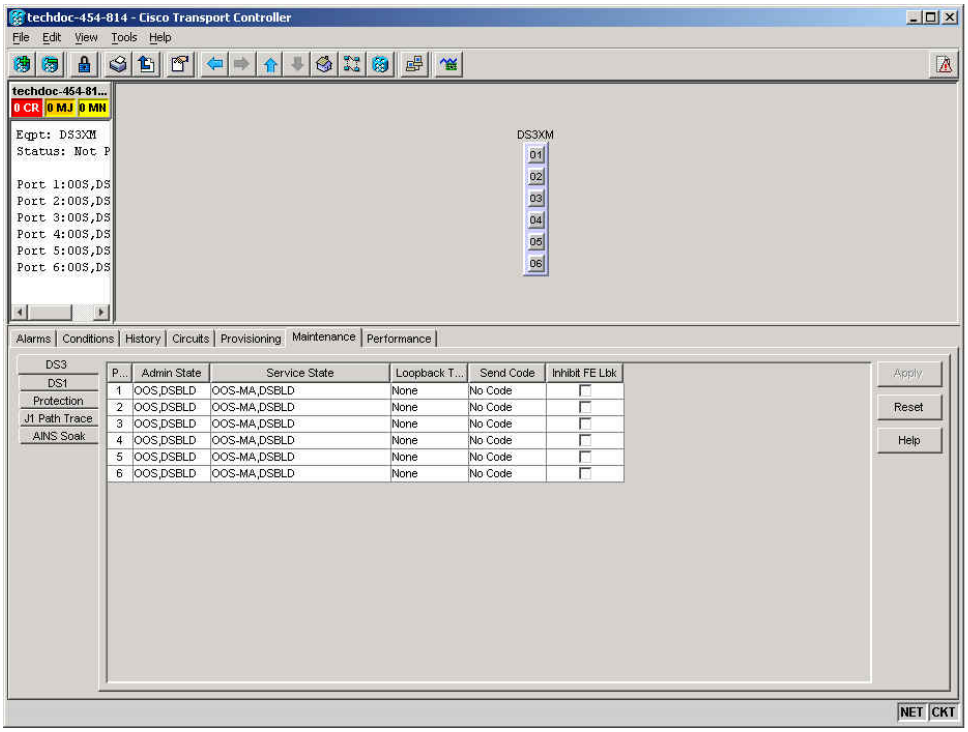
c. Click **Delete**.

All tests for this circuit are completed.

1.3 Troubleshooting DS3XM-6 or DS3XM-12 Card Electrical Paths With FEAC Loopbacks

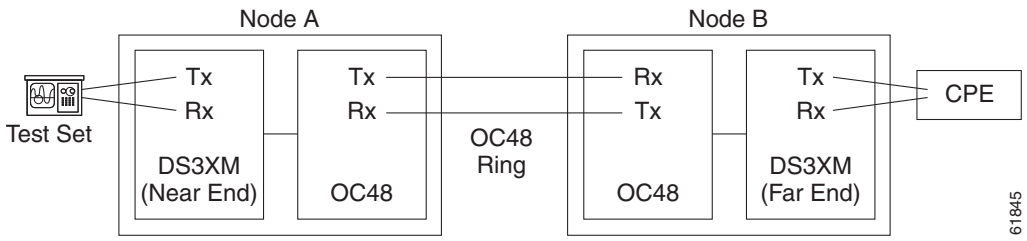
The DS3XM-6 card, DS3XM-12 card and DS3-EC1-48 cards support far-end alarm and control(FEAC) functions that are not available on basic DS-3 cards. Click the DS3XM-6 or DS3XM-12 **Maintenance > DS3** tab at the card view to reveal the two additional function columns. Figure 1-19 shows the DS3 subtab and the additional Send Code and Inhibit FE Lbk function columns.

Figure 1-19 Accessing FEAC Functions on the DS3XM-6 Card



The “far end” in FEAC refers to the equipment connected to the DS3XM card and not to the far end of a circuit. In Figure 1-20, if a DS3XM-6/DS3XM-12/DS3-EC1-48 (near-end) port is configured to send a line loop code, the code will be sent to the connected test set, not the DS3XM-6/DS3XM-12/DS3-EC1-48 (far-end) port. FEAC functions will be available only when the DS3 port is configured in CBIT Framing.

Figure 1-20 Diagram of FEAC Circuit



1.3.1 FEAC Send Code

The Send Code column on the DS3XM-6 or DS3XM-12 or DS3-EC1-48 card Maintenance tab only applies to OOS-MA,MT ports configured for CBIT framing. The column lets a user select No Code (the default) or line loop code. Selecting line loop code inserts a line loop activate FEAC in the CBIT overhead transmitting to the connected facility (line). This code initiates a loopback from the facility to the ONS 15454. Selecting No Code sends a line-loop-deactivate FEAC code to the connected equipment, which will remove the loopback. You can also insert a FEAC for the 28 individual DS-1 circuits transmuxed into a DS-3 circuit.

1.3.2 DS-3E and DS3i-N-12 Inhibit Loopback

DS-3E and DS-3i-N-12 cards respond to (but do not send) DS-3-level FEAC codes. You can inhibit FEAC response on ports for these cards using the Inhibit Lbk check box on their Maintenance windows.

1.3.3 DS3XM-6, DS3XM-12 and DS3-EC1-48 Inhibit FEAC Loopback

DS3XM-6 and DS3XM-12 ports and transmuxed DS-1 circuits initiate loopbacks when they receive FEAC line loop codes. If the Inhibit FE Lbk check box is checked for a DS-3 port, that port ignores any FEAC line loop codes it receives and will not loop back (return them). In DS3XM-6 and DS3XM-12 Cards, only DS-3 ports can be configured to inhibit FEAC loopback responses; individual DS-1 ports (accessed on the DS3XM DS1 tab) cannot inhibit their responses. If you inhibit a DS-3 port's far end loopback response, this DS-3 port and the DS-1 lines it contains are not restricted from terminal (inward) or facility (line) loopbacks.

1.3.4 FEAC Alarms

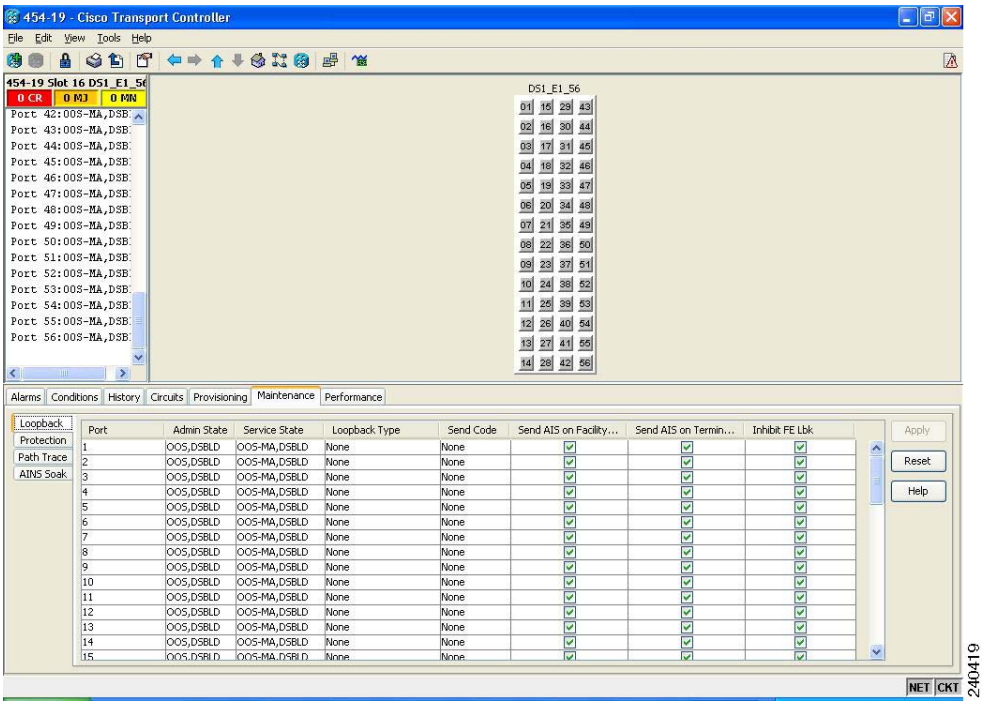
When an ONS 15454 port receives an activation code for a FEAC loopback, it raises the "LPBKDS1FEAC-CMD" condition on page 2-150 or the "LPBKDS3FEAC" condition on page 2-151. The condition clears when the port receives the command to deactivate the FEAC loopback. If a node sends a FEAC loopback command to the far end, the sending node raises a "LPBKDS1FEAC-CMD" condition on page 2-150 or the "LPBKDS3FEAC-CMD" condition on page 2-151 for the near-end port.

1.4 Troubleshooting DS1-E1-56 Card with Far End Loopcodes

DS1-E1-56 Card supports Far End Loopcodes when the DS1 port is operating in ESF Framing mode. Click the DS1-E1-56 **Maintenance->DS1** tab to reveal additional columns, namely , "Inhibit FE Lbk" and "Send Code". Here we use the term FE Loopcodes instead of FEAC in DS1, as DS1 supports only Far End Loopcodes, and NOT Alarms.

Note The term "Far End" refers to the equipment connected to the DS1_E1-56 card and not to the far end of a circuit.

Figure 1-21 Accessing Far End troubleshooting Functions on the DS1-E1-56 Card



1.4.1 Far End Send Code

The Send Code column on the DS1-E1-56 card Maintenance tab only applies to OOS-MA, MT ports configured for ESF framing. The column allows the user to select No Code (the default) or line loop code. Selecting line loop code inserts a line loop activate Far End Loopcode in the ESF overhead transmitting to the connected facility. This code initiates a loopback from the facility to the ONS 15454. Selecting No Code sends a line-loop-deactivate Far End Loopcode to the connected equipment, which will remove the loopback.

1.4.2 DS1-E1-56 Inhibit Far End Loopback

DS1-E1-56 ports and transmuxed DS1 circuits initiate loopbacks when they receive Far End line loop codes. If the Inhibit FE Lbk check box is checked for a DS1 port, that port ignores any Far End line loop codes it receives and will not loop back. If you inhibit a DS1 port's far end loopback response, this DS1 port is not restricted from terminal or facility loopbacks.

1.5 Troubleshooting Optical Circuit Paths With Loopbacks

Facility (line) loopbacks, terminal (inward) loopbacks, and cross-connect loopback circuits are often used together to test the circuit path through the network or to logically isolate a fault. Performing a loopback test at each point along the circuit path systematically isolates possible points of failure.

The procedures in this section apply to OC-N cards. (For instructions on G-Series Ethernet cards, go to the "1.6 Troubleshooting Ethernet Circuit Paths With Loopbacks" section on page 1-71. For information about troubleshooting MXP and TXP cards, go to the "1.7 Troubleshooting MXP, TXP, or FC_MR-4 Circuit Paths With Loopbacks" section on page 1-90.) The example in this section tests an OC-N circuit on a three-node BLSR. Using a series of facility, cross-connect, and terminal (inward) loopbacks, the example scenario traces the circuit path, tests the possible failure points, and eliminates them. The logical progression contains seven network test procedures:

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

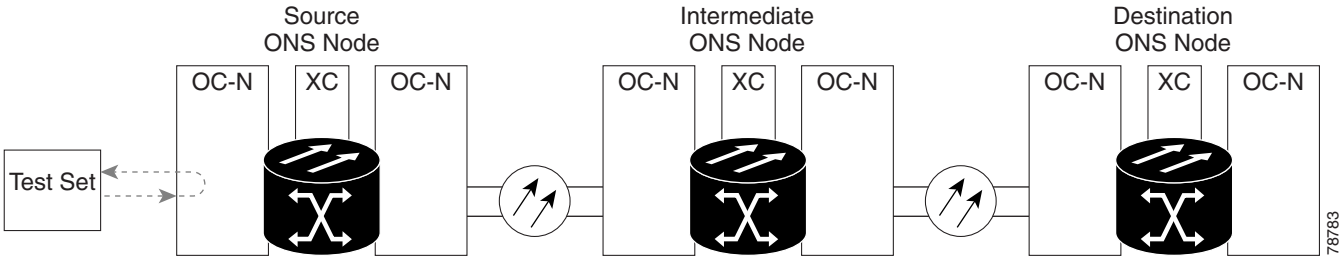
1. A facility (line) loopback on the source-node OC-N port
2. A terminal (inward) loopback on the source-node OC-N port
3. A cross-connect loopback on the source OC-N port
4. A facility (line) loopback on the intermediate-node OC-N port
5. A terminal (inward) loopback on the intermediate-node OC-N port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

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

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

The facility (line) loopback test is performed on the node source port in the network circuit. In the testing situation used in this example, the source OC-N port in the source node. Completing a successful facility (line) loopback on this port isolates the OC-N port as a possible failure point. Figure 1-22 shows an example of a facility loopback on a circuit source OC-N port.

Figure 1-22 Facility (Line) Loopback on a Circuit Source OC-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 (Line) Loopback on the Source Optical Port" procedure on page 1-50.

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

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

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

Use appropriate cabling to attach the 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. 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 Click the **Maintenance > Loopback > Port** tab.

Step 4 Choose **OOS,MT** from the Admin State column for the port being tested. If this is a multiport card, select the appropriate row for the desired port.

Step 5 Choose **Facility (Line)** from the Loopback Type column for the port being tested. If this is a multiport card, select the appropriate row for the desired port.

Step 6 Click **Apply**.

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

Note It is normal for the "LPBKFACILITY (OCN)" condition on page 2-155 or the "LPBKFACILITY (G1000)" condition on page 2-155 to appear during loopback setup. The condition clears when you remove the loopback.

Step 8 Complete the "Test and Clear the Facility (Line) Loopback Circuit" procedure on page 1-50.

Test and Clear the Facility (Line) Loopback Circuit

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

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

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

- **a.** Click the **Maintenance > Loopback > Port** tab.
- **b.** Choose **None** from the Loopback Type column for the port being tested.
- **c.** Choose the appropriate state (**IS**; **OOS,DSBLD**; **OOS,MT**; **IS,AINS**) 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 OC-N Card" procedure on page 1-51.

Test the OC-N Card

Step 1 Complete the "Physically Replace a Traffic Card" procedure on page 2-243 for the suspected bad card and replace it with a known-good one.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Refer to the procedures in the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-231. For more information, refer to the "Maintain the Node" chapter in the *Cisco ONS 15454 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 "Physically Replace a Traffic Card" procedure on page 2-243 for the faulty card.

Step 5 Clear the facility (line) loopback:

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

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

c. Choose the appropriate state (**IS**; **OOS,DSBLD**; **OOS,MT**; **IS,AINS**) from the Admin State column for the port being tested.

d. Click **Apply**.

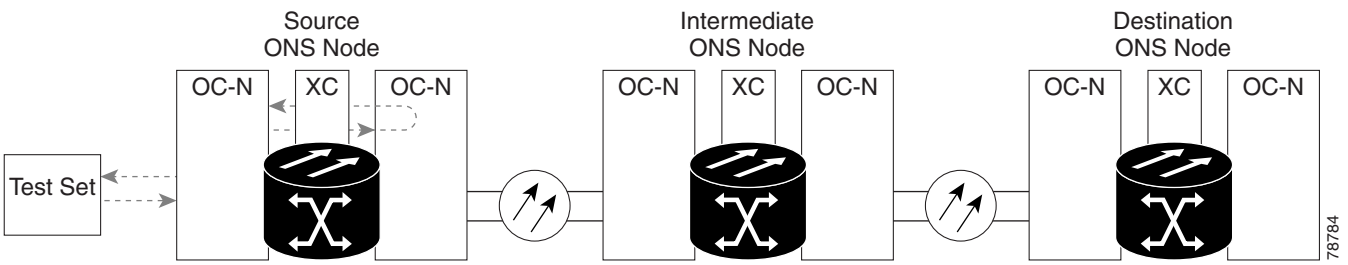
e. Click **Yes** in the confirmation dialog box.

Step 6 Complete the "1.5.2 Perform a Terminal (Inward) Loopback on a Source-Node Optical Port" procedure on page 1-51.

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

The terminal (inward) loopback test is performed on the source-node optical port. For the circuit in this example, it is the source OC-N port in the source node. You first create a bidirectional circuit that starts on the node destination optical port and loops 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 1-23 shows an example of a terminal loopback on a source OC-N port.

Figure 1-23 Terminal (Inward) Loopback on a Source-Node OC-N Port



OC-N cards placed in terminal loopback state display an icon in the CTC graphical user interface (GUI), shown in Figure 1-24.

Figure 1-24 Terminal Loopback Indicator

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

Note Terminal loopbacks require on-site personnel.

Complete the "Create the Terminal (Inward) Loopback on a Source-Node Optical Port" procedure on page 1-52.

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

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

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

a. If you just completed the "1.5.1 Perform a Facility (Line) Loopback on a Source-Node Optical Port" procedure on page 1-49, leave the optical test set hooked up to the OC-N port in the source node.

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

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

Step 2 Use CTC to set up the terminal (inward) loopback on the test port:

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

b. In the Circuit Creation dialog box, choose the type, such as STS, and number, such as 1.

c. Click **Next**.

d. In the next Circuit Creation dialog box, give the circuit an easily identifiable name such as OCN1toOCN2.

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 STS (or VT) 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 STS (or VT) 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 (OCN)" condition on page 2-160 to appear during a loopback setup. The condition clears when you remove the loopback.

Step 4 Create the terminal (inward) loopback on the destination port being tested:

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

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

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

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

e. Click **Apply**.

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

Step 5 Complete the "Test and Clear the Terminal Loopback Circuit" procedure on page 1-53.

Test and Clear the Terminal Loopback Circuit

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

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

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

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

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

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

d. Select the appropriate state (**IS**; **OOS,DSBLD**; **OOS,MT**; **IS,AINS**) in the Admin State column for the port being tested.

e. Click **Apply**.

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

Step 4 Clear the terminal loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

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

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

Test the Optical Card

Step 1 Complete the "Physically Replace a Traffic Card" procedure on page 2-243 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 (1 800 553-2447).

Step 4 Complete the "Physically Replace a Traffic Card" procedure on page 2-243 for the defective card.

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

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

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

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

d. Select the appropriate state (**IS**; **OOS,DSBLD**; **OOS,MT**; **IS,AINS**) in the Admin State column for the port being tested.

e. Click **Apply**.

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

Step 6 Clear the terminal loopback circuit before testing the next segment of the network circuit path:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

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

Step 7 Complete the "1.5.3 Perform an XC Loopback on the Source Optical Port" procedure on page 1-54.

1.5.3 Perform an XC Loopback on the Source Optical Port

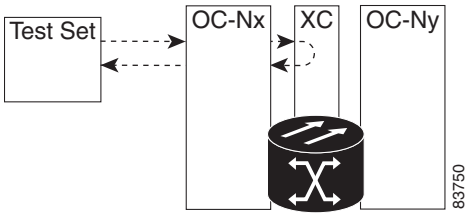
Note This procedure is only performed on OC-N cards and tests the cross-connect circuit connection.

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 occurs on the cross-connect card in a network circuit. Completing a successful XC loopback from an OC-N card through the cross-connect card eliminates the cross-connect card as the source of trouble for a faulty circuit. Figure 1-25 shows an example of an XC loopback path on a source OC-N port.

Figure 1-25 XC Loopback on a Source OC-N Port



Complete the "Create the XC Loopback on the Source-Node Optical Port" procedure on page 1-55.

Create the XC Loopback on the Source-Node Optical Port

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

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

a. If you just completed the "1.5.2 Perform a Terminal (Inward) Loopback on a Source-Node Optical Port" procedure on page 1-51, leave the optical test set hooked up to the source-node port.

b. If you are starting the current procedure without the optical test set hooked up to the source port, use appropriate cabling to attach the 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 **OOS,MT** 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 OC-N card to display the card view.

b. Click the **Maintenance > Loopback > SONET STS** tab.

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 1-56.

Test and Clear the XC Loopback Circuit

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

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

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

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

a. In card view, click the **Maintenance > Loopback > SONET STS** tab.

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

c. Click **Apply**.

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

Step 4 Complete the "Test the Standby Cross-Connect Card" procedure on page 1-56.

Test the Standby Cross-Connect Card

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

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

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

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

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

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

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

Caution Cross-connect side switches, with the exception of side switches using XC-VXC-10G cards, are service-affecting. Any live traffic on any card in the node endures a hit of up to 50 ms. XC-VXC-10G side switches are errorless.

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

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

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

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

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

Step 3 Resend test traffic on the loopback circuit.

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

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

a. Click the **Circuits** tab.

b. Choose the XC loopback circuit being tested.

c. Click **Delete**.

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

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

Step 5 To confirm a defective original cross-connect card, complete the "Retest the Original Cross-Connect Card" procedure on page 1-57.

Retest the Original Cross-Connect Card

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

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

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

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

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

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

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

Step 2 Resend test traffic on the loopback circuit.

Step 3 If the test set indicates a faulty circuit, the problem is probably the defective card. Return the defective card to Cisco through the RMA process. 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 "Physically Replace an In-Service Cross-Connect Card" procedure on page 2-243 for the defective card.

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**.

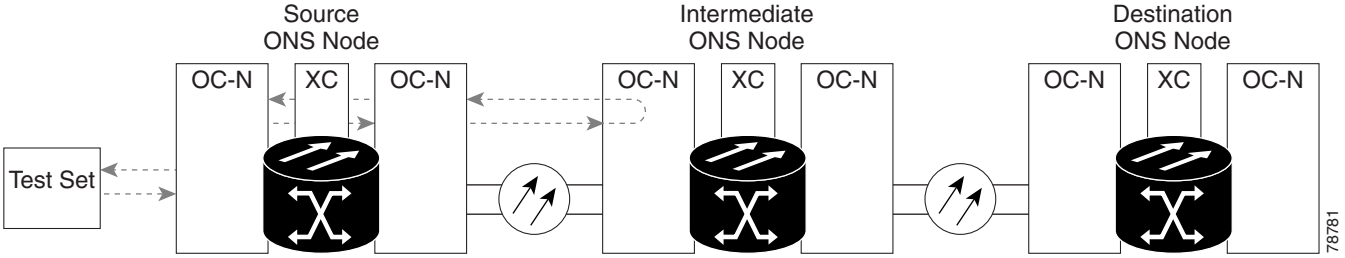
d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

Step 6 Complete the "1.5.4 Perform a Facility (Line) Loopback on an Intermediate-Node Optical Port" procedure on page 1-58.

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

Performing the facility (line) loopback test on an intermediate port isolates whether this node is causing circuit failure. In the situation shown in Figure 1-26, the test is being performed on an intermediate OC-N port.

Figure 1-26 Facility (Line) Loopback Path to an Intermediate-Node OC-N 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 (Line) Loopback on an Intermediate-Node Optical Port" procedure on page 1-58.

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

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

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

a. If you just completed the "1.5.3 Perform an XC Loopback on the Source Optical Port" procedure on page 1-54, leave the optical test set hooked up to the source-node port.

b. If you are starting the current procedure without the optical test set hooked up to the source port 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 facility (line) loopback on the test port:

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

b. In the Circuit Creation dialog box, choose the type, such as STS, and number, such as 1.

c. Click **Next**.

d. In the next Circuit Creation dialog box, give the circuit an easily identifiable name such as OCN1toOCN3.

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 STS (or VT) 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 STS (or VT) 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 (OCN)" condition on page 2-155 to appear during a loopback setup. The condition clears when you remove the loopback.

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

a. Go to the node view of the 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** tab.

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

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

f. Click **Apply**.

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

Step 6 Complete the "Test and Clear the Facility (Line) Loopback Circuit" procedure on page 1-60.

Test and Clear the Facility (Line) Loopback Circuit

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

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

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

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

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

c. Choose the appropriate state (**IS**; **OOS,DSBLD**; **OOS,MT**; **IS,AINS**) from the Admin State column for the port being tested.

d. Click **Apply**.

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

Step 4 Clear the facility (line) loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

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

Step 5 Complete the "Test the Optical Card" procedure on page 1-60.

Test the Optical Card

Step 1 Complete the "Physically Replace a Traffic Card" procedure on page 2-243 for the suspected bad card and replace it with a known-good one.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Refer to the procedures in the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-231. For more information, refer to the "Maintain the Node" chapter in the *Cisco ONS 15454 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 "Physically Replace a Traffic Card" procedure on page 2-243 for the faulty card.

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

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

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

c. Choose the appropriate state (**IS**; **OOS,DSBLD**; **OOS,MT**; **IS,AINS**) from the Admin State column for the port being tested.

d. Click **Apply**.

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

Step 6 Clear the facility loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

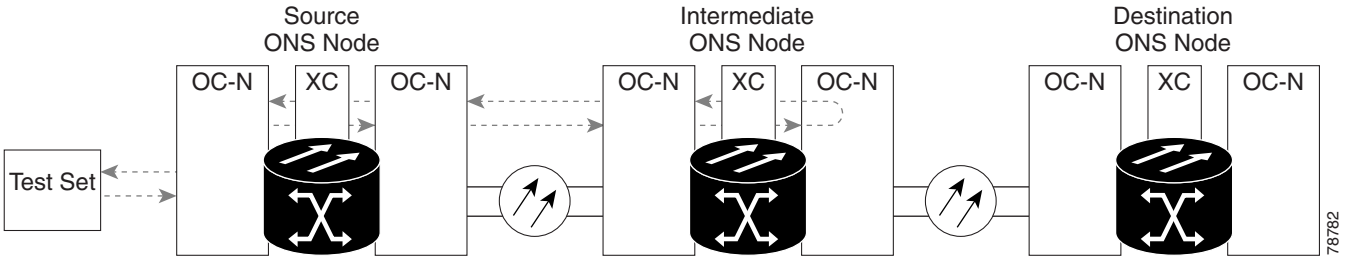
d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

Step 7 Complete the "1.5.5 Perform a Terminal (Inward) Loopback on Intermediate-Node Optical Ports" procedure on page 1-61.

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

In the next troubleshooting test, you perform a terminal loopback on the intermediate-node port to isolate whether the destination port is causing circuit trouble. In the example situation in Figure 1-27, 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 1-27 Terminal Loopback Path to an Intermediate-Node OC-N Port



OC-N cards placed in facility loopback state display an icon, shown in Figure 1-28.

Figure 1-28 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 1-62.

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 "1.5.4 Perform a Facility (Line) Loopback on an Intermediate-Node Optical Port" section on page 1-58, 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 (inward) loopback on the test port:

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

b. In the Circuit Creation dialog box, choose the type, such as STS, and number, such as 1.

c. Click **Next**.

d. In the next Circuit Creation dialog box, give the circuit an easily identifiable name such as OCN1toOCN4.

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 STS (or VT) 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 STS (or VT) 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 (OCN)" condition on page 2-160 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** tab.

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

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

f. Click **Apply**.

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

Step 6 Complete the "Test and Clear the Optical Terminal Loopback Circuit" procedure on page 1-63.

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 display the card view.

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

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

d. Select the appropriate state (**IS**; **OOS,DSBLD**; **OOS,MT**; **IS,AINS**) 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 1-64.

Test the Optical Card

Step 1 Complete the "Physically Replace a Traffic Card" procedure on page 2-243 for the suspected bad card and replace it with a known-good one.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Refer to the procedures in the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-231. For more information, refer to the "Maintain the Node" chapter in the *Cisco ONS 15454 Procedure Guide*.

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 (1 800 553-2447).

Step 4 Complete the "Physically Replace a Traffic Card" procedure on page 2-243 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** tab.

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

d. Select the appropriate state (**IS**; **OOS,DSBLD**; **OOS,MT**; **IS,AINS**) 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**.

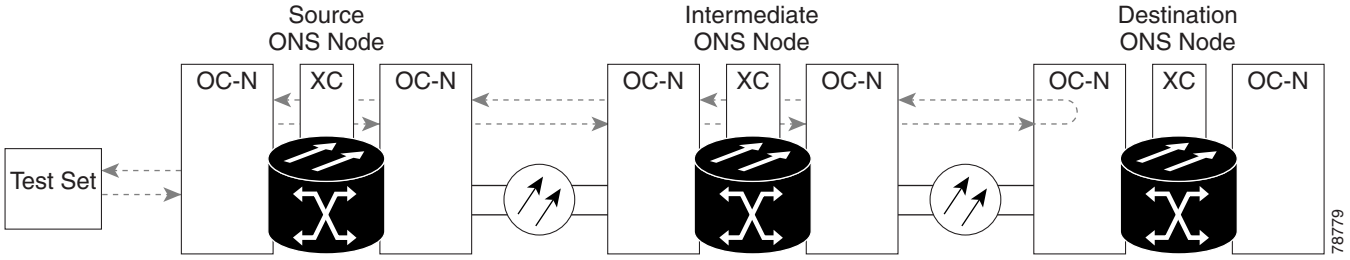
d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

Step 7 Complete the "1.5.6 Perform a Facility (Line) Loopback on a Destination-Node Optical Port" procedure on page 1-64.

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

You perform a facility (line) loopback test at the destination port to determine whether this local port is the source of circuit trouble. The example in Figure 1-29 shows a facility loopback being performed on a destination-node OC-N port.

Figure 1-29 Facility (Line) Loopback Path to a Destination-Node OC-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 (Line) Loopback on a Destination-Node Optical Port" procedure on page 1-65.

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

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

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

a. If you just completed the "1.5.5 Perform a Terminal (Inward) Loopback on Intermediate-Node Optical Ports" procedure on page 1-61, 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 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 STS, and number, such as 1.

c. Click **Next**.

d. In the next Circuit Creation dialog box, give the circuit an easily identifiable name such as OCN1toOCN5.

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 STS (or VT) 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 STS (or VT) 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 (OCN)" condition on page 2-155 to appear during a loopback setup. The condition clears when you remove the loopback.

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

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

- 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** tab.

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

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

f. Click **Apply**.

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

Step 6 Complete the "Test and Clear the Optical Facility (Line) Loopback Circuit" procedure on page 1-66.

Test and Clear the Optical Facility (Line) Loopback Circuit

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

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

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

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

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

c. Choose the appropriate state (**IS**; **OOS,DSBLD**; **OOS,MT**; **IS,AINS**) from the Admin State column for the port being tested.

d. Click **Apply**.

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

Step 4 Clear the facility (line) loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

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

Step 5 Complete the "Test the Optical Card" procedure on page 1-67.

Test the Optical Card

Step 1 Complete the "Physically Replace a Traffic Card" procedure on page 2-243 for the suspected bad card and replace it with a known-good one.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Refer to the procedures in the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-231. For more information, refer to the "Maintain the Node" chapter in the *Cisco ONS 15454 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 "Physically Replace a Traffic Card" procedure on page 2-243 for the faulty card.

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

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

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

c. Choose the appropriate state (**IS**; **OOS,DSBLD**; **OOS,MT**; **IS,AINS**) from the Admin State column for the port being tested.

d. Click **Apply**.

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

Step 6 Clear the facility loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

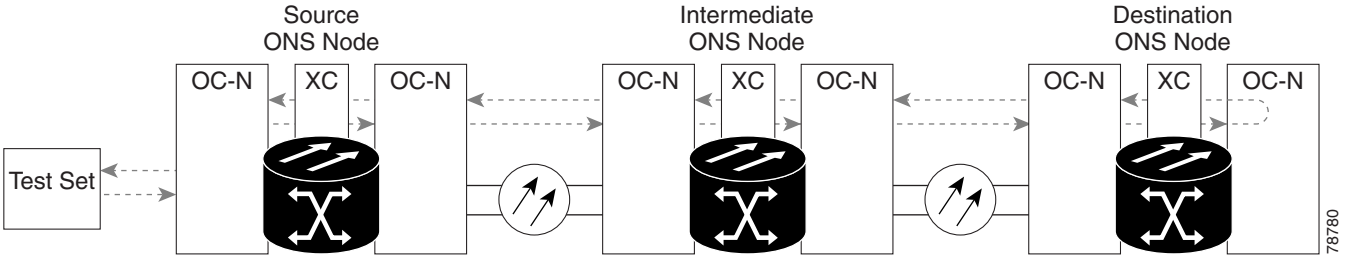
d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

Step 7 Complete the "1.5.7 Perform a Terminal Loopback on a Destination-Node Optical Port" procedure on page 1-67.

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

The terminal loopback at the destination-node port is the final local hardware error elimination in the circuit troubleshooting process. If this test is completed successfully, you have verified that the circuit is good up to the destination port. The example in Figure 1-30 shows a terminal loopback on an intermediate-node destination OC-N port.

Figure 1-30 Terminal Loopback Path to a Destination-Node OC-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 Destination-Node Optical Port" procedure on page 1-68.

Create the Terminal Loopback on a Destination-Node Optical Port

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

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

a. If you just completed the "1.5.6 Perform a Facility (Line) Loopback on a Destination-Node Optical Port" procedure on page 1-64, 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 STS, and number, such as 1.

c. Click **Next**.

d. In the next Circuit Creation dialog box, give the circuit an easily identifiable name such as OCN1toOCN6.

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 STS (or VT) 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 STS (or VT) 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 (OCN)" condition on page 2-160 to appear during a loopback setup. The condition clears when you remove the loopback.

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

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

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

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

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

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

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

f. Click **Apply**.

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

Step 6 Complete the "Test and Clear the Optical Terminal Loopback Circuit" procedure on page 1-69.

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.

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

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

d. Select the appropriate state (**IS**; **OOS,DSBLD**; **OOS,MT**; **IS,AINS**) 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 Optical Card" procedure on page 1-70.

Test the Optical Card

Step 1 Complete the "Physically Replace a Traffic Card" procedure on page 2-243 for the suspected bad card and replace it with a known-good 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. Refer to the procedures in the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-231. For more information, refer to the "Maintain the Node" chapter in the *Cisco ONS 15454 Procedure Guide*.

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 (1 800 553-2447).

Step 4 Complete the "Physically Replace a Traffic Card" procedure on page 2-243 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** tab.

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

d. Select the appropriate state (**IS**; **OOS,DSBLD**; **OOS,MT**; **IS,AINS**) in the Admin State column for the port being tested.

e. Click **Apply**.

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

Step 6 Clear the terminal loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

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

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

1.6 Troubleshooting Ethernet Circuit Paths With Loopbacks

Facility (line) loopbacks, terminal (inward) loopbacks, and cross-connect loopback circuits are often used together to test the circuit path through the network or to logically isolate a fault. Performing a loopback test at each point along the circuit path systematically isolates possible points of failure.

You can use these procedures on G-Series Ethernet cards and CE100T-8 cards but not on E-Series or ML-Series Ethernet cards. The example in this section tests a G-Series card circuit on a three-node BLSR. Using a series of facility (line) loopbacks and terminal (inward) loopbacks, the example scenario traces the circuit path, tests the possible failure points, and eliminates them. The logical progression contains six network test procedures:

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

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

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

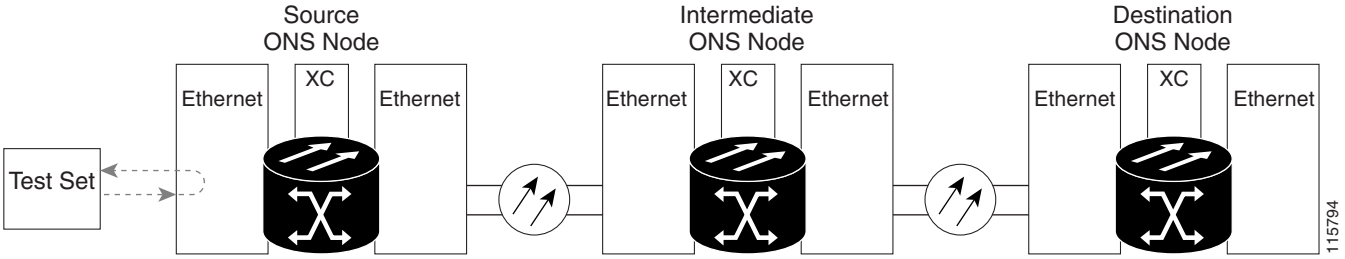
1.6.1 Perform a Facility (Line) Loopback on a Source-Node Ethernet Port

The facility (line) loopback test is performed on the node source port in the network circuit. In the testing situation used in this example, the source G-Series port in the source node. Completing a successful facility (line) loopback on this port isolates the G-Series port as a possible failure point. Figure 1-22 shows an example of a facility loopback on a circuit source Ethernet port.

Note Facility (line) loopbacks are not available for Release 4.1 or earlier G-Series cards.

Note Facility loopbacks require on-site personnel.

Figure 1-31 Facility (Line) Loopback on a Circuit Source Ethernet Port



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

Complete the "Create the Facility (Line) Loopback on the Source-Node Ethernet Port" procedure on page 1-72.

Create the Facility (Line) Loopback on the Source-Node Ethernet Port

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

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

Use appropriate cabling to attach the 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 > Loopback** tab.

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

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

Step 7 Click **Apply**.

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

Note It is normal for the "LPBKFACILITY (G1000)" condition on page 2-155 to appear during loopback setup. The condition clears when you remove the loopback.

Step 9 Complete the "Test and Clear the Facility (Line) Loopback Circuit" procedure on page 1-73.

Test and Clear the Facility (Line) Loopback Circuit

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

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

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

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

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

c. Choose the appropriate state (IS; OOS,DSBLD; OOS,MT) from the Admin State column for the port being tested.

d. Click **Apply**.

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

Step 4 Complete the "Test the Ethernet Card" procedure on page 1-73.

Test the Ethernet Card

Step 1 Complete the "Physically Replace a Traffic Card" procedure on page 2-243 for the suspected bad card and replace it with a known-good one.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Refer to the procedures in the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-231. For more information, refer to the "Maintain the Node" chapter in the *Cisco ONS 15454 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 "Physically Replace a Traffic Card" procedure on page 2-243 for the faulty card.

Step 5 Clear the facility (line) loopback:

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

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

c. Choose the appropriate state (IS; OOS,DSBLD; OOS,MT) from the Admin State column for the port being tested.

d. Click **Apply**.

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

Step 6 Complete the "1.6.2 Perform a Terminal (Inward) Loopback on a Source-Node Ethernet Port" procedure on page 1-74.

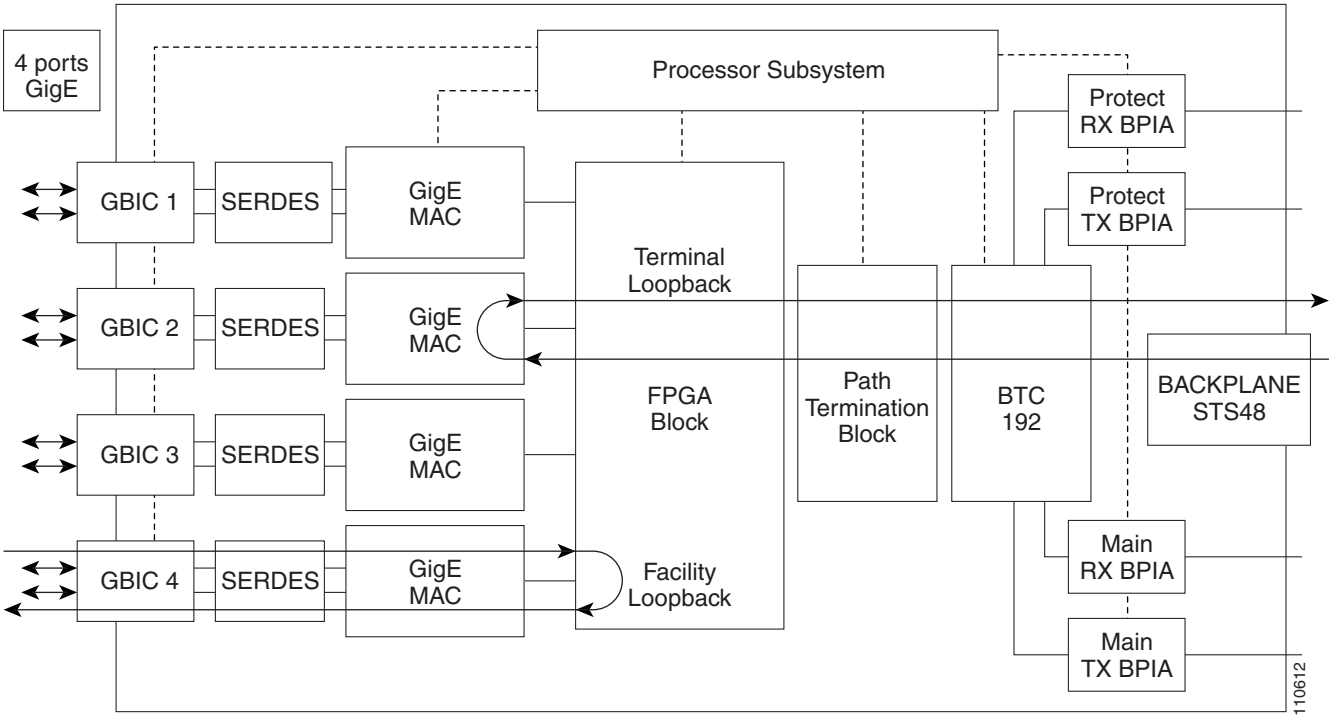
1.6.2 Perform a Terminal (Inward) Loopback on a Source-Node Ethernet Port

The terminal (inward) loopback test is performed on the node source Ethernet port. For the circuit in this example, it is the source G-Series port in the source node. You first create a bidirectional circuit that starts on the node destination G-Series port and loops back on the node source G-Series 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 1-32 shows terminal loopback on a G-Series port.

Note Terminal (inward) loopbacks are not available for R4.0 and earlier G-Series cards.

Note Terminal loopbacks require on-site personnel.

Figure 1-32 Terminal (Inward) Loopback on a G-Series Port



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

Complete the "Create the Terminal (Inward) Loopback on a Source-Node Ethernet Port" procedure on page 1-74.

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

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

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

a. If you just completed the "1.6.1 Perform a Facility (Line) Loopback on a Source-Node Ethernet Port" procedure on page 1-71, leave the optical test set hooked up to the Ethernet port in the source node.

b. If you are starting the current procedure without the optical test set hooked up to the source port, use appropriate cabling to attach the 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 (inward) loopback on the test port:

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

b. In the Circuit Creation dialog box, choose the type, such as STS, and number, such as 1.

c. Click **Next**.

d. In the next Circuit Creation dialog box, give the circuit an easily identifiable name such as G1K1toG1K2.

e. Leave the **Bidirectional** check box checked.

f. Click **Next**.

g. In the Circuit Creation source dialog box, select the same Node, card Slot, Port, and STS (or VT) 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 STS (or VT) used for the source dialog box.

j. Click **Next**.

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

Step 4 Confirm that the newly created circuit appears on the Circuits tab list as a two-way circuit.

Note It is normal for the "LPBKTERMINAL (G1000)" condition on page 2-159 to appear during a loopback setup. The condition clears when you remove the loopback.

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

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

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

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

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

e. Click **Apply**.

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

Step 6 Complete the "Test and Clear the Ethernet Terminal Loopback Circuit" procedure on page 1-76.

Test and Clear the Ethernet Terminal Loopback Circuit

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

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

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

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

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

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

d. Select the appropriate state (IS; OOS,DSBLD; OOS,MT) in the Admin State column for the port being tested.

e. Click **Apply**.

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

Step 4 Clear the terminal loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

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

Step 5 Complete the "Test the Ethernet Card" procedure on page 1-76.

Test the Ethernet Card

Step 1 Complete the "Physically Replace a Traffic Card" procedure on page 2-243 for the suspected bad card and replace it with a known-good one.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Refer to the procedures in the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-231. For more information, refer to the "Maintain the Node" chapter in the *Cisco ONS 15454 Procedure Guide*.

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 (1 800 553-2447).

Step 4 Complete the "Physically Replace a Traffic Card" procedure on page 2-243 for the defective card.

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

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

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

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

d. Select the appropriate state (IS; OOS,DSBLD; OOS,MT) in the Admin State column for the port being tested.

e. Click **Apply**.

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

Step 6 Clear the terminal loopback circuit before testing the next segment of the network circuit path:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

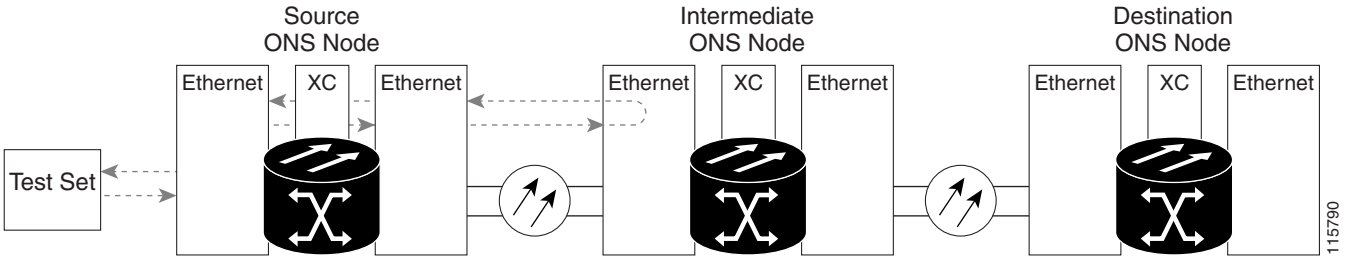
d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

Step 7 Complete the "1.6.3 Create a Facility (Line) Loopback on an Intermediate-Node Ethernet Port" procedure on page 1-77.

1.6.3 Create a Facility (Line) Loopback on an Intermediate-Node Ethernet Port

Performing the facility (line) loopback test on an intermediate port isolates whether this node is causing circuit failure. It is shown in Figure 1-33.

Figure 1-33 Facility (Line) 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 (Line) Loopback on an Intermediate-Node Ethernet Port" procedure on page 1-78.

Create a Facility (Line) Loopback on an Intermediate-Node Ethernet Port

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

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

a. If you just completed the "1.6.2 Perform a Terminal (Inward) Loopback on a Source-Node Ethernet Port" procedure on page 1-74, leave the optical test set hooked up to the source-node port.

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

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

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

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

b. In the Circuit Creation dialog box, choose the type, such as STS, and number, such as 1.

c. Click **Next**.

d. In the next Circuit Creation dialog box, give the circuit an easily identifiable name such as G1KtoG1K3.

e. Leave the **Bidirectional** check box checked.

f. Click **Next**.

g. In the Circuit Creation source dialog box, select the same Node, card Slot, Port, and STS (or VT) 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 STS (or VT) used for the source dialog box.

j. Click **Next**.

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

Step 4 Confirm that the newly created circuit appears on the Circuits tab list as a two-way circuit.

Note It is normal for the "LPBKFACILITY (G1000)" condition on page 2-155 or the "LPBKFACILITY (OCN)" condition on page 2-155 to appear during a loopback setup. The condition clears when you remove the loopback.

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

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

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

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

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

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

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

f. Click **Apply**.

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

Step 6 Complete the "Test and Clear the Ethernet Facility (Line) Loopback Circuit" procedure on page 1-79.

Test and Clear the Ethernet Facility (Line) Loopback Circuit

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

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

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

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

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

c. Choose the appropriate state (IS; OOS,DSBLD; OOS,MT) from the Admin State column for the port being tested.

d. Click **Apply**.

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

Step 4 Clear the facility (line) loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

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

Step 5 Complete the "Test the Ethernet Card" procedure on page 1-79.

Test the Ethernet Card

Step 1 Complete the "Physically Replace a Traffic Card" procedure on page 2-243 for the suspected bad card and replace it with a known-good one.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Refer to the procedures in the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-231. For more information, refer to the "Maintain the Node" chapter in the *Cisco ONS 15454 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 "Physically Replace a Traffic Card" procedure on page 2-243 for the faulty card.

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

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

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

c. Choose the appropriate state (IS; OOS,DSBLD; OOS,MT) from the Admin State column for the port being tested.

d. Click **Apply**.

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

Step 6 Clear the facility loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

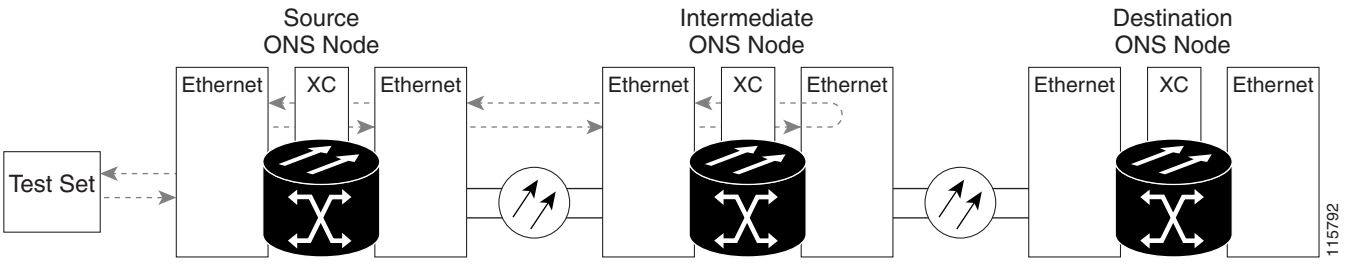
d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

Step 7 Complete the "1.6.4 Create a Terminal (Inward) Loopback on Intermediate-Node Ethernet Ports" procedure on page 1-80.

1.6.4 Create a Terminal (Inward) Loopback on Intermediate-Node Ethernet Ports

In the next troubleshooting test, you perform a terminal loopback on the intermediate-node port to isolate whether the destination port is causing circuit trouble. In the example situation in Figure 1-34, 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 1-34 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 Intermediate-Node Ethernet Ports" procedure on page 1-81.

Create a Terminal Loopback on Intermediate-Node Ethernet 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 "1.6.3 Create a Facility (Line) Loopback on an Intermediate-Node Ethernet Port" procedure on page 1-77 for the Ethernet circuit, 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 (inward) loopback on the test port:

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

b. In the Circuit Creation dialog box, choose the type, such as STS, and number, such as 1.

c. Click **Next**.

d. In the next Circuit Creation dialog box, give the circuit an easily identifiable name such as G1K1toG1K4.

e. Leave the **Bidirectional** check box checked.

f. Click **Next**.

g. In the Circuit Creation source dialog box, select the same Node, card Slot, Port, and STS (or VT) 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 STS (or VT) used for the source dialog box.

j. Click **Next**.

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

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

Note It is normal for the "LPBKTERMINAL (G1000)" condition on page 2-159 to appear during a loopback setup. The condition clears when you remove the loopback.

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

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

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

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

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

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

f. Click **Apply**.

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

Step 6 Complete the "Test and Clear the Ethernet Terminal Loopback Circuit" procedure on page 1-82.

Test and Clear the Ethernet Terminal Loopback Circuit

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

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

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

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

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

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

d. Select the appropriate state (IS; OOS,DSBLD; OOS,MT) in the Admin State column for the port being tested.

e. Click **Apply**.

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

Step 4 Clear the terminal loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

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

Step 5 Complete the "Test the Ethernet Card" procedure on page 1-83.

Test the Ethernet Card

Step 1 Complete the "Physically Replace a Traffic Card" procedure on page 2-243 for the suspected bad card and replace it with a known-good one.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Refer to the procedures in the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-231. For more information, refer to the "Maintain the Node" chapter in the *Cisco ONS 15454 Procedure Guide*.

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 (1 800 553-2447).

Step 4 Complete the "Physically Replace a Traffic Card" procedure on page 2-243 for the defective card.

Step 5 Clear the terminal loopback on the port:

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

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

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

d. Select the appropriate state (IS; OOS,DSBLD; OOS,MT) 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**.

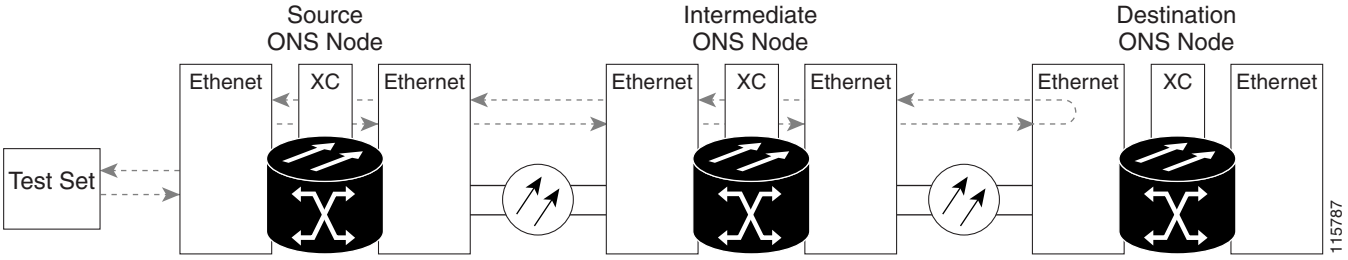
d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

Step 7 Complete the "1.6.5 Perform a Facility (Line) Loopback on a Destination-Node Ethernet Port" procedure on page 1-83.

1.6.5 Perform a Facility (Line) Loopback on a Destination-Node Ethernet Port

You perform a facility (line) loopback test at the destination port to determine whether this local port is the source of circuit trouble. The example in Figure 1-35 shows a facility loopback being performed on an Ethernet port.

Figure 1-35 Facility (Line) 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 (Line) Loopback on a Destination-Node Ethernet Port" procedure on page 1-84.

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

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

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

a. If you just completed the "1.6.4 Create a Terminal (Inward) Loopback on Intermediate-Node Ethernet Ports" section on page 1-80, 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 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 STS, and number, such as 1.

c. Click **Next**.

d. In the next Circuit Creation dialog box, give the circuit an easily identifiable name such as G1K1toG1K5.

e. Leave the **Bidirectional** check box checked.

f. Click **Next**.

g. In the Circuit Creation source dialog box, select the same Node, card Slot, Port, and STS (or VT) 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 STS (or VT) used for the source dialog box.

j. Click **Next**.

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

Step 4 Confirm that the newly created circuit appears on the Circuits tab list as a two-way circuit.

Note It is normal for the "LPBKFACILITY (G1000)" condition on page 2-155 to appear during a loopback setup. The condition clears when you remove the loopback.

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

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

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

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

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

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

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

f. Click **Apply**.

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

Step 6 Complete the "Test and Clear the Ethernet Facility (Line) Loopback Circuit" procedure on page 1-85.

Test and Clear the Ethernet Facility (Line) Loopback Circuit

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

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

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

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

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

c. Choose the appropriate state (IS; OOS,DSBLD; OOS,MT) from the Admin State column for the port being tested.

d. Click **Apply**.

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

Step 4 Clear the facility (line) loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

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

Step 5 Complete the "Test the Ethernet Card" procedure on page 1-86.

Test the Ethernet Card

Step 1 Complete the "Physically Replace a Traffic Card" procedure on page 2-243 for the suspected bad card and replace it with a known-good one.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Refer to the procedures in the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-231. For more information, refer to the "Maintain the Node" chapter in the *Cisco ONS 15454 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 "Physically Replace a Traffic Card" procedure on page 2-243 for the faulty card.

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

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

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

c. Choose the appropriate state (IS; OOS,DSBLD; OOS,MT) from the Admin State column for the port being tested.

d. Click **Apply**.

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

Step 6 Clear the facility loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

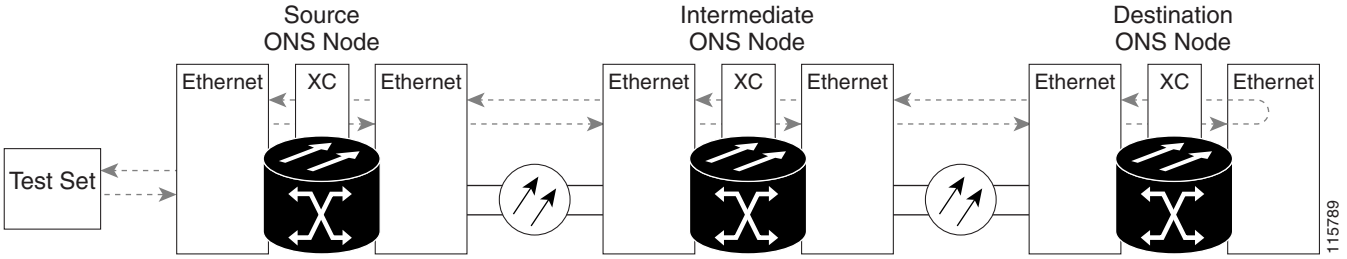
d. Click **Yes** in the Delete Circuits dialog box. Do not check any check boxes.

Step 7 Complete the "1.6.6 Perform a Terminal Loopback on a Destination-Node Ethernet Port" procedure on page 1-86.

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

The terminal loopback at the destination-node port is the final local hardware error elimination in the circuit troubleshooting process. If this test is completed successfully, you have verified that the circuit is good up to the destination port. The example in Figure 1-30 shows a terminal loopback on an intermediate-node destination Ethernet port.

Figure 1-36 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 1-87.

Create the Terminal Loopback on a Destination-Node Ethernet Port

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

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

a. If you just completed the "1.6.5 Perform a Facility (Line) Loopback on a Destination-Node Ethernet Port" procedure on page 1-83, 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 STS, and number, such as 1.

c. Click **Next**.

d. In the next Circuit Creation dialog box, give the circuit an easily identifiable name such as G1K1toG1K6.

e. Leave the **Bidirectional** check box checked.

f. Click **Next**.

g. In the Circuit Creation source dialog box, select the same Node, card Slot, Port, and STS (or VT) 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 STS (or VT) used for the source dialog box.

j. Click **Next**.

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

Step 4 Confirm that the newly created circuit appears on the Circuits tab list as a two-way circuit.

Note It is normal for the "LPBKTERMINAL (G1000)" condition on page 2-159 to appear during a loopback setup. The condition clears when you remove the loopback.

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

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

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

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

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

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

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

f. Click **Apply**.

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

Step 6 Complete the "Test and Clear the Ethernet Terminal Loopback Circuit" procedure on page 1-88.

Test and Clear the Ethernet Terminal Loopback Circuit

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

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

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

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

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

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

d. Select the appropriate state (IS; OOS,DSBLD; OOS,MT) in the Admin State column for the port being tested.

e. Click **Apply**.

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

Step 4 Clear the terminal loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

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

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

Step 5 If the test set indicates a faulty circuit, the problem might be a faulty card.

Step 6 Complete the "Test the Ethernet Card" procedure on page 1-89.

Test the Ethernet Card

Step 1 Complete the "Physically Replace a Traffic Card" procedure on page 2-243 for the suspected bad card and replace it with a known-good 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. Refer to the procedures in the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-231. For more information, refer to the "Maintain the Node" chapter in the *Cisco ONS 15454 Procedure Guide*.

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 (1 800 553-2447).

Step 4 Complete the "Physically Replace a Traffic Card" procedure on page 2-243 for the defective card.

Step 5 Clear the terminal loopback on the port:

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

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

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

d. Select the appropriate state (IS; OOS,DSBLD; OOS,MT) in the Admin State column for the port being tested.

e. Click **Apply**.

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

Step 6 Clear the terminal loopback circuit:

a. Click the **Circuits** tab.

b. Choose the loopback circuit being tested.

c. Click **Delete**.

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

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

1.7 Troubleshooting MXP, TXP, or FC_MR-4 Circuit Paths With Loopbacks

Facility (line) loopbacks, terminal (inward) loopbacks, and cross-connect loopback circuits are often used together to test the circuit path through the network or to logically isolate a fault. Performing a loopback test at each point along the circuit path systematically isolates possible points of failure. MXP/TXP/FC_MR-4 loopback tests differ from electrical, optical, and Ethernet testing in that loopback testing does not require circuit creation. MXP, TXP, and FC_MR-4 client ports are statically mapped to the trunk ports so no signal needs to traverse the cross-connect card (in a circuit) to test the loopback.

You can use these procedures on transponder cards (TXP, TXPP), muxponder cards (MXP, MXPP), and fibre channel data storage (FC_MR-4) cards. The example in this section tests an MXP/TXP/FC_MR-4 circuit on a three-node BLSR. Using a series of facility (line) loopbacks and terminal (inward) loopbacks, the example scenario traces the circuit path, tests the possible failure points, and eliminates them. The logical progression contains seven network test procedures:

Note MXP/TXP/FC_MR-4 card client ports do not appear in the Maintenance > Loopback tab unless they have been provisioned. Do this in the card view Provisioning > Pluggable Port Modules tab. For information about provisioning client ports, refer to the *Cisco ONS 15454 Procedure Guide*.

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

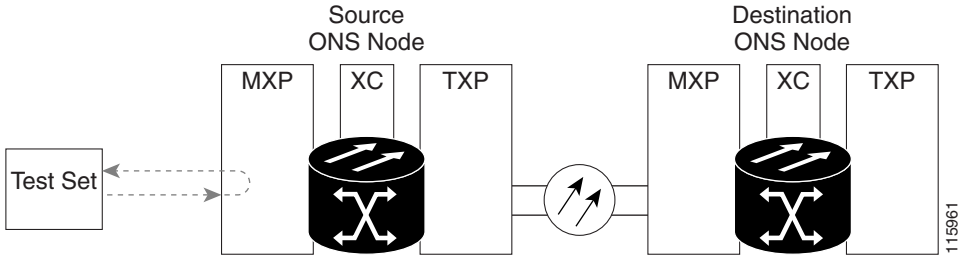
1. A facility (line) loopback on the source-node MXP/TXP/FC_MR-4 port
2. A terminal (inward) loopback on the source-node MXP/TXP/FC_MR-4 port
3. A facility (line) loopback on the intermediate-node MXP/TXP/FC_MR-4 port
4. A terminal (inward) loopback on the intermediate-node MXP/TXP/FC_MR-4 port
5. A facility (line) loopback on the destination-node MXP/TXP/FC_MR-4 port
6. A terminal (inward) loopback on the destination-node MXP/TXP/FC_MR-4 port

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

1.7.1 Perform a Facility (Line) Loopback on a Source-Node MXP/TXP/FC_MR-4 Port

The facility (line) loopback test is performed on the node source port in the network circuit. In the testing situation used in this example, the source muxponder or transponder port in the source node. Completing a successful facility (line) loopback on this port isolates the MXP/TXP/FC_MR-4 port as a possible failure point. Figure 1-37 shows an example of a facility loopback on a circuit source MXP/TXP/FC_MR-4 port.

Figure 1-37 Facility (Line) Loopback on a Circuit Source MXP/TXP/FC_MR-4 Port



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

Note Facility loopbacks require on-site personnel.

Complete the "Create the Facility (Line) Loopback on the Source-Node MXP/TXP/FC_MR-4 Port" procedure on page 1-91.

Create the Facility (Line) Loopback on the Source-Node MXP/TXP/FC_MR-4 Port

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

Note For specific procedures to connect, set up, and 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 > Loopback** tab.

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

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

Step 7 Click **Apply**.

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

Note It is normal for the "LPBKFACILITY (OCN)" condition on page 2-155 or the "LPBKFACILITY (G1000)" condition on page 2-155 to appear during loopback setup. The condition clears when you remove the loopback.

Step 9 Complete the "Test and Clear the MXP/TXP/FC_MR-4 Facility (Line) Loopback Circuit" procedure on page 1-92.

Test and Clear the MXP/TXP/FC_MR-4 Facility (Line) Loopback Circuit

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

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

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

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

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

c. Choose the appropriate state (**IS**; **OOS,DSBLD**; **OOS,MT**; **IS,AINS**) from the Admin State column for the port being tested.

d. Click **Apply**.

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

Step 4 Complete the "Test the MXP/TXP/FC_MR-4 Card" procedure on page 1-92.

Test the MXP/TXP/FC_MR-4 Card

Step 1 Complete the "Physically Replace a Traffic Card" procedure on page 2-243 for the suspected bad card and replace it with a known-good one.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Refer to the procedures in the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-231. For more information, refer to the "Maintain the Node" chapter in the *Cisco ONS 15454 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 "Physically Replace a Traffic Card" procedure on page 2-243 for the faulty card.

Step 5 Clear the facility (line) loopback:

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

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

c. Choose the appropriate state (**IS**; **OOS,DSBLD**; **OOS,MT**; **IS,AINS**) from the Admin State column for the port being tested.

d. Click **Apply**.

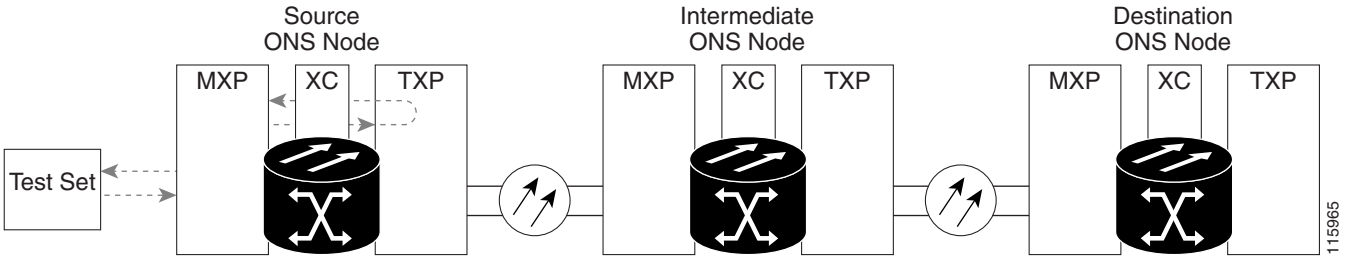
e. Click **Yes** in the confirmation dialog box.

Step 6 Complete the "1.7.2 Perform a Terminal (Inward) Loopback on a Source-Node MXP/TXP/FC_MR-4 Port" procedure on page 1-93.

1.7.2 Perform a Terminal (Inward) Loopback on a Source-Node MXP/TXP/FC_MR-4 Port

The terminal (inward) loopback test is performed on the node source MXP/TXP/FC_MR-4 muxponder or transponder port. For the circuit in this example, it is the source MXP port in the source node. Completing a successful terminal loopback to a node source port verifies that the circuit is good to the source port. Figure 1-38 shows an example of a terminal loopback on a source MXP/TXP/FC_MR-4 port.

Figure 1-38 Terminal (Inward) Loopback on a Source-Node MXP/TXP/FC_MR-4 Port



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

Note Terminal loopbacks require on-site personnel.

Complete the "Create the Terminal (Inward) Loopback on a Source-Node MXP/TXP/FC_MR-4 Port" procedure on page 1-93.

Create the Terminal (Inward) Loopback on a Source-Node MXP/TXP/FC_MR-4 Port

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

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

a. If you just completed the "1.7.1 Perform a Facility (Line) Loopback on a Source-Node MXP/TXP/FC_MR-4 Port" procedure on page 1-90, leave the optical test set hooked up to the MXP or TXP port in the source node.

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

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

Step 3 In node view, double-click the card that requires the loopback, such as the destination OC-N card in the source node.

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

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

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

Step 7 Click **Apply**.

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

Step 9 Complete the "Test and Clear the MXP/TXP/FC_MR-4 Port Terminal Loopback Circuit" procedure on page 1-94.

Test and Clear the MXP/TXP/FC_MR-4 Port Terminal Loopback Circuit

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

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

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

- **a.** Double-click the card in the source node with the terminal loopback.
- **b.** Click the **Maintenance > Loopback** tab.
- **c.** Select **None** from the Loopback Type column for the port being tested.
- **d.** Select the appropriate state (**IS**; **OOS,DSBLD**; **OOS,MT**; **IS,AINS**) in the Admin State column for the port being tested.
- **e.** Click **Apply**.
- **f.** Click **Yes** in the confirmation dialog box.

Step 4 Complete the "Test the MXP/TXP/FC_MR-4 Card" procedure on page 1-94.

Test the MXP/TXP/FC_MR-4 Card

Step 1 Complete the "Physically Replace a Traffic Card" procedure on page 2-243 for the suspected bad card and replace it with a known-good one.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Refer to the procedures in the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-231. For more information, refer to the "Maintain the Node" chapter in the *Cisco ONS 15454 Procedure Guide*.

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 (1 800 553-2447).

Step 4 Complete the "Physically Replace a Traffic Card" procedure on page 2-243 for the defective card.

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

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

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

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

d. Select the appropriate state (**IS**; **OOS,DSBLD**; **OOS,MT**; **IS,AINS**) in the Admin State column for the port being tested.

e. Click **Apply**.

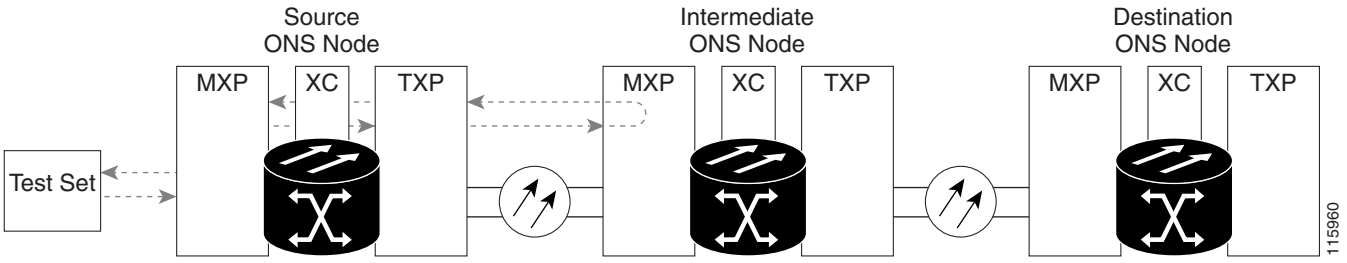
f. Click **Yes** in the confirmation dialog box.

Step 6 Complete the "1.7.3 Create a Facility (Line) Loopback on an Intermediate-Node MXP/TXP/FC_MR-4 Port" procedure on page 1-95.

1.7.3 Create a Facility (Line) Loopback on an Intermediate-Node MXP/TXP/FC_MR-4 Port

Performing the facility (line) loopback test on an intermediate port isolates whether this node is causing circuit failure. In the situation shown in Figure 1-39, the test is being performed on an intermediate MXP/TXP/FC_MR-4 port.

Figure 1-39 Facility (Line) Loopback on an Intermediate-Node MXP/TXP/FC_MR-4 Port



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

Note Facility loopbacks require on-site personnel.

Complete the "Create a Facility (Line) Loopback on an Intermediate-Node MXP/TXP/FC_MR-4 Port" procedure on page 1-96.

Create a Facility (Line) Loopback on an Intermediate-Node MXP/TXP/FC_MR-4 Port

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

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

a. If you just completed the "1.7.2 Perform a Terminal (Inward) Loopback on a Source-Node MXP/TXP/FC_MR-4 Port" procedure on page 1-93, leave the optical test set hooked up to the source-node port.

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

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

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

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

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

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

Step 7 Click **Apply**.

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

Step 9 Complete the "Test and Clear the MXP/TXP/FC_MR-4 Port Facility (Line) Loopback Circuit" procedure on page 1-96.

Test and Clear the MXP/TXP/FC_MR-4 Port Facility (Line) Loopback Circuit

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

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

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

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

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

c. Choose the appropriate state (**IS**; **OOS,DSBLD**; **OOS,MT**; **IS,AINS**) from the Admin State column for the port being tested.

d. Click **Apply**.

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

Step 4 Complete the "Test the MXP/TXP/FC_MR-4 Card" procedure on page 1-97.

Test the MXP/TXP/FC_MR-4 Card

Step 1 Complete the "Physically Replace a Traffic Card" procedure on page 2-243 for the suspected bad card and replace it with a known-good one.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Refer to the procedures in the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-231. For more information, refer to the "Maintain the Node" chapter in the *Cisco ONS 15454 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 "Physically Replace a Traffic Card" procedure on page 2-243 for the faulty card.

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

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

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

c. Choose the appropriate state (**IS**; **OOS,DSBLD**; **OOS,MT**; **IS,AINS**) from the Admin State column for the port being tested.

d. Click **Apply**.

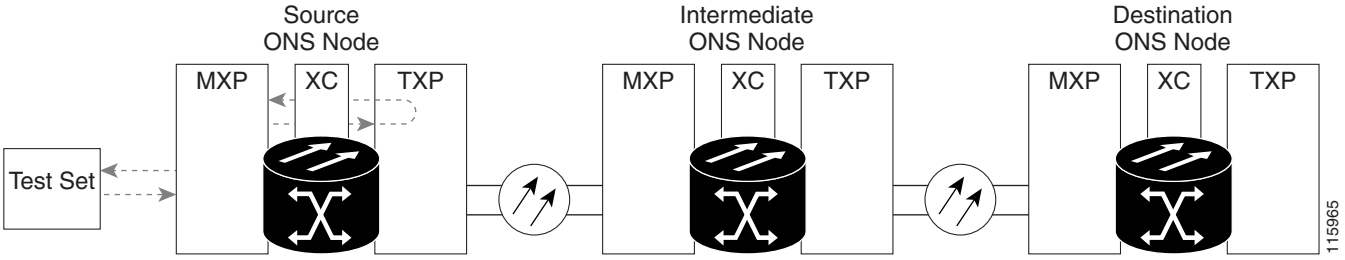
e. Click **Yes** in the confirmation dialog box.

Step 6 Complete the "1.7.4 Create a Terminal (Inward) Loopback on Intermediate-Node MXP/TXP/FC_MR-4 Ports" procedure on page 1-97.

1.7.4 Create a Terminal (Inward) Loopback on Intermediate-Node MXP/TXP/FC_MR-4 Ports

In the next troubleshooting test, you perform a terminal loopback on the intermediate-node port to isolate whether the destination port is causing circuit trouble. In the example situation in Figure 1-40, the terminal loopback is performed on an intermediate MXP/TXP/FC_MR-4 port in the circuit. If you successfully complete a terminal loopback on the node, this node is excluded from possible sources of circuit trouble.

Figure 1-40 Terminal Loopback on an Intermediate-Node MXP/TXP/FC_MR-4 Port



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

Note Terminal loopbacks require on-site personnel.

Complete the "Create a Terminal Loopback on Intermediate-Node MXP/TXP/FC_MR-4 Ports" procedure on page 1-98.

Create a Terminal Loopback on Intermediate-Node MXP/TXP/FC_MR-4 Ports

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

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

a. If you just completed the "1.7.3 Create a Facility (Line) Loopback on an Intermediate-Node MXP/TXP/FC_MR-4 Port" section on page 1-95, leave the optical test set hooked up to the source-node port.

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

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

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

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

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

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

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

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

f. Click **Apply**.

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

Step 4 Complete the "Test and Clear the MXP/TXP/FC_MR-4 Terminal Loopback Circuit" procedure on page 1-99.

Test and Clear the MXP/TXP/FC_MR-4 Terminal Loopback Circuit

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

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

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

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

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

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

d. Select the appropriate state (**IS**; **OOS,DSBLD**; **OOS,MT**; **IS,AINS**) in the Admin State column for the port being tested.

e. Click **Apply**.

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

Step 4 Complete the "Test the MXP/TXP/FC_MR-4 Card" procedure on page 1-99.

Test the MXP/TXP/FC_MR-4 Card

Step 1 Complete the "Physically Replace a Traffic Card" procedure on page 2-243 for the suspected bad card and replace it with a known-good one.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Refer to the procedures in the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-231. For more information, refer to the "Maintain the Node" chapter in the *Cisco ONS 15454 Procedure Guide*.

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 (1 800 553-2447).

Step 4 Complete the "Physically Replace a Traffic Card" procedure on page 2-243 for the defective card.

Step 5 Clear the terminal loopback on the port:

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

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

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

d. Select the appropriate state (**IS**; **OOS,DSBLD**; **OOS,MT**; **IS,AINS**) in the Admin State column for the port being tested.

e. Click **Apply**.

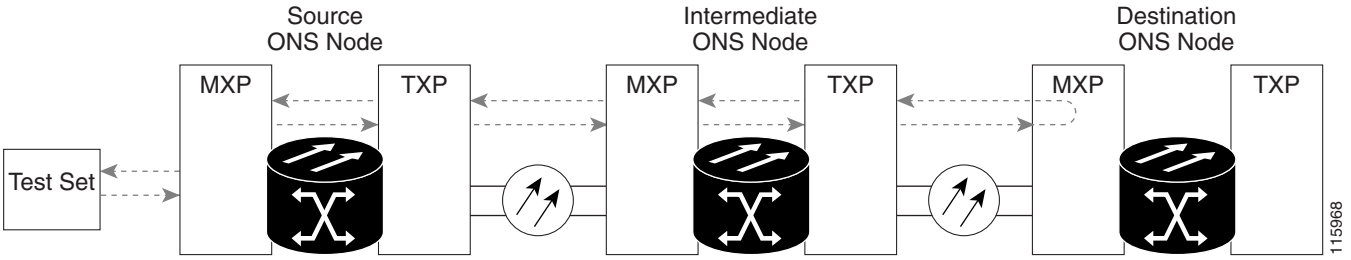
f. Click **Yes** in the confirmation dialog box.

Step 6 Complete the "1.7.5 Perform a Facility (Line) Loopback on a Destination-Node MXP/TXP/FC_MR-4 Port" procedure on page 1-100.

1.7.5 Perform a Facility (Line) Loopback on a Destination-Node MXP/TXP/FC_MR-4 Port

You perform a facility (line) loopback test at the destination port to determine whether this local port is the source of circuit trouble. The example in Figure 1-41 shows a facility loopback being performed on an MXP/TXP/FC_MR-4 port.

Figure 1-41 Facility (Line) Loopback on a Destination-Node MXP/TXP/FC_MR-4 Port



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

Note Facility loopbacks require on-site personnel.

Complete the "Create the Facility (Line) Loopback on a Destination-Node MXP/TXP/FC_MR-4 Port" procedure on page 1-100.

Create the Facility (Line) Loopback on a Destination-Node MXP/TXP/FC_MR-4 Port

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

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

a. If you just completed the "1.7.4 Create a Terminal (Inward) Loopback on Intermediate-Node MXP/TXP/FC_MR-4 Ports" procedure on page 1-97, leave the optical test set hooked up to the source-node port.

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

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

Step 3 Create the facility (line) loopback on the destination port being tested:

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

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

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

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

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

f. Click **Apply**.

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

Step 4 Complete the "Test and Clear the MXP/TXP/FC_MR-4 Facility (Line) Loopback Circuit" procedure on page 1-101.

Test and Clear the MXP/TXP/FC_MR-4 Facility (Line) Loopback Circuit

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

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

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

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

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

c. Choose the appropriate state (**IS**; **OOS,DSBLD**; **OOS,MT**; **IS,AINS**) from the Admin State column for the port being tested.

d. Click **Apply**.

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

Step 4 Complete the "Test the MXP/TXP/FC_MR-4 Card" procedure on page 1-101.

Test the MXP/TXP/FC_MR-4 Card

Step 1 Complete the "Physically Replace a Traffic Card" procedure on page 2-243 for the suspected bad card and replace it with a known-good one.

Caution Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. Refer to the procedures in the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-231. For more information, refer to the "Maintain the Node" chapter in the *Cisco ONS 15454 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 "Physically Replace a Traffic Card" procedure on page 2-243 for the faulty card.

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

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

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

c. Choose the appropriate state (**IS**; **OOS,DSBLD**; **OOS,MT**; **IS,AINS**) from the Admin State column for the port being tested.

d. Click **Apply**.

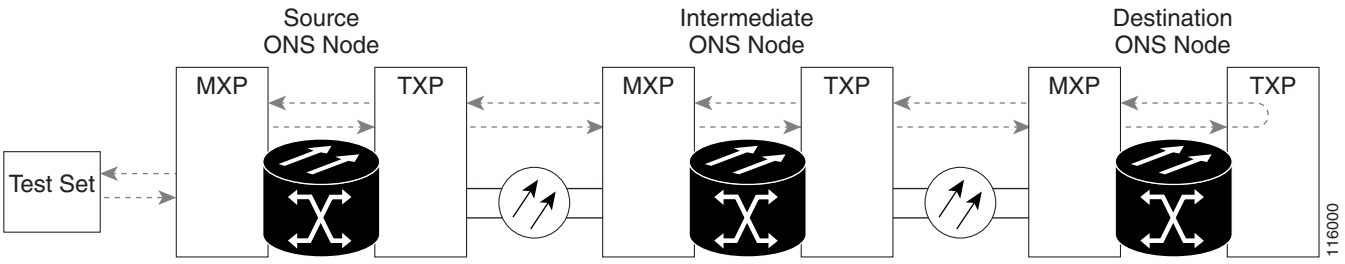
e. Click **Yes** in the confirmation dialog box.

Step 6 Complete the "1.7.6 Perform a Terminal Loopback on a Destination-Node MXP/TXP/FC_MR-4 Port" procedure on page 1-102.

1.7.6 Perform a Terminal Loopback on a Destination-Node MXP/TXP/FC_MR-4 Port

The terminal loopback at the destination-node port is the final local hardware error elimination in the circuit troubleshooting process. If this test is completed successfully, you have verified that the circuit is good up to the destination port. The example in Figure 1-42 shows a terminal loopback on an intermediate-node destination MXP/TXP/FC_MR-4 port.

Figure 1-42 Terminal Loopback on a Destination-Node MXP/TXP/FC_MR-4 Port



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

Note Terminal loopbacks require on-site personnel.

Complete the "Create the Terminal Loopback on a Destination-Node MXP/TXP/FC_MR-4 Port" procedure on page 1-103.

Create the Terminal Loopback on a Destination-Node MXP/TXP/FC_MR-4 Port

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

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

a. If you just completed the "1.7.5 Perform a Facility (Line) Loopback on a Destination-Node MXP/TXP/FC_MR-4 Port" procedure on page 1-100, 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 Confirm that the newly created circuit appears on the Circuits tab list as a two-way circuit.

Note It is normal for the "LPBKTERMINAL (OCN)" condition on page 2-160 to appear during a loopback setup. The condition clears when you remove the loopback.

Step 4 Create the terminal loopback on the destination port being tested:

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

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

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

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

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

f. Click **Apply**.

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

Step 5 Complete the "Test and Clear the MXP/TXP/FC_MR-4 Terminal Loopback Circuit" procedure on page 1-104.

Test and Clear the MXP/TXP/FC_MR-4 Terminal Loopback Circuit

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

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

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

- **a.** Double-click the intermediate-node card with the terminal loopback.
- **b.** Click the **Maintenance > Loopback** tab.
- **c.** Select **None** from the Loopback Type column for the port being tested.
- **d.** Select the appropriate state (**IS**; **OOS,DSBLD**; **OOS,MT**; **IS,AINS**) in the Admin State column for the port being tested.
- **e.** Click **Apply**.
- **f.** Click **Yes** in the confirmation dialog box.

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

Step 5 Complete the "Test the MXP/TXP/FC_MR-4 Card" procedure on page 1-104.

Test the MXP/TXP/FC_MR-4 Card

Step 1 Complete the "Physically Replace a Traffic Card" procedure on page 2-243 for the suspected bad card and replace it with a known-good 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 procedures in the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-231. For more information, refer to the "Maintain the Node" chapter in the *Cisco ONS 15454 Procedure Guide*.

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 (1 800 553-2447).

Step 4 Complete the "Physically Replace a Traffic Card" procedure on page 2-243 for the defective card.

Step 5 Clear the terminal loopback on the port:

- **a.** Double-click the source-node card with the terminal loopback.
- **b.** Click the **Maintenance > Loopback** tab.
- **c.** Select **None** from the Loopback Type column for the port being tested.
- **d.** Select the appropriate state (**IS**; **OOS,DSBLD**; **OOS,MT**; **IS,AINS**) in the Admin State column for the port being tested.
- **e.** Click **Apply**.
- **f.** Click **Yes** in the confirmation dialog box.

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

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

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

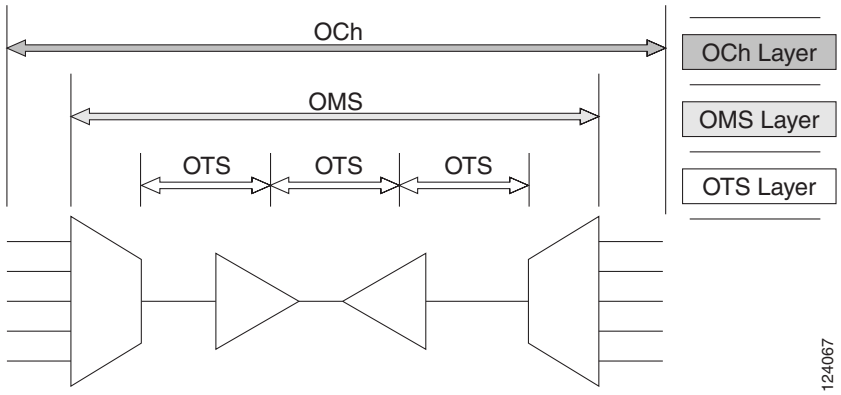
1.8.1 G.709 Monitoring in Optical Transport Networks

Recommendation ITU-T G.709 is part of a suite of recommendations covering the full functionality of an OTN. ITU-T G.709 takes single-wavelength SONET technology a step further by enabling transparent optical wavelength-based networks. It adds extra overhead to existing SONET, Ethernet, or asynchronous transfer mode (ATM) bit streams for performance management and improvement.

ITU-T G.709 adds the operations, administration, maintenance and provisioning (OAM&P) functionality of SONET/SDH to DWDM optical networks.

Like traditional SONET networks, ITU-T G.709 optical networks have a layered design (Figure 1-43). This structure enables localized monitoring that helps you isolate and troubleshoot network problems.

Figure 1-43 Optical Transport Network Layers



1.8.2 Optical Channel Layer

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

1. A client signal such as SONET, Gigabit Ethernet, IP, ATM, fiber channel, or enterprise system connection (ESCON) is mapped to a client payload area and combined with an overhead to create the optical channel payload unit (OPUk).

2. A second overhead is added to the OPUk unit to create the optical channel data unit (ODUk).
3. A third overhead including forward error correction (FEC) is added to the ODUk to create the optical channel transport unit (OTUk).
4. A fourth overhead is added to the OTUk to create the entire OCh layer

1.8.3 Optical Multiplex Section Layer

The optical multiplex section (OMS) of the OTN allows carriers to identify errors occurring within DWDM network sections. The OMS layer consists of a payload and an overhead (OMS-OH). It supports the ability to monitor multiplexed sections of the network, for example the span between an optical multiplexer such as the 3 2MUX-O and a demultiplexer such as the 32 DMX-O.

1.8.4 Optical Transmission Section Layer

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

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

1.8.5 Performance Monitoring Counters and Threshold Crossing Alerts

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

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

Different performance monitoring count parameters are associated with different read points in a network. Figure 1-44 illustrates the performance monitoring read points that are useful in identifying DWDM circuit points of failure. Chapter 5, "Performance Monitoring," lists all PM parameters and provides block diagrams of signal entry points, exit points and interconnections between the individual circuit cards. Consult these specifications to determine which performance monitoring parameters are associated with the system points you want to monitor or provision with CTC or TL1. The monitoring points can vary according to your configuration.

Figure 1-44 Performance Monitoring Points on ONS DWDM

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

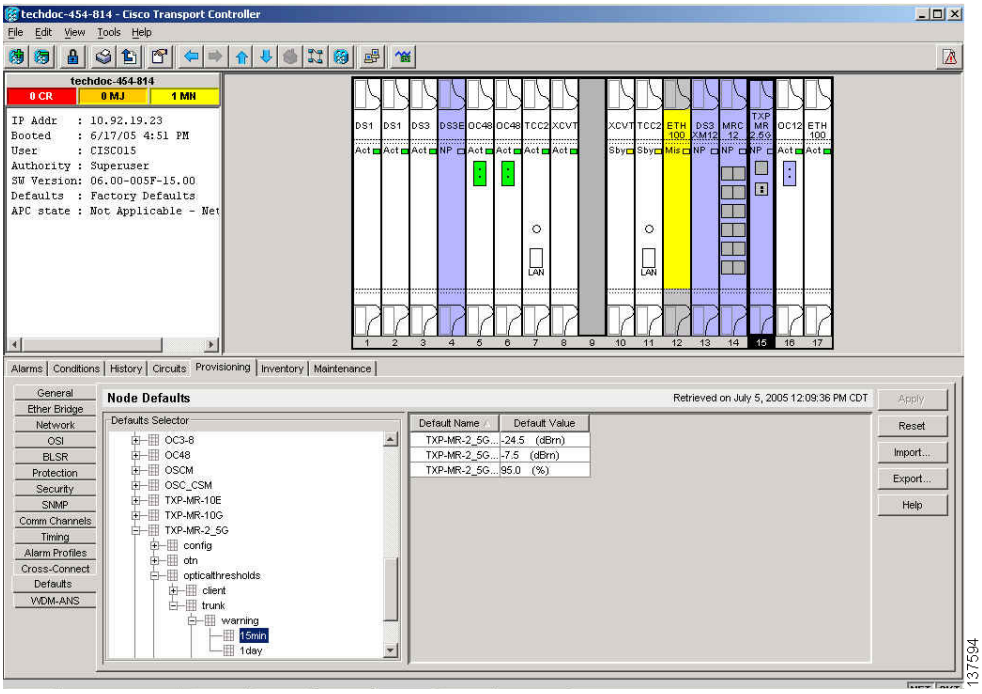
Select and complete the provisioning procedure below according to your network parameters.

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

Set Node Default BBE or SES Card Thresholds

Step 1 In node view, click the **Provisioning > Defaults** tabs (Figure 1-45).

Figure 1-45 Set Default BBE/SES Card Thresholds



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

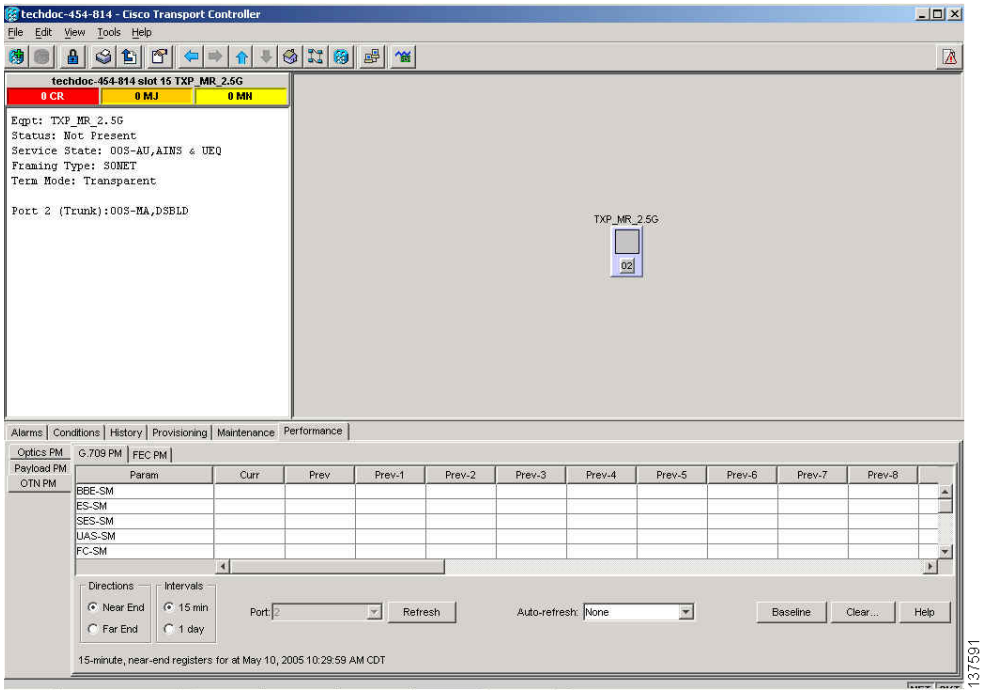
Complete the following procedure to provision BBE or SES PM thresholds in CTC for an individual TXP card.

Provision Individual Card BBE or SES Thresholds in CTC

Step 1 In node view, double-click the TXP_MR_2.5G card.
(In this example, other transponder and muxponder cards are also applicable, such as TXP_MR_10G, TXPP_MR_2.5G, and MXP_2.5G_10G.)

Step 2 Click the **Provisioning > OTN > G.709 Thresholds** tabs (Figure 1-46).

Figure 1-46 Provision Card BBE/SES Thresholds



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

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

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

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

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

Provision Card PM Thresholds Using TL1

Step 1 Open a TL1 command line.

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

```
set-th-{och,clnt}::aid:ctag::montype,thlev,,,[tmper];
```

Where:

- The modifier is och, as applicable to the trunk port.
- Montype can be:
  - BBE-PM
  - SES-PM
  - LBCL-MAX
- The parameter thlev is optional and indicates a threshold count value (the number of errors which must be exceeded before the threshold is crossed).

- The parameter tmper is optional and is an accumulation time period for performance counters, with possible values of 1-DAY, 1-HR, 1-MIN, 15-MIN, and RAW-DATA.

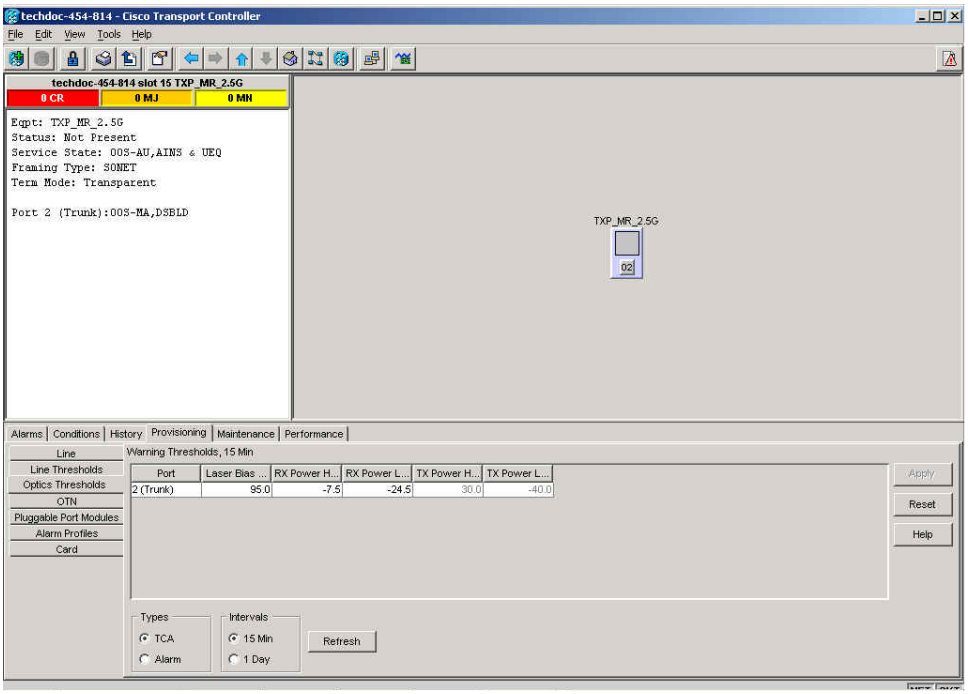
Note For a list of TL1 commands, refer to the *Cisco SONET TL1 Command Guide* .

Complete the following procedure to provision TCA thresholds in CTC.

Provision Optical TCA Thresholds

Step 1 In node view, click the **Provisioning** > **Optics Thresholds** tabs (Figure 1-47).

Figure 1-47 Provision Optical TCA Thresholds



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

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

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

1.8.6 Forward Error Correction

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

- BIT-EC—Bit errors corrected (BIT-EC) indicates the number of bit errors corrected in the DWDM trunk line during the PM time interval.
- UNC-WORDS—The number of uncorrectable words detected in the DWDM trunk line during the PM time interval.

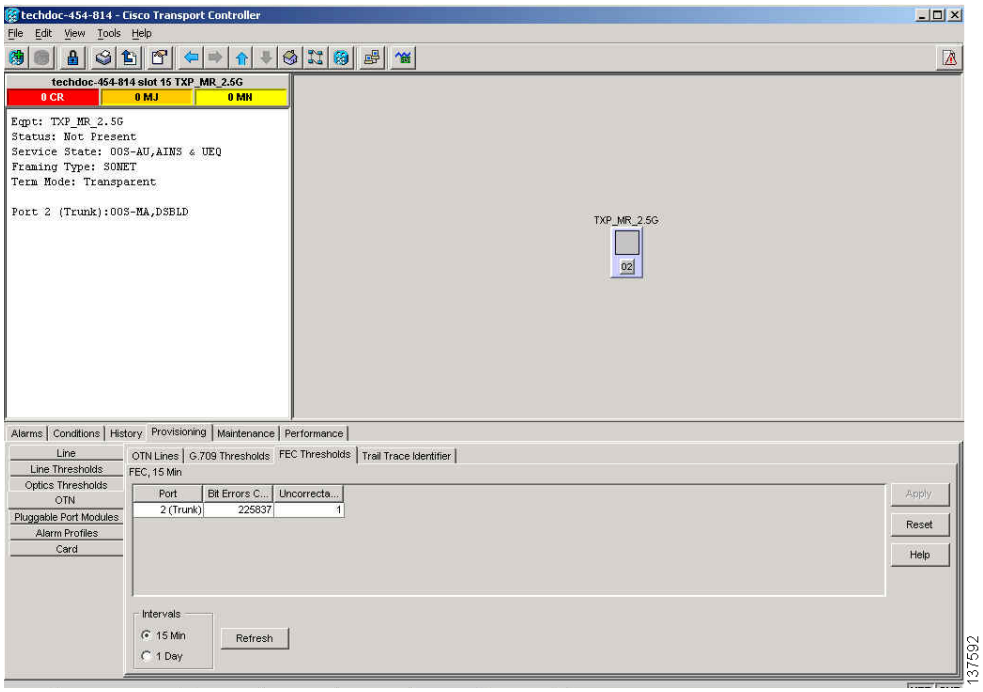
Complete the following procedure to provision BIT-EC and UNC-WORDS PM parameters for FEC.

Provision Card FEC Thresholds

Step 1 In node view, double-click the TXP_MR_2.5G card to open the card view.
(In this example, other transponder and muxponder cards are also applicable, such as TXP_MR_10G, TXPP_MR_2.5G, and MXP_2.5G_10G.)

Step 2 Click the **Provisioning > OTN > FEC Thresholds** tabs (Figure 1-48).

Figure 1-48 Provision Card FEC Thresholds



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

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

1.8.7 Sample Trouble Resolutions

Some sample trouble resolutions using performance monitoring and TCAs for isolating points of degrade are provided below.

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

Possible Cause The transponder input power is out of range.

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

Possible Cause There are dirty trunk connectors on the transponder.

Recommended Action Check the connector on the trunk port.

Possible Cause There is a degraded trunk patch-cord between the transponder and the DWDM port.

Recommended Action Check the patch-cord on the transponder DWDM port.

Possible Cause There are dirty client connectors on the channel add-drop (ADxC) transmit port or the demultiplexer (DMX) has crossed the near-end TCA.

Recommended Action Check the connector on the OCH port of the ADxC.

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

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

Symptom There is a BBE TCA on all transponders connected to a band add-drop card (ADxB).

Possible Cause The transponder input power is out of range.

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

Possible Cause There is a dirty connector on the 4MD port.

Recommended Action Check the connector on the drop port of the ADxB.

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

Recommended Action Check the connector on the drop port of the 4MD.

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

Recommended Action Check the patch-cord on the 4MD or AD1Bx.

Possible Cause There is a degraded patch-cord between the ADxB and the 4MD.

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

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

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

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

Symptom You have an LBC TCA on a single transponder.

Possible Cause The laser of the transponder is degrading.

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

1.9 Using CTC Diagnostics

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

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

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

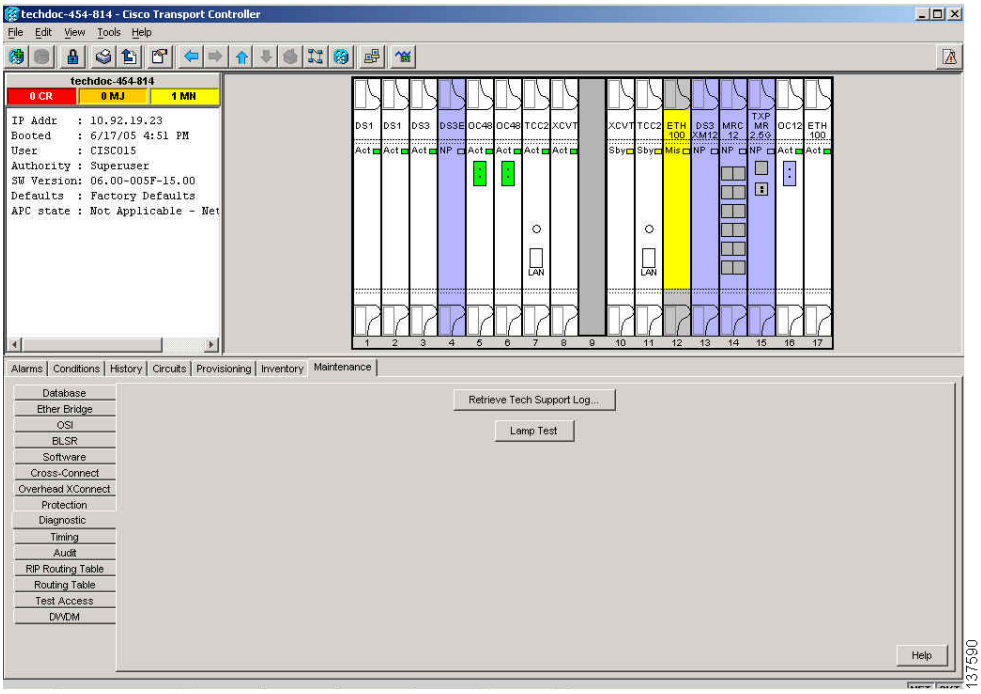
1.9.1 Card LED Lamp Tests

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

Verify General Card LED Operation

Step 1 In node view, click the **Maintenance > Diagnostic** tab (Figure 1-49).

Figure 1-49 CTC Node View Diagnostic Window



Step 2 Click **Lamp Test**.

Step 3 Watch to make sure all the port LEDs illuminate simultaneously for several seconds, with the following durations:

- For tri-color LEDs: three 5-second cycles
- For dual-color LEDs: one 5-second cycle and one 10-second cycle
- For the AIC or AIC-I: one 15-second cycle

Step 4 Click **OK** in the Lamp Test Run dialog box.

With the exceptions previously described, if an OC-N or DS-N LED does not light up, the LED is faulty. Return the defective card to Cisco through the RMA process. Contact Cisco Technical Support (1 800 553-2447).

Verify G-Series Ethernet or FC_MR-4 Card Port-Level LED Operation

Note G-Series and FC_MR-4 card-level LEDs illuminate during a lamp test, but the port-level LEDs do not.

Step 1 Complete the "Verify General Card LED Operation" procedure on page 1-113 to verify that card-level LEDs are operational.

Step 2 Use the following list of guidelines to physically test whether the G-Series Ethernet port LEDs are operating correctly. If the LED appears as described when the listed state is occurring for the port, the LED is considered to be functioning correctly.

- Clear port LED: Should only occur if there is a loss of receive link (such as a disconnected link or unplugged Gigabit Interface Converter, [GBIC]). An LOS alarm could be present on the port.
- Amber port LED: Should only occur if a port is disabled but the link is connected, or if the port is enabled and the link is connected but a transport failure is present. A TPTFAIL alarm can be present on the port.
- Green port LED: Should occur if the port is enabled and has no errors against it or traffic in it. Can also occur if the port is enabled, has no errors, and is running traffic proportionate to the blink rate. No traffic-affecting port alarms should be present.

Step 3 If you are unable to determine the port state, contact Cisco Technical Support (1 800 553-2447).

Verify E-Series and ML-Series Ethernet Card Port-Level LED Operation

Note E-Series and ML-Series card-level LEDs illuminate during a lamp test, but the port-level LEDs do not.

Note For information about the ML-Series card, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.

Step 1 Complete the "Verify General Card LED Operation" procedure on page 1-113 to verify that card-level LEDs are operational.

Step 2 Use the following list of guidelines to physically test whether the single E-Series or ML-Series Ethernet port LED is operating correctly. If the LED appears as described when the listed state is occurring for the port, the LED is considered to be functioning correctly.

- Clear port LED: Should only occur if there is a loss of receive link (such as a disconnected link or unplugged GBIC), or if traffic is flowing in one direction (either transmit or receive). A CARLOSS alarm could be present on the port.
- Amber port LED: Should only occur if the link is connected and the physical port is transmitting and receiving traffic.
- Green port LED: Should occur if the link is up and no traffic is flowing on the port.

Step 3 If you are unable to determine the port state, contact Cisco Technical Support (1 800 553-2447).

1.9.2 Retrieve Diagnostics File Button

When you click the Retrieve Diagnostics File button in the Maintenance window, CTC retrieves system data that can be off-loaded by a Maintenance or higher-level user to a local directory and sent to Technical Support for troubleshooting purposes. The diagnostics file is in machine language and is not human-readable, but can be used by Cisco Technical Support for problem analysis. Complete the following task to off-load the diagnostics file.

Note In addition to the machine-readable diagnostics file, the ONS 15454 also stores an audit trail of all system events such as user logins, remote logins, configuration, and changes. This audit trail is considered a record-keeping feature rather than a troubleshooting feature. Information about the feature is located in the "Maintain the Node" chapter of the *Cisco ONS 15454 Procedure Guide*.

Off-Load the Diagnostics File

Step 1 In the node view, click the **Maintenance > Diagnostic** tab (Figure 1-49).

Step 2 Click **Retrieve Tech Support Log**.

Step 3 In the Saving Diagnostic File dialog box, navigate to the directory (local or network) where you want to save the file.

Step 4 Enter a name in the File Name field.

You do not have to give the archive file a particular extension. It is a compressed file (gzip) that can be unzipped and read by Cisco Technical Support.

Step 5 Click **Save**.

The Get Diagnostics status window shows a progress bar indicating the percentage of the file being saved, then shows "Get Diagnostics Complete."

Step 6 Click **OK**.

1.9.3 Bidirectional Diagnostic Circuit

CTC provides a diagnostic bidirectional loopback circuit feature that uses pseudo-random bit sequence (PRBS) error detection to monitor standby path protection, BLSR, 1+1, or unprotected circuit path readiness.

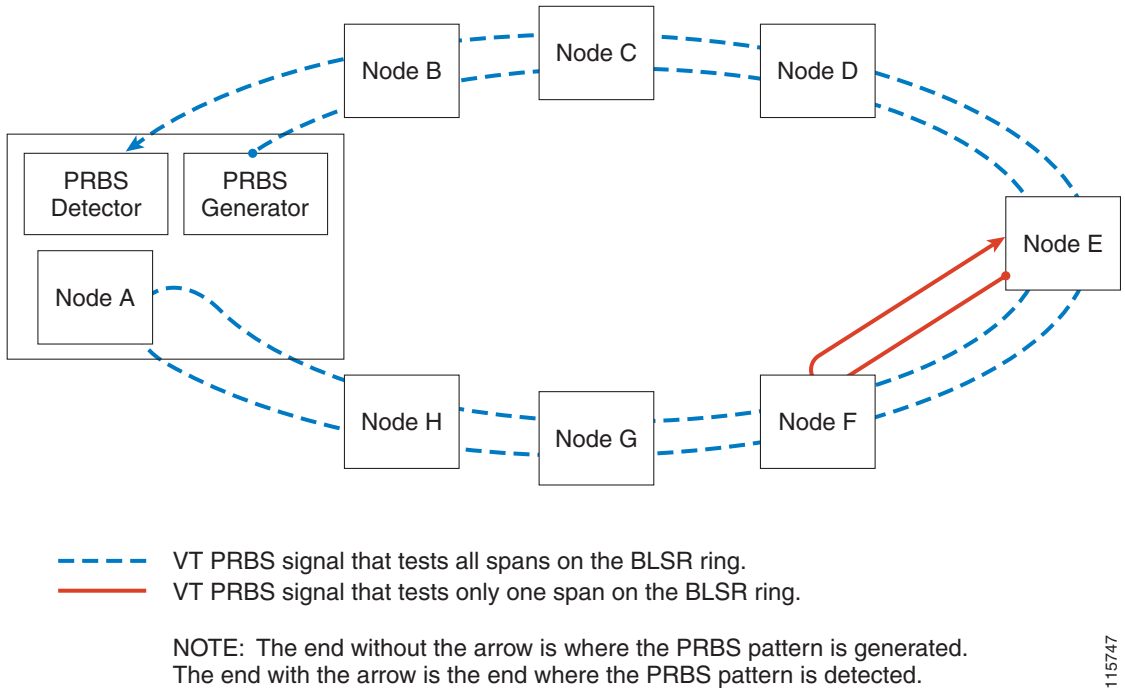
The diagnostic circuit is bidirectional and uses a single VT 1.5 in an STS. The circuit can traverse multiple nodes, but it must be carried by the same STS for the entire path. The circuit originates and ultimately destinates on the same node, but can be looped (by a hairpin circuit) through other nodes. After the circuit returns to the originating node, the signal result is detected and analyzed for errors by PRBS.

This type of circuit is created much the same way as a normal standby protection channel access (PCA) circuit, but is designated by checking the Diagnostic check box during circuit creation. A normal circuit uses line cards as the endpoints, but if a circuit is configured as a diagnostic, the endpoints are cross-connect cards.

Each card type utilizes the diagnostic feature differently. Standby electrical cards run PRBS tests to ensure signal path integrity. Optical cards do not run PRBS tests, but instead run ASIC tests to test card operability. Cross-connect cards verify the standby paths.

The diagnostic circuit can be configured for an end-to-end or multiple-node path layout, traversing the transmit and receive standby paths as shown in Figure 1-50.

Figure 1-50 CTC Node View Diagnostic Window



The maximum diagnostic circuit size is VT1.5, and the maximum quantity of available diagnostic circuits is one per node. (In other words, if you create a diagnostic VT within an STS, the remaining 27 VTs can still be provisioned, and they may also contain diagnostic circuits originating on other nodes.)

As with all bidirectional circuits, a diagnostic circuit can only be created if the same STS is available on each span the circuit traverses. When you use a bidirectional diagnostic that traverses one or more intermediate nodes, create or utilize an existing bidirectional circuit on each intermediate node. At the terminating node, you will need to create a hairpin loopback at the end of the PRBS source span to return the signal.

Note The diagnostic VT circuit does not raise a failure alarm if AIS-P or UNEQ-P is returned to the PRBS detector. In order to see an alarm indicating a failed diagnostic circuit, the circuit must be returned to the PRBS detector with a different payload than the generator sources and without the AIS-P or UNEQ-P conditions.

Create a Bidirectional Diagnostic Circuit

Step 1 Log into the node where you will create the diagnostic circuit. (For login instructions, refer to the "Connect the PC and Log into the GUI" chapter in the *Cisco ONS 15454 Procedure Guide*.)

Step 2 If you want to assign a name to the circuit source and destination ports before you create the circuit, refer to the task for assigning a name to a port in the "Create Circuits and VT Tunnels" chapter of the *Cisco ONS 15454 Procedure Guide*. If not, continue with Step 3.

Step 3 From the View menu, choose **Go to Network View**.

Step 4 Click the **Circuits** tab, then click **Create**.

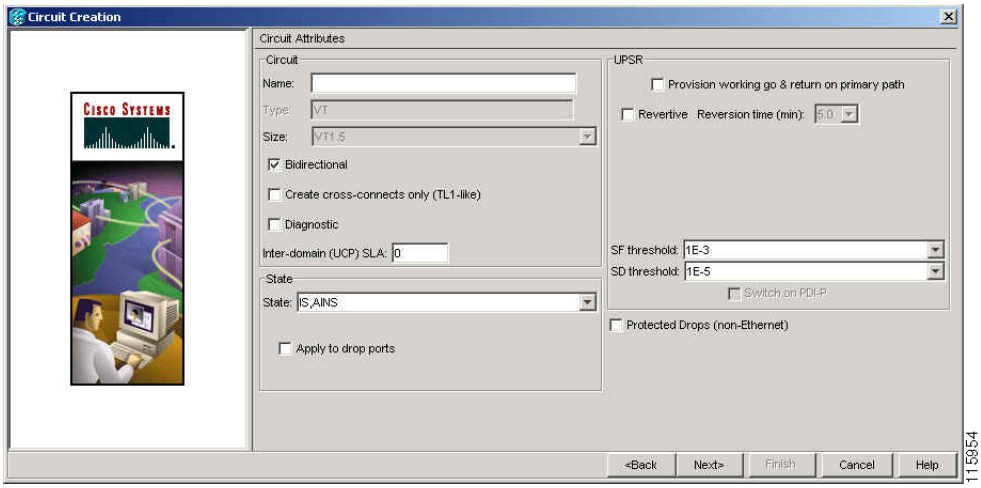
Step 5 In the Circuit Creation dialog box, complete the following fields:

- Circuit Type—Choose **VT**.
- Number of Circuits—Enter 1 (the maximum diagnostic circuit quantity available per STS).
- Auto-ranged—Uncheck the box. (This option is not applicable to diagnostic circuits.)

Step 6 Click **Next**.

Step 7 Define the circuit attributes in the Circuit Creation Dialog Box (Figure 1-51) using the following parameters:

Figure 1-51 Network View Circuit Creation Dialog Box



- Name—Assign a name to the circuit. The name can be alphanumeric and up to 48 characters, (including spaces). Circuit names should be 44 characters or less if you want the ability to create monitor circuits. If you leave the field blank, CTC assigns a default name to the circuit.
- Size—VT1.5 is the default. You cannot change it.
- Bidirectional—This is the default value. Leave it checked for this circuit.
- State—This option is not available when you check the Diagnostic option.
- Diagnostic—Check this box to create a diagnostic circuit.
- Apply to drop ports—Leave this box unchecked.
- Create cross-connects only (TL1-like)—Not applicable to diagnostic circuits.
- Inter-domain (UCP) SLA—Not applicable to diagnostic circuits.
- Protected Drops—Not applicable to diagnostic circuits.

Step 8 Click **Next**.

Step 9 In the Source area of the Circuit Creation pane, complete the following:

a. From the Node drop-down list, choose the node.

b. From the Slot drop-down list, choose **PRBS Generator**.

c. Click **Next**.

Step 10 In the Destination area of the Circuit Creation pane, complete the following:

a. From the Node drop-down list, choose the node. The only selectable item in the list is the node chosen as the source node.

b. From the Slot drop-down list, choose the slot where the span originates.

c. From the STS drop-down list, choose the STS.

d. From the VT drop-down list, choose the VT.

e. Click **Next**.

Step 11 Click **Finish**.

Step 12 In the Circuits window, verify that the new circuit(s) appear in the circuits list.

1.10 Restoring the Database and Default Settings

This section contains troubleshooting for node operation errors that require restoration of software data or the default node setup.

1.10.1 Restore the Node Database

Symptom One or more nodes does not function properly or has incorrect data.

Possible Cause Incorrect or corrupted node database.

Recommended Action Complete the procedures in the "Maintain the Node" chapter of the *Cisco ONS 15454 Procedure Guide*.

1.11 PC Connectivity Troubleshooting

This section contains information about system minimum requirements, supported platforms, browsers, and JREs for R6.0, and troubleshooting procedures for PC and network connectivity to the ONS 15454.

1.11.1 PC System Minimum Requirements

Workstations running CTC R6.0 for the ONS products on Windows platforms need to have the following minimum requirements:

- Pentium III or higher processor
- Processor speed of at least 700 MHz
- 256 MB or more of RAM
- 50 MB or more of available hard disk space
- 20 GB or larger hard drive

1.11.2 Sun System Minimum Requirements

Workstations running CTC R6.0 for the ONS products on Sun workstations need to have the following minimum requirements:

- UltraSPARC or faster processor
- 256 MB or more of RAM
- 50 MB or more of available hard disk space

1.11.3 Supported Platforms, Browsers, and JREs

Software R6.0 CTC supports the following platforms:

- Windows NT
- Windows 98
- Windows XP
- Windows 2000
- Solaris 8
- Solaris 9

Software R6.0 CTC supports the following browsers and JREs:

- Netscape 7 browser (PC or Solaris 8 or 9 with Java plug-in 1.4.2)
- PC platforms with Java plug-in 1.4.2
- Internet Explorer 6.0 browser (on PC platforms with Java plug-in 1.4.2)
- Mozilla 1.7 (Solaris only)

Note You can obtain browsers at the following URLs:
Internet Explorer: http://www.microsoft.com
Mozilla: http://www.mozilla.org/

Note The required JRE version is JRE 1.4.2.

Note JRE 1.4.2 for Windows and Solaris is available on R6.0 product CDs.

1.11.4 Unsupported Platforms and Browsers

Software R6.0 does not support the following platforms:

- Windows 95
- Solaris 2.5
- Solaris 2.6

Software R6.0 does not support the following browsers and JREs:

- Netscape 4.73 for Windows.
- Netscape 4.76 on Solaris is not supported.
- Netscape 7 on Solaris 8 or 9 is only supported with JRE 1.4.2

1.11.5 Unable to Verify the IP Configuration of Your PC

Symptom When connecting your PC to the ONS 15454, you are unable to successfully ping the IP address of your PC to verify the IP configuration.

Possible Cause The IP address was entered incorrectly.

Recommended Action Verify that the IP address used to ping the PC matches the IP address displayed when in the Windows IP Configuration information retrieved from the system. See the "Verify the IP Configuration of Your PC" procedure on page 1-121.

Possible Cause The IP configuration of your PC is not properly set.

Recommended Action Verify the IP configuration of your PC. Complete the "Verify the IP Configuration of Your PC" procedure on page 1-121. If this procedure is unsuccessful, contact your Network Administrator for instructions to correct the IP configuration of your PC.

Verify the IP Configuration of Your PC

Step 1 Open a DOS command window by selecting **Start > Run** from the Start menu.

Step 2 In the Open field, type **command** and then click **OK**. The DOS command window appears.

Step 3 At the prompt in the DOS window, type one of the following commands:

- For Windows 98, NT, 2000, and XP, type **ipconfig** and press the **Enter** key.

The Windows IP configuration information appears, including the IP address, subnet mask, and the default gateway.

Note The winipcfg command only returns the information above if you are on a network.

Step 4 At the prompt in the DOS window, type **ping** followed by the IP address shown in the Windows IP configuration information previously displayed.

Step 5 Press the **Enter** key to execute the command.

If the DOS window returns multiple (usually four) replies, the IP configuration is working properly.

If you do not receive a reply, your IP configuration might not be properly set. Contact your Network Administrator for instructions to correct the IP configuration of your PC.

1.11.6 Browser Login Does Not Launch Java

Symptom The message "Loading Java Applet" does not appear and the JRE does not launch during the initial login.

Possible Cause The PC operating system and browser are not properly configured.

Recommended Action Reconfigure the PC operating system java plug-in control panel and the browser settings. Complete the "Reconfigure the PC Operating System Java Plug-in Control Panel" procedure on page 1-122 and the "Reconfigure the Browser" procedure on page 1-122.

Reconfigure the PC Operating System Java Plug-in Control Panel

Step 1 From the Windows start menu, click **Settings > Control Panel**.

Step 2 If **Java Plug-in** does not appear, the JRE might not be installed on your PC:

a. Run the Cisco ONS 15454 software CD.

b. Open the *CD-drive*:\Windows\JRE folder.

c. Double-click the **j2re-1_4_2-win** icon to run the JRE installation wizard.

d. Follow the JRE installation wizard steps.

Step 3 From the Windows start menu, click **Settings > Control Panel**.

Step 4 In the Java Plug-in Control Panel window, double-click the **Java Plug-in 1.4.2** icon.

Step 5 Click the **Advanced** tab on the Java Plug-in Control Panel.

Step 6 Navigate to **C:\ProgramFiles\JavaSoft\JRE\1.4.2**.

Step 7 Select **JRE 1.4**.

Step 8 Click **Apply**.

Step 9 Close the Java Plug-in Control Panel window.

Reconfigure the Browser

Step 1 From the Start Menu, launch your browser application.

Step 2 If you are using Netscape Navigator:

a. On the Netscape Navigator menu bar, click the **Edit > Preferences** menus.

b. In the Preferences window, click the **Advanced > Proxies** categories.

c. In the Proxies window, click the **Direct connection to the Internet** check box and click **OK**.

d. On the Netscape Navigator menu bar, click the **Edit > Preferences** menus.

e. In the Preferences window, click the **Advanced > Cache** categories.

f. Confirm that the Disk Cache Folder field shows one of the following paths:

- For Windows 98/ME, **C:\ProgramFiles\Netscape\Communicator\cache**
- For Windows NT/2000/XP, **C:\ProgramFiles\Netscape***username***Communicator\cache**.

g. If the Disk Cache Folder field is not correct, click **Choose Folder**.

h. Navigate to the file listed in Step f, and click **OK**.

i. Click **OK** on the Preferences window and exit the browser.

Step 3 If you are using Internet Explorer:

a. On the Internet Explorer menu bar, click the **Tools > Internet Options** menus.

b. In the Internet Options window, click the **Advanced** tab.

c. In the Settings menu, scroll down to Java (Sun) and click the **Use Java 2 v1.4.2 for** *applet* **(requires restart)** check box.

d. Click **OK** in the Internet Options window and exit the browser.

Step 4 Temporarily disable any virus-scanning software on the computer. See the "1.12.4 Browser Stalls When Downloading CTC JAR Files From TCC2/TCC2P Card" section on page 1-128.

Step 5 Verify that the computer does not have two network interface cards (NICs) installed. If the computer does have two NICs, remove one.

Step 6 Restart the browser and log on to the ONS 15454.

1.11.7 Unable to Verify the NIC Connection on Your PC

Symptom When connecting your PC to the ONS 15454, you are unable to verify that the network interface card (NIC) connection is working properly because the link LED is not illuminated or flashing.

Possible Cause The Category-5 cable is not plugged in properly.

Recommended Action Confirm that both ends of the cable are properly inserted. If the cable is not fully inserted due to a broken locking clip, the cable should be replaced.

Possible Cause The Category-5 cable is damaged.

Recommended Action Ensure that the cable is in good condition. If in doubt, use a known-good cable. Often, cabling is damaged due to pulling or bending. (For information about installing cable, refer to the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15454 Procedure Guide*.)

Possible Cause Incorrect type of Category-5 cable is being used.

Recommended Action If connecting an ONS 15454 directly to your laptop, a PC, or a router, use a straight-through Category-5 cable. When connecting the ONS 15454 to a hub or a LAN switch, use a crossover Category-5 cable. For details on the types of Category-5 cables, see the "1.14.2.1 Crimp Replacement LAN Cables" section on page 1-148.

Possible Cause The NIC is improperly inserted or installed.

Recommended Action If you are using a Personal Computer Memory Card International Association (PCMCIA)-based NIC, remove and reinsert the NIC to make sure the NIC is fully inserted. (If the NIC is built into the laptop or PC, verify that the NIC is not faulty.)

Possible Cause The NIC is faulty.

Recommended Action Confirm that the NIC is working properly. If you have no issues connecting to the network (or any other node), then the NIC should be working correctly. If you have difficulty connecting a to the network (or any other node), then the NIC might be faulty and needs to be replaced.

1.11.8 Verify PC Connection to the ONS 15454 (ping)

Symptom The TCP/IP connection was established and then lost.

Possible Cause A lost connection between the PC and the ONS 15454.

Recommended Action Use a standard ping command to verify the TCP/IP connection between the PC and the ONS 15454 TCC2/TCC2P card. A ping command should work if the PC connects directly to the TCC2/TCC2P card or uses a LAN to access the TCC2/TCC2P card. Complete the "Ping the ONS 15454" procedure on page 1-124.

Ping the ONS 15454

Step 1 Display the command prompt:

a. If you are using a Microsoft Windows operating system, from the Start Menu choose **Run**, enter **command** in the Open field of the Run dialog box, and click **OK**.

b. If you are using a Sun Solaris operating system, from the Common Desktop Environment (CDE) click the **Personal Application tab** and click **Terminal.**

Step 2 For both the Sun and Microsoft operating systems, at the prompt enter:

ping *ONS-15454-IP-address*

For example:

```
ping 198.168.10.10
```

Step 3 If the workstation has connectivity to the ONS 15454, the ping is successful and displays a reply from the IP address. If the workstation does not have connectivity, a "Request timed out" message appears.

Step 4 If the ping is successful, it demonstrates that an active TCP/IP connection exists. Restart CTC.

Step 5 If the ping is not successful, and the workstation connects to the ONS 15454 through a LAN, check that the workstation's IP address is on the same subnet as the ONS node.

Step 6 If the ping is not successful and the workstation connects directly to the ONS 15454, check that the link light on the workstation's NIC is illuminated.

1.11.9 The IP Address of the Node is Unknown

Symptom The IP address of the node is unknown and you are unable to login.

Possible Cause The node is not set to the default IP address.

Recommended Action Leave one TCC2/TCC2P card in the shelf. Connect a PC directly to the remaining TCC2/TCC2P card and perform a hardware reset of the card. The TCC2/TCC2P card transmits the IP address after the reset to enable you to capture the IP address for login. Complete the "Retrieve Unknown Node IP Address" procedure on page 1-125.

Retrieve Unknown Node IP Address

Step 1 Connect your PC directly to the active TCC2/TCC2P card Ethernet port on the faceplate.

Step 2 Start the Sniffer application on your PC.

Step 3 Perform a hardware reset by pulling and reseating the active TCC2/TCC2P card.

Step 4 After the TCC2/TCC2P card completes resetting, it broadcasts its IP address. The Sniffer software on your PC will capture the IP address being broadcast.

1.12 CTC Operation Troubleshooting

This section contains troubleshooting procedures for CTC login or operation problems.

1.12.1 CTC Colors Do Not Appear Correctly on a UNIX Workstation

Symptom When running CTC on a UNIX workstation, the colors do not appear correctly. For example, both major and minor alarms appear in the same color.

Possible Cause When running in 256-color mode on a UNIX workstation, color-intensive applications such as Netscape might use all of the colors.

Recommended Action CTC requires a full 24-color palette to run properly. When logging into CTC on a UNIX workstation, run as many colors as your adapter will support. In addition, you can use the -install or the -ncols 32 command line options to limit the number of colors that Netscape uses. Complete the "Limit Netscape Colors" procedure on page 1-125. If the problem persists after limiting Netscape colors, exit any other color-intensive applications in use.

Limit Netscape Colors

Step 1 Close the current session of Netscape.

Step 2 Launch Netscape from the command line by entering:

`netscape -install` (installs Netscape colors for Netscape use)

or

`netscape -ncols 32` (limits Netscape to 32 colors so that if the requested color is not available, Netscape chooses the closest color option)

1.12.2 Unable to Launch CTC Help After Removing Netscape

Symptom After removing Netscape and running CTC using Internet Explorer, you are unable to launch CTC Help and receive an "MSIE is not the default browser" error message.

Possible Cause Loss of association between browser and Help files.

Recommended Action When the CTC software and Netscape are installed, the Help files are associated with Netscape by default. When you remove Netscape, the Help files are not automatically associated with Internet Explorer as the default browser. Reset Internet Explorer as the default browser so that CTC associates the Help files to the correct browser. Complete the "Reset Internet Explorer as the Default Browser for CTC" procedure on page 1-126 to associate the CTC Help files to the correct browser.

Reset Internet Explorer as the Default Browser for CTC

Step 1 Open the Internet Explorer browser.

Step 2 From the menu bar, click **Tools > Internet Options**. The Internet Options window appears.

Step 3 In the Internet Options window, click the **Programs** tab.

Step 4 Click the **Internet Explorer should check to see whether it is the default browser** check box.

Step 5 Click **OK**.

Step 6 Exit any and all open and running CTC and Internet Explorer applications.

Step 7 Launch Internet Explorer and open a new CTC session. You should now be able to access the CTC Help.

1.12.3 Unable to Change Node View to Network View

Symptom When activating a large, multinode BLSR from Software R3.2 to Software R3.3, some of the nodes appear grayed out. Logging into the new CTC, the user is unable to change node view to network view on any and all nodes, from any workstation. This is accompanied by an "Exception occurred during event dispatching: java.lang.OutOfMemoryError" in the java window.

Possible Cause The large, multinode BLSR requires more memory for the graphical user interface (GUI) environment variables.

Recommended Action Set the system or user CTC_HEAP environment variable to increase the memory limits. Complete the "Set the CTC_HEAP and CTC_MAX_PERM_SIZE_HEAP Environment Variables for Windows" procedure on page 1-127 or the "Set the CTC_HEAP and CTC_MAX_PERM_SIZE_HEAP Environment Variables for Solaris" procedure on page 1-128 to enable the CTC_HEAP variable change.

Note This problem typically affects large networks where additional memory is required to manage large numbers of nodes and circuits.

Set the CTC_HEAP and CTC_MAX_PERM_SIZE_HEAP Environment Variables for Windows

Note Before proceeding with the following steps, ensure that your system has a minimum of 1 GB of RAM. If your system does not have a minimum of 1 GB of RAM, contact the Cisco Technical Assistance Center (TAC).

Step 1 Close all open CTC sessions and browser windows.

Step 2 From the Windows **Start** menu, choose **Control Panel > System**.

Step 3 In the System Properties window, click the **Advanced** tab.

Step 4 Click the **Environment Variables** button to open the Environment Variables window.

Step 5 Click the **New** button under the System variables field.

Step 6 Type `CTC_HEAP` in the Variable Name field.

Step 7 Type `512` in the Variable Value field, and then click the **OK** button to create the variable.

Step 8 Again, click the **New** button under the System variables field.

Step 9 Type `CTC_MAX_PERM_SIZE_HEAP` in the Variable Name field.

Step 10 Type `128` in the Variable Value field, and then click the **OK** button to create the variable.

Step 11 Click the **OK** button in the Environment Variables window to accept the changes.

Step 12 Click the **OK** button in the System Properties window to accept the changes.

Set the CTC_HEAP and CTC_MAX_PERM_SIZE_HEAP Environment Variables for Solaris

Step 1 From the user shell window, kill any CTC sessions and broswer applications.

Step 2 In the user shell window, set the environment variables to increase the heap size.

Example

The following example shows how to set the environment variables in the C shell:

```
% setenv CTC_HEAP 512
% setenv CTC_MAX_PERM_SIZE_HEAP 128
```

1.12.4 Browser Stalls When Downloading CTC JAR Files From TCC2/TCC2P Card

Symptom The browser stalls or hangs when downloading a CTC Java archive (JAR) file from the TCC2/TCC2P card.

Possible Cause McAfee VirusScan software might be interfering with the operation. The problem occurs when the VirusScan Download Scan is enabled on McAfee VirusScan 4.5 or later.

Recommended Action Disable the VirusScan Download Scan feature. Complete the "Disable the VirusScan Download Scan" procedure on page 1-128.

Disable the VirusScan Download Scan

Step 1 From the Windows Start menu, choose **Programs > Network Associates > VirusScan Console**.

Step 2 Double-click the **VShield** icon listed in the VirusScan Console dialog box.

Step 3 Click **Configure** on the lower part of the Task Properties window.

Step 4 Click the **Download Scan** icon on the left of the System Scan Properties dialog box.

Step 5 Uncheck the **Enable Internet download scanning** check box.

Step 6 Click **Yes** when the warning message appears.

Step 7 Click **OK** in the System Scan Properties dialog box.

Step 8 Click **OK** in the Task Properties window.

Step 9 Close the McAfee VirusScan window.

1.12.5 CTC Does Not Launch

Symptom CTC does not launch; usually an error message appears before the login window appears.

Possible Cause The Netscape browser cache might point to an invalid directory.

Recommended Action Redirect the Netscape cache to a valid directory. Complete the "Redirect the Netscape Cache to a Valid Directory" procedure on page 1-129.

Redirect the Netscape Cache to a Valid Directory

Step 1 Launch Netscape.

Step 2 Open the **Edit** menu.

Step 3 Choose **Preferences**.

Step 4 Under the Category column on the left side, expand the **Advanced** category and choose the **Cache** tab.

Step 5 Change your disk cache folder to point to the cache file location.

The cache file location is usually C:\ProgramFiles\Netscape\Users*yourname*\cache. The *yourname* segment of the file location is often the same as the user name.

1.12.6 Slow CTC Operation or Login Problems

Symptom You experience slow CTC operation or have problems logging into CTC.

Table 1-3 describes the potential cause of the symptom and the solution.

Table 1-3 Slow CTC Operation or Login Problems

Possible Problem	Solution
The CTC cache file might be corrupted or might need to be replaced.	Search for and delete cache files. This operation forces the ONS 15454 to download a new set of Java archive (JAR) files to your computer hard drive. Complete the "Delete the CTC Cache File Automatically" procedure on page 1-130 or the "Delete the CTC Cache File Manually" procedure on page 1-131.
Insufficient heap memory allocation.	Increase the heap size if you are using CTC to manage more than 50 nodes concurrently. See the "Set the CTC_HEAP and CTC_MAX_PERM_SIZE_HEAP Environment Variables for Windows" procedure on page 1-127 or the "Set the CTC_HEAP and CTC_MAX_PERM_SIZE_HEAP Environment Variables for Solaris" procedure on page 1-128. **Note** To avoid network performance issues, Cisco recommends managing a maximum of 50 nodes concurrently with CTC. To manage more than 50 nodes, Cisco recommends using Cisco Transport Manager (CTM). Cisco does not recommend running multiple CTC sessions when managing two or more large networks.

Delete the CTC Cache File Automatically

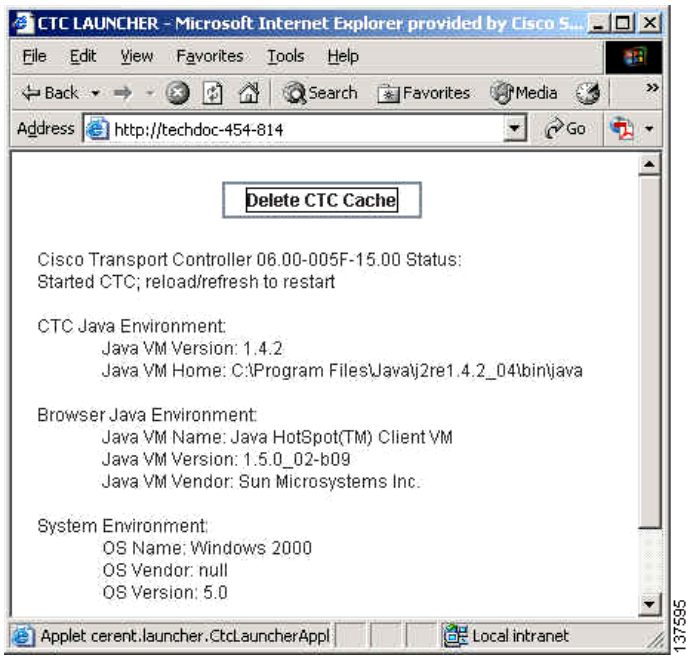
Caution All running sessions of CTC must be halted before deleting the CTC cache. Deleting CTC cache might cause any CTC running on this system to behave in an unexpected manner.

Step 1 Enter an ONS 15454 IP address into the browser URL field. The initial browser window shows a **Delete CTC Cache** button.

Step 2 Close all open CTC sessions and browser windows. The PC operating system does not allow you to delete files that are in use.

Step 3 Click **Delete CTC Cache** on the initial browser window to clear the CTC cache. Figure 1-52 shows the Delete CTC Cache window.

Figure 1-52 Deleting the CTC Cache



Delete the CTC Cache File Manually

Caution All running sessions of CTC must be halted before deleting the CTC cache. Deleting the CTC cache might cause any CTC running on this system to behave in an unexpected manner.

Step 1 To delete the JAR files manually, from the Windows Start menu choose **Search > For Files or Folders**.

Step 2 Enter **ctc*.jar** or **cms*.jar** in the Search for files or folders named field in the Search Results dialog box and click **Search Now**.

Step 3 Click the **Modified** column in the Search Results dialog box to find the JAR files that match the date when you downloaded the files from the TCC2/TCC2P.

Step 4 Highlight the files and press the keyboard **Delete** key.

Step 5 Click **Yes** in the Confirm dialog box.

1.12.7 Node Icon is Gray on CTC Network View

Symptom The CTC network view shows one or more node icons as gray in color and without a node name.

Possible Cause Different CTC releases do not recognize each other.

Recommended Action Correct the core version build as described in the "1.12.10 Different CTC Releases Do Not Recognize Each Other" section on page 1-134.

Possible Cause Username and password do not match.

Recommended Action Correct the username and password as described in the "1.12.11 Username or Password Do Not Match" section on page 1-135.

Possible Cause No IP connectivity between nodes.

Recommended Action Usually accompanied by Ethernet-specific alarms. Verify the Ethernet connections as described in the "1.12.16 Ethernet Connections" section on page 1-137.

Possible Cause A lost DCC connection.

Recommended Action Usually accompanied by an embedded operations channel (EOC) alarm. Clear the EOC alarm and verify the DCC connection as described in the "EOC" alarm.

1.12.8 CTC Cannot Launch Due to Applet Security Restrictions

Symptom The error message "Unable to launch CTC due to applet security restrictions" appears after you enter the IP address in the browser window.

Possible Cause You are logging into a node running CTC Software R4.0 or earlier. Releases earlier than R4.1 require a modification to the java.policy file so that CTC JAR files can be downloaded to the computer. The modified java.policy file might not exist on the computer.

Recommended Action Install the software CD for the release of the node you are logging into. Run the CTC Setup Wizard (double-click **Setup.exe**). Choose **Custom installation**, then choose the Java Policy option. For additional information, refer to the CTC installation information in the "Connect the PC and Log into the GUI" chapter of the *Cisco ONS 15454 Procedure Guide*. If the software CD is not available, you must manually edit the java.policy file on your computer. Complete the "Manually Edit the java.policy File" procedure on page 1-132.

Manually Edit the java.policy File

Step 1 Search your computer for java.policy file and open it with a text editor (Notepad or Wordpad).

Step 2 Verify that the end of this file has the following lines:

```
    // Insert this into the system-wide or a per-user java.policy file.
// DO NOT OVERWRITE THE SYSTEM-WIDE POLICY FILE--ADD THESE LINES!

grant codeBase "http://*/fs/LAUNCHER.jar {
```

```
permission java.security.AllPermission;
    };
```

Step 3 If these five lines are not in the file, enter them manually.

Step 4 Save the file and restart Netscape.

CTC should now start correctly.

Step 5 If the error message is still reported, save the java.policy file as **.java.policy**. On Win98/2000/XP PCs, save the file to the C:\Windows folder. On Windows NT 4.0 or later PCs, save the file to all of the user folders on that PC, for example, C:\Winnt\profiles\joeuser.

1.12.9 Java Runtime Environment Incompatible

Symptom The CTC application does not run properly.

Possible Cause The compatible Java 2 JRE is not installed.

Recommended Action The JRE contains the Java virtual machine, runtime class libraries, and Java application launcher that are necessary to run programs written in the Java programming language. The ONS 15454 CTC is a Java application. A Java application, unlike an applet, cannot rely completely on a web browser for installation and runtime services. When you run an application written in the Java programming language, you need the correct JRE installed. The correct JRE for each CTC software release is included on the Cisco ONS 15454 software CD and on the Cisco ONS 15454 documentation CD. Complete the "Launch CTC to Correct the Core Version Build" procedure on page 1-134. If you are running multiple CTC software releases on a network, the JRE installed on the computer must be compatible with the different software releases. Table 1-4 shows JRE compatibility with ONS 15454 software releases.

Table 1-4 JRE Compatibility

Software Release	JRE 1.2.2 Compatible	JRE 1.3 Compatible	JRE 1.4 Compatible
ONS 15454 R2.2.1 and earlier	Yes	No	No
ONS 15454 R2.2.2	Yes	Yes	No
ONS 15454 R3.0	Yes	Yes	No
ONS 15454 R3.1	Yes	Yes	No
ONS 15454 R3.2	Yes	Yes	No
ONS 15454 R3.3	Yes	Yes	No
ONS 15454 R3.4	No	Yes	No
ONS 15454 **Note** R4.0 Software R4.0 notifies you if an earlier JRE version is running on your PC or UNIX workstation.	No	Yes	No
ONS 15454 R4.1	No	Yes	No

Table 1-4 JRE Compatibility (continued)

Software Release	JRE 1.2.2 Compatible	JRE 1.3 Compatible	JRE 1.4 Compatible
ONS 15454 R4.5	No	Yes	No
ONS 15454 R4.6	No	Yes	Yes
ONS 15454 R4.7	No	Yes	Yes
ONS 15454 R5.0	No	Yes	Yes
ONS 15454 R6.0	No	No	Yes

Launch CTC to Correct the Core Version Build

Step 1 Exit the current CTC session and completely close the browser.

Step 2 Start the browser.

Step 3 Enter the ONS 15454 IP address of the node that reported the alarm. This can be the original IP address you logged in with or an IP address other than the original.

Step 4 Log into CTC. The browser downloads the JAR file from CTC.

1.12.10 Different CTC Releases Do Not Recognize Each Other

Symptom Different CTC releases do not recognize each other. This situation is often accompanied by the INCOMPATIBLE-SW alarm.

Possible Cause The software loaded on the connecting workstation and the software on the TCC2/TCC2P card are incompatible.

Recommended Action This occurs when the TCC2/TCC2P software is upgraded but the PC has not yet upgraded the compatible CTC JAR file. It also occurs on login nodes with compatible software that encounter other nodes in the network that have a newer software version. Complete the "Launch CTC to Correct the Core Version Build" procedure on page 1-134.

Note Remember to always log into the ONS node with the latest CTC core version first. If you initially log into an ONS node running a CTC core version of 2.2 or lower and then attempt to log into another ONS node in the network running a higher CTC core version, the lower version node does not recognize the new node.

Launch CTC to Correct the Core Version Build

Step 1 Exit the current CTC session and completely close the browser.

Step 2 Start the browser.

Step 3 Enter the ONS 15454 IP address of the node that reported the alarm. This can be the original IP address you logged on with or an IP address other than the original.

Step 4 Log into CTC. The browser downloads the JAR file from CTC.

1.12.11 Username or Password Do Not Match

Symptom A username/password mismatch often occurs concurrently with a NOT-AUTHENTICATED alarm.

Possible Cause The username or password entered does not match the information stored in the TCC2/TCC2P.

Recommended Action All ONS nodes must have the same username and password created to display every ONS node in the network. You can also be locked out of certain ONS nodes on a network if your username and password were not created on those specific ONS nodes. For initial login to the ONS 15454, enter the CISCO15 user name in capital letters and click **Login** and use the password "otbu+1," which is case-sensitive. Complete the "Verify Correct Username and Password" procedure on page 1-135. If the node has been configured for Radius authentication (new in R6.0), the username and password are verified against the Radius server database rather than the security information in the local node database. For more information about Radius security, refer to the "Security" chapter in the *Cisco ONS 15454 Reference Manual*.

Verify Correct Username and Password

Step 1 Ensure that your keyboard Caps Lock key is not turned on and affecting the case-sensitive entry of the username and password.

Step 2 Contact your system administrator to verify the username and password.

Step 3 Call Cisco Technical Support (1 800 553-2447) to have them enter your system and create a new user name and password.

1.12.12 No IP Connectivity Exists Between Nodes

Symptom No IP connectivity exists between nodes. The nodes have a gray icon. This problem is usually accompanied by alarms.

Possible Cause A lost Ethernet connection.

Recommended Action Usually is accompanied by Ethernet-specific alarms. Verify the Ethernet connections as described in the "1.12.16 Ethernet Connections" section on page 1-137.

1.12.13 DCC Connection Lost

Symptom DCC connection is lost. The node usually has alarms and the nodes in the network view have a gray icon. This symptom is usually accompanied by an EOC alarm.

Possible Cause A lost DCC connection.

Recommended Action Usually accompanied by an EOC alarm. Clear the EOC alarm and verify the DCC connection as described in the "EOC" alarm.

1.12.14 "Path in Use" Error When Creating a Circuit

Symptom While creating a circuit, you get a "Path in Use" error that prevents you from completing the circuit creation.

Possible Cause Another user has already selected the same source port to create another circuit.

Recommended Action CTC does not remove a card or port from the available list until a circuit is completely provisioned. If two users simultaneously select the same source port to create a circuit, the first user to complete circuit provisioning gets use of the port. The other user gets the "Path in Use" error. Cancel the circuit creation and start over, or click **Back** until you return to the initial circuit creation window. The source port that was previously selected no longer appears in the available list because it is now part of a provisioned circuit. Select a different available port and begin the circuit creation process again.

1.12.15 Calculate and Design IP Subnets

Symptom You cannot calculate or design IP subnets on the ONS 15454.

Possible Cause The IP capabilities of the ONS 15454 require specific calculations to properly design IP subnets.

Recommended Action Cisco provides a free online tool to calculate and design IP subnets.
Go to http://www.cisco.com/pcgi-bin/Support/IpSubnet/home.pl.
For information about ONS 15454 IP capability, refer to the "Management Network Connectivity" chapter in the *Cisco ONS 15454 Reference Manual*.

1.12.16 Ethernet Connections

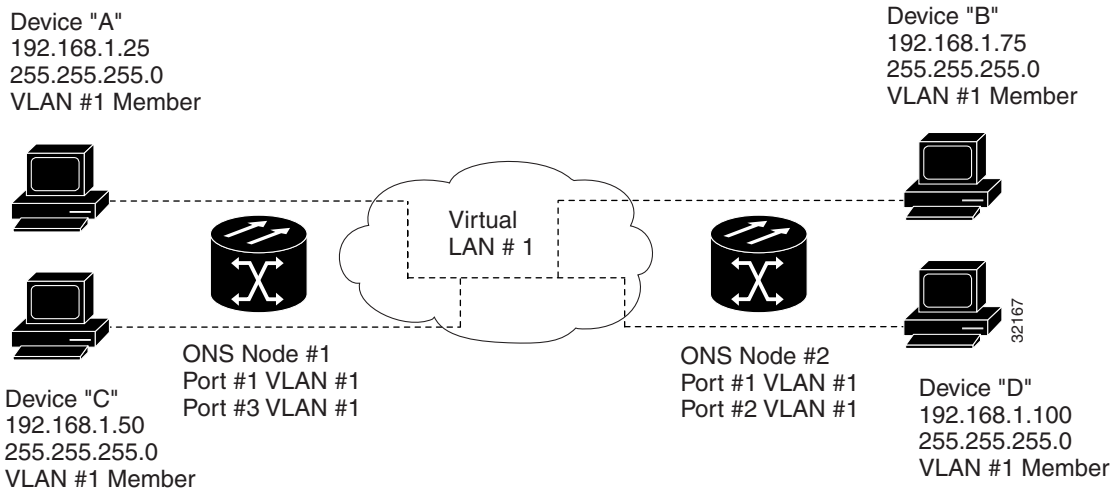
Symptom Ethernet connections appear to be broken or are not working properly.

Possible Cause Improperly seated connections.

Possible Cause Incorrect connections.

Recommended Action You can fix most connectivity problems in an Ethernet network by following a few guidelines. See Figure 1-53 when using the steps in the "Verify Ethernet Connections" procedure on page 1-137.

Figure 1-53 Ethernet Connectivity Reference



Verify Ethernet Connections

Step 1 Verify that the alarm filter is turned OFF.

Step 2 Check for SONET and DWDM alarms on the STS that carries the VLAN Ethernet circuit. Clear any alarms by looking them up in Chapter 2, "Alarm Troubleshooting."

Step 3 Check for Ethernet-specific alarms. Clear any raised alarms by looking up that alarm in Chapter 2, "Alarm Troubleshooting."

Step 4 Verify that the ACT LED on the Ethernet card is green.

Step 5 Verify that Ports 1 and 3 on ONS 15454 #1 and Ports 1 and 2 on ONS 15454 #2 have green link-integrity LEDs illuminated.

Step 6 If no green link-integrity LED is illuminated for any of these ports:

- **a.** Verify physical connectivity between the ONS 15454s and the attached device.
- **b.** Verify that the ports are enabled on the Ethernet cards.
- **c.** Verify that you are using the proper Ethernet cable and that it is wired correctly, or replace the cable with a known-good Ethernet cable.

d. Check the status LED on the Ethernet card faceplate to ensure the card booted up properly. This LED should be steady green. If necessary, remove and reinsert the card and allow it to reboot.

e. It is possible that the Ethernet port is functioning properly but the link LED itself is broken. Complete the "Verify General Card LED Operation" procedure on page 1-113.

Step 7 Verify connectivity between device A and device C by pinging between these locally attached devices. Complete the "1.11.8 Verify PC Connection to the ONS 15454 (ping)" procedure on page 1-124. If the ping is unsuccessful:

a. Verify that device A and device C are on the same IP subnet.

b. Open the Ethernet card in CTC card view and click the **Provisioning > VLAN** tab to verify that both Port 1 and Port 3 on the card are assigned to the same VLAN.

c. If a port is not assigned to the correct VLAN, click that port column in the VLAN row and set the port to Tagged or Untag. Click **Apply**.

Step 8 Repeat Step 7 for devices B and D.

Step 9 Verify that the Ethernet circuit that carries VLAN #1 is provisioned and that ONS 15454 #1 and ONS 15454 #2 ports also use VLAN #1.

1.12.17 VLAN Cannot Connect to Network Device from Untag Port

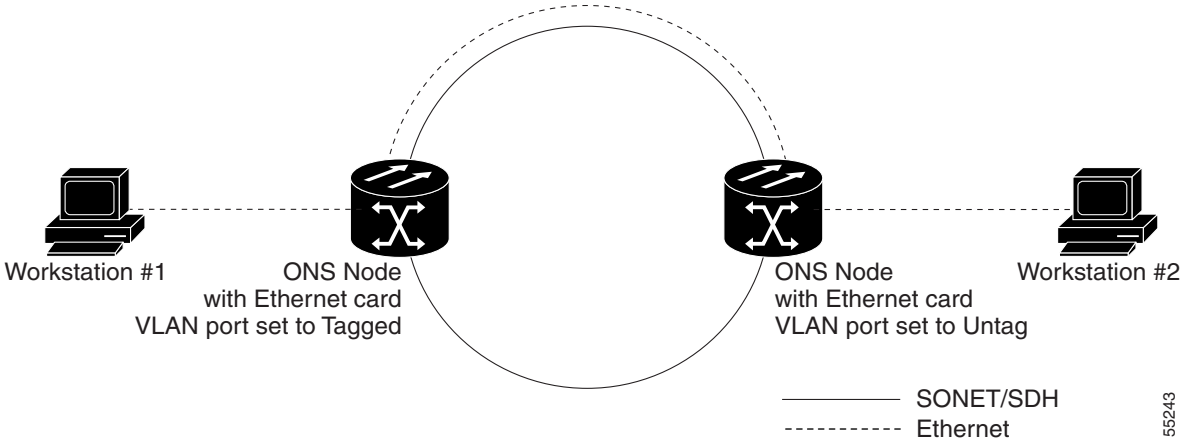
Symptom Networks that have a VLAN with one ONS 15454 Ethernet card port set to Tagged and one ONS 15454 Ethernet card set to Untag might have difficulty implementing Address Resolution Protocol (ARP) for a network device attached to the Untag port (Figure 1-54). They might also see a higher than normal runt packets count at the network device attached to the Untag port. This symptom/limitation also exists when ports within the same card or ports within the same chassis are put on the same VLAN, with a mix of tagged and untagged.

Possible Cause The Tagged ONS 15454 adds the IEEE 802.1Q tag and the Untag ONS 15454 removes the Q-tag without replacing the bytes. The NIC of the network device categorizes the packet as a runt and drops the packet.

Possible Cause Dropped packets can also occur when ARP attempts to match the IP address of the network device attached to the Untag port with the physical MAC address required by the network access layer.

Recommended Action The solution is to set both ports in the VLAN to Tagged to stop the stripping of the 4 bytes from the data packet and prevent the NIC card in the network access device from recognizing the packet as a runt and dropping it. Network devices with IEEE 802.1Q-compliant NIC cards accept the tagged packets. Network devices with non IEEE 802.1Q compliant NIC cards still drop these tagged packets. The solution might require upgrading network devices with non-IEEE 802.1Q compliant NIC cards to IEEE 802.1Q compliant NIC cards. You can also set both ports in the VLAN to Untag, but you will lose IEEE 802.1Q compliance.

Figure 1-54 VLAN with Ethernet Ports at Tagged and Untag

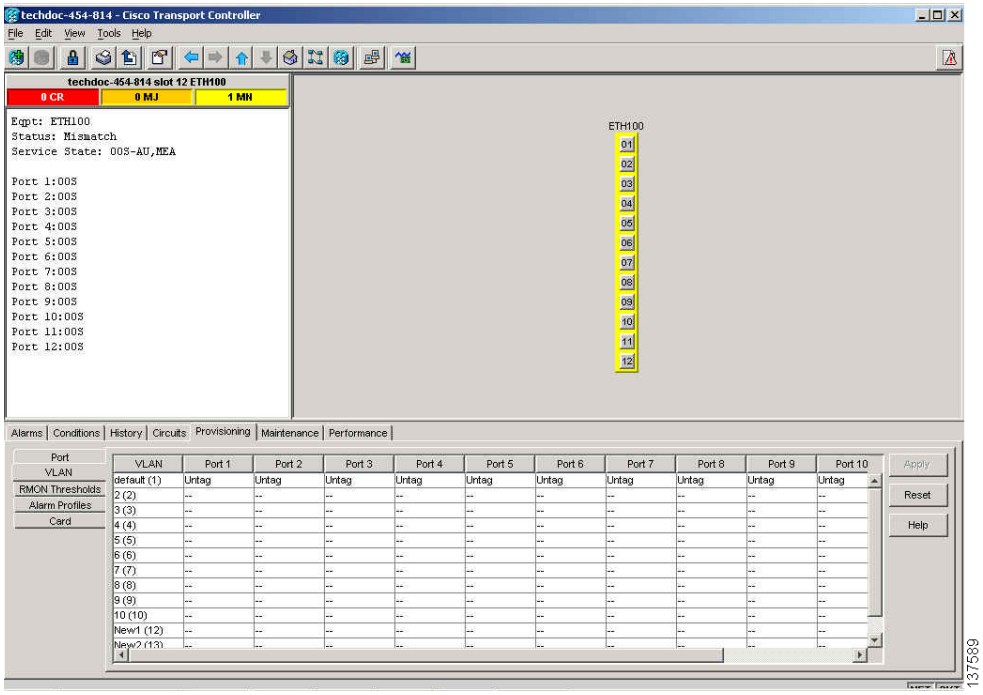


Change VLAN Port Tagged and Untag Settings

Step 1 Display the CTC card view for the Ethernet card involved in the problem VLAN.

Step 2 Click the **Provisioning > Ether VLAN** tab (Figure 1-55).

Figure 1-55 Configuring VLAN Membership for Individual Ethernet Ports



Step 3 If the port is set to **Tagged**, continue to look at other cards and their ports in the VLAN until you find the port that is set to **Untag**.

Step 4 At the VLAN port set to **Untag**, click the port and choose **Tagged**.

Note The attached external devices must recognize IEEE 802.1Q VLANs.

Step 5 After each port is in the appropriate VLAN, click **Apply**.

1.13 Circuits and Timing

This section provides solutions to circuit creation and reporting errors, as well as common timing reference errors and alarms.

1.13.1 OC-N Circuit Transitions to Partial State

Symptom An automatic or manual transition of a circuit from one state to another state results in the OOS-PARTIAL status, which indicates that not all OC-N connections in the circuit are in the IS-NR service state.

Possible Cause During a manual transition, CTC cannot communicate with one of the nodes or one of the nodes is on a version of software that does not support the new state model.

Recommended Action Repeat the manual transition operation. If the partial state persists, determine which node in the circuit is not changing to the desired state. Complete the "View the State of OC-N Circuit Nodes" procedure on page 1-140. Log into the circuit node that did not change to the desired state and determine the version of software. If the software on the node is Software R3.3 or earlier, upgrade the software. Refer to the *Cisco ONS 15454 Software Upgrade Guide* for software upgrade procedures.

Note If the node software cannot be upgraded to R4.0, the partial state condition can be avoided by using only the circuit state supported in the earlier software version.

Possible Cause During an automatic transition, some path-level defects and/or alarms were detected on the circuit.

Possible Cause One end of the circuit is not properly terminated.

Recommended Action Determine which node in the circuit is not changing to the desired state. Complete the "View the State of OC-N Circuit Nodes" procedure on page 1-140. Log onto the circuit node that did not change to the desired state and examine the circuit for path-level defects, improper circuit termination, or alarms. See Chapter 2, "Alarm Troubleshooting," for procedures to clear alarms. Refer to the "Manage Circuits" chapter in the *Cisco ONS 15454 Procedure Guide* for instructions to change circuit configuration settings. Resolve and clear the defects and/or alarms on the circuit node and verify that the circuit transitions to the desired state.

View the State of OC-N Circuit Nodes

Step 1 Click the **Circuits** tab.

Step 2 From the Circuits tab list, select the circuit with the *_PARTIAL status condition.

Step 3 Click **Edit**. The Edit Circuit window appears.

Step 4 In the Edit Circuit window, click the **State** tab (if you are viewing a SONET circuit).

The State tab window lists the Node, End A, End B, CRS Admin State, and CRS Service State for each of the nodes in the circuit.

1.13.2 AIS-V on DS3XM-6 or DS3XM-12 Unused VT Circuits

Symptom An incomplete circuit path causes an AIS.

Possible Cause The port on the reporting node is in-service but a node upstream on the circuit does not have an OC-N port in service.

Recommended Action An AIS-V indicates that an upstream failure occurred at the virtual tributary (VT) layer. AIS-V alarms also occur on DS3XM-6 and DS3XM-12 VT circuits that are not carrying traffic and on stranded bandwidth. Complete the "Clear AIS-V on DS3XM-6 or DS3XM-12 Unused VT Circuits" procedure on page 1-141.

Clear AIS-V on DS3XM-6 or DS3XM-12 Unused VT Circuits

Step 1 Determine the affected port.

Step 2 Record the node ID, slot number, port number, or VT number.

Step 3 Create a unidirectional VT circuit from the affected port back to itself, such as Source node/Slot 2/Port 2/VT 13 cross connected to Source node/Slot 2/Port 2/VT 13.

Step 4 Uncheck the **Bidirectional** check box in the circuit creation window.

Step 5 Give the unidirectional VT circuit an easily recognizable name, such as delete me.

Step 6 Display the DS3XM-6 card in CTC card view. Click the **Maintenance > DS1** tab.

Step 7 Locate the VT that is reporting the alarm (for example, DS3 #2, DS1 #13).

Step 8 From the Loopback Type list, choose **Facility (Line)** and click **Apply**.

Step 9 Click **Circuits**.

Step 10 Find the one-way circuit you created in Step 3. Select the circuit and click **Delete**. Do not check any check boxes.

Step 11 Click **Yes** in the Delete Confirmation dialog box.

Step 12 Display the DS3XM-6 or DS3XM-12 card in CTC card view. Click **Maintenance > DS1**.

Step 13 Locate the VT in Facility (line) Loopback.

Step 14 From the Loopback Type list, choose **None** and then click **Apply**.

Step 15 Click the **Alarms** tab and verify that the AIS-V alarms have cleared.

Step 16 Repeat this procedure for all the AIS-V alarms on the DS3XM-6 or DS3XM-12 cards.

1.13.3 Circuit Creation Error with VT1.5 Circuit

Symptom You receive an "Error while finishing circuit creation. Unable to provision circuit. Unable to create connection object at *node_name*" message when trying to create a VT1.5 circuit in CTC.

Possible Cause You might have run out of bandwidth on the VT cross-connect matrix at the ONS 15454 indicated in the error message.

Recommended Action The matrix has a maximum capacity of 336 bidirectional VT1.5 cross-connects. Certain configurations exhaust VT capacity with less than 336 bidirectional VT1.5s in a BLSR or less than 224 bidirectional VT1.5s in a unidirectional path switched ring (path protection) or 1+1 protection group. Refer to the *Cisco ONS 15454 Reference Manual* for more information.

1.13.4 Unable to Create Circuit From DS-3 Card to DS3XM-6 or DS3XM-12 Card

Symptom You cannot create a circuit from a DS-3 card to a DS3XM-6 or DS3XM-12 card.

Possible Cause A DS-3 card and a DS3XM-6 or DS3XM-12 card have different functions.

Recommended Action A DS3XM-6 card converts each of its six DS-3 interfaces into 28 DS-1s for cross-connection through the network. The DS3XM-12 converts each of its 12 interfaces into up to 48 DS-1s. Thus, you can create a circuit from a DS3XM-6 or DS3XM-12 card to a DS-1 card, but not from a DS3XM card to a DS-3 card. These differences are evident in the STS path overhead. The DS-3 card uses asynchronous mapping for DS-3, which is indicated by the C2 byte in the STS path overhead that has a hex code of 04. A DS3XM-6 or DS3XM-12 has a VT payload with a C2 hex value of 02.

Note You can find instructions for creating circuits in the "Create Circuits and VT Tunnels" chapter of the *Cisco ONS 15454 Procedure Guide*.

1.13.5 DS-3 Card Does Not Report AIS-P From External Equipment

Symptom A DS3-12, DS3N-12, DS3-12E, or DS3N-12E card does not report STS AIS-P from the external equipment/line side.

Possible Cause The card is functioning as designed.

Recommended Action This card terminates the port signal at the backplane so STS AIS-P is not reported from the external equipment/line side. DS3-12, DS3N-12, DS3-12E, and DS3N-12E cards have DS3 header monitoring functionality, which allows you to view PM on the DS3 path. Nevertheless, you cannot view AIS-P on the STS path. For more information about the PM capabilities of the DS3-12, DS3N-12, DS3-12E or DS3N-12E cards, go to Chapter 5, "Performance Monitoring."

1.13.6 OC-3 and DCC Limitations

Symptom Limitations to OC-3 and DCC usage.

Possible Cause OC-3 and DCC have limitations for the ONS 15454.

Recommended Action For an explanation of OC-3 and DCC limitations, refer to the "Circuits and Tunnels" chapter in the *Cisco ONS 15454 Reference Manual*.

1.13.7 ONS 15454 Switches Timing Reference

Symptom Timing references switch when one or more problems occur.

Possible Cause The optical or BITS input is receiving loss of signal (LOS), loss of frame (LOF), or AIS alarms from its timing source.

Possible Cause The optical or building integrated timing supply (BITS) input is not functioning.

Possible Cause The synchronization status messaging (SSM) message is set to do not use for synchronization (DUS).

Possible Cause SSM indicates a Stratum 3 or lower clock quality.

Possible Cause The input frequency is off by more than 15 ppm.

Possible Cause The input clock wanders and has more than three slips in 30 seconds.

Possible Cause A bad timing reference existed for at least two minutes.

Recommended Action The ONS 15454 internal clock operates at a Stratum 3E level of accuracy. This gives the ONS 15454 a free-running synchronization accuracy of +/– 4.6 ppm and a holdover stability of less than 255 slips in the first 24 hours or 3.7 x 10^{-7}/day, including temperature. ONS 15454 free-running synchronization relies on the Stratum 3 internal clock. Over an extended time period, using a higher quality Stratum 1 or Stratum 2 timing source results in fewer timing slips than a lower quality Stratum 3 timing source.

1.13.8 Holdover Synchronization Alarm

Symptom The clock is running at a different frequency than normal and the "HLDOVRSYNC" alarm appears.

Possible Cause The last reference input has failed.

Recommended Action The clock is running at the frequency of the last known-good reference input. This alarm is raised when the last reference input fails. See the "HLDOVRSYNC" alarm on page 2-116 for a detailed description.

Note The ONS 15454 supports holdover timing per Telcordia GR-436 when provisioned for external (BITS) timing.

1.13.9 Free-Running Synchronization Mode

Symptom The clock is running at a different frequency than normal and the "FRNGSYNC" alarm appears.

Possible Cause No reliable reference input is available.

Recommended Action The clock is using the internal oscillator as its only frequency reference. This occurs when no reliable, prior timing reference is available. See the "FRNGSYNC" condition on page 2-105 for a detailed description.

1.13.10 Daisy-Chained BITS Not Functioning

Symptom You are unable to daisy chain the BITS sources.

Possible Cause Daisy-chained BITS sources are not supported on the ONS 15454.

Recommended Action Daisy-chained BITS sources cause additional wander buildup in the network and are therefore not supported. Instead, use a timing signal generator to create multiple copies of the BITS clock and separately link them to each ONS 15454.

1.13.11 Blinking STAT LED after Installing a Card

Symptom After installing a card, the STAT LED blinks continuously for more than 60 seconds.

Possible Cause The card cannot boot because it failed the Power On Shelf Test (POST) diagnostics.

Recommended Action The blinking STAT LED indicates that POST diagnostics are being performed. If the LED continues to blink more than 60 seconds, the card has failed the POST diagnostics test and has failed to boot. If the card has truly failed, an "EQPT" alarm is raised against the slot number with an "Equipment Failure" description. Check the alarm tab for this alarm to appear for the slot where the card was installed. To attempt recovery, remove and reinstall the card and observe the card boot process. If the card fails to boot, replace the card. Complete the "Physically Replace a Traffic Card" procedure on page 2-243.

Error Message

```
Above paragraph is not clear. Why we need to complete Air Filter and Fan Procedure
if the card is failed. If this applicable for FAN and AIR Filter, rephrase the
sentence
```

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 "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-231. For more information, refer to the "Maintain the Node" chapter in the *Cisco ONS 15454 Procedure Guide*.

1.14 Fiber and Cabling

This section explains problems typically caused by cabling connectivity errors. It also includes instructions for crimping Category-5 cable and lists the optical fiber connectivity levels.

1.14.1 Bit Errors Appear for a Traffic Card

Symptom A traffic card has multiple bit errors.

Possible Cause Faulty cabling or low optical-line levels.

Recommended Action Bit errors on line (traffic) cards usually originate from cabling problems or low optical-line levels. The errors can be caused by synchronization problems, especially if pointer justification (PJ) errors are reported. Moving cards into different error-free slots will isolate the cause. Use a test set whenever possible because the cause of the errors could be external cabling, fiber, or external equipment connecting to the ONS 15454. Troubleshoot low optical levels using the "1.14.2 Faulty Fiber-Optic Connections" section on page 1-145.

1.14.2 Faulty Fiber-Optic Connections

Symptom A line card has multiple SONET/DWDM alarms and/or signal errors.

Possible Cause Faulty fiber-optic connections.

Recommended Action Faulty fiber-optic connections can be the source of SONET/DWDM alarms and signal errors. Complete the "Verify Fiber-Optic Connections" procedure on page 1-146.

Possible Cause Faulty Category-5 cables.

Recommended Action Faulty Category-5 cables can be the source of SONET/DWDM alarms and signal errors. Complete the "1.14.2.1 Crimp Replacement LAN Cables" section on page 1-148.

Possible Cause Faulty GBICs.

Recommended Action Faulty GBICs can be the source of SONET/DWDM alarms and signal errors. See the "1.14.2.2 Replace Faulty GBIC, SFP, or XFP Connectors" section on page 1-149.

Warning **Invisible laser radiation may be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments.** Statement 272

Warning **Laser radiation presents an invisible hazard, so personnel should avoid exposure to the laser beam. Personnel must be qualified in laser safety procedures and must use proper eye protection before working on this equipment.** Statement 300

Verify Fiber-Optic Connections

Step 1 Ensure that a single-mode fiber connects to the ONS 15454 OC-N card.

Note SM or SM Fiber should be printed on the fiber span cable. ONS 15454 OC-N cards do not use multimode fiber.

Step 2 Ensure that the connector keys on the SC fiber connector are properly aligned and locked.

Step 3 Check that the single-mode fiber power level is within the specified range:

- **a.** Remove the 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 fiber with the fiber-optic power meter.
- **d.** Verify that the power meter is set to the appropriate wavelength for the OC-N card being tested (either 1310 nm or 1550 nm depending on the specific card).
- **e.** Verify that the power level falls within the range specified for the card if it is an OC-N card; see the "1.14.3 OC-N Card Transmit and Receive Levels" section on page 1-154.

Step 4 If the power level falls below the specified range for the OC-N card:

- **a.** Clean or replace the fiber patch cords. Clean the fiber according to site practice or, if none exists, follow the procedure in the "Maintain the Node" chapter in the *Cisco ONS 15454 Procedure Guide*. If possible, do this for the OC-N card you are working on and the far-end card.
- **b.** Clean the optical connectors on the card. Clean the connectors according to site practice or, if none exists, follow the procedure in the "Maintain the Node" chapter in the *Cisco ONS 15454 Procedure Guide*. If possible, do this for the OC-N card you are working on and the far-end card.
- **c.** Ensure that the far-end transmitting card is not an ONS intermediate-range (IR) card when an ONS long-range (LR) card is appropriate.

  IR cards transmit a lower output power than LR cards.
- **d.** Replace the far-end transmitting OC-N card to eliminate the possibility of a degrading transmitter on this OC-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 procedures in the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-231. For more information, refer to the "Maintain the Node" chapter in the *Cisco ONS 15454 Procedure Guide*.

e. If the power level still falls below the specified range with the replacement fibers and replacement card, check for one of these three factors that attenuate the power level and affect link loss (LL):
   - Excessive fiber distance; single-mode fiber attenuates at approximately 0.5 dB/km.
   - Excessive number or fiber connectors; connectors take approximately 0.5 dB each.
   - Excessive number of fiber splices; splices take approximately 0.5 dB each.

Note These are typical attenuation values. Refer to the specific product documentation for the actual values or use an optical time domain reflectometer (OTDR) to establish precise link loss and budget requirements.

Step 5 If no power level shows on the fiber, the fiber is bad or the transmitter on the OC-N card failed.

a. Check that the Tx and Rx fibers are not reversed. LOS and EOC alarms normally accompany reversed Tx and Rx fibers. Switching reversed Tx and Rx fibers clears the alarms and restores the signal.

b. Clean or replace the fiber patch cords. Clean the fiber according to site practice or, if none exists, follow the procedure in the "Maintain the Node" chapter in the *Cisco ONS 15454 Procedure Guide*. If possible, do this for the OC-N card you are working on and the far-end card.

c. Retest the fiber power level.

d. If the replacement fiber still shows no power, replace the OC-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 procedures in the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-231. For more information, refer to the "Maintain the Node" chapter in the *Cisco ONS 15454 Procedure Guide*.

Step 6 If the power level on the fiber is above the range specified for the card, ensure that an ONS LR card is not being used when an ONS IR card is appropriate.

LR cards transmit a higher output power than IR cards. When used with short runs of fiber, an LR transmitter is too powerful for the receiver on the receiving OC-N card.

Receiver overloads occur when maximum receiver power is exceeded.

Tip To prevent overloading the receiver, use an attenuator on the fiber between the ONS OC-N card transmitter and the receiver. Place the attenuator on the receive transmitter of the ONS OC-N cards. Refer to the attenuator documentation for specific instructions.

Tip Most fiber has text printed on only one of the two fiber strands. Use this to identify which fiber is connected to Tx and which fiber is connected to Rx.

1.14.2.1 Crimp Replacement LAN Cables

You can crimp your own LAN cables for use with the ONS 15454. Use a cross-over cable when connecting an ONS 15454 to a hub, LAN modem, or switch, and use a LAN cable when connecting an ONS 15454 to a router or workstation. Use Category-5 cable RJ-45 T-568B, Color Code (100 Mbps), and a crimping tool. Figure 1-56 shows the wiring of an RJ-45 connector. Figure 1-57 shows a LAN cable layout, and Table 1-5 shows the cable pinouts. Figure 1-58 shows a cross-over cable layout, and Table 1-6 shows the cross-over pinouts.

Figure 1-56 RJ-45 Pin Numbers

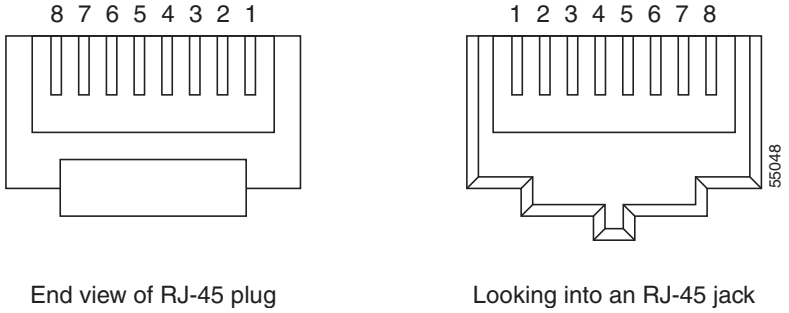


Figure 1-57 LAN Cable Layout

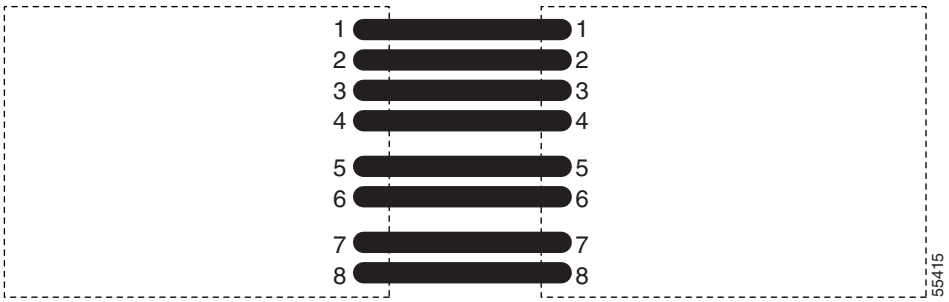


Table 1-5 LAN Cable Pinout

Pin	Color	Pair	Name	Pin
1	white/orange	2	Transmit Data +	1
2	orange	2	Transmit Data –	2
3	white/green	3	Receive Data +	3
4	blue	1	—	4
5	white/blue	1	—	5
6	green	3	Receive Data –	6
7	white/brown	4	—	7
8	brown	4	—	8

Figure 1-58 Cross-Over Cable Layout

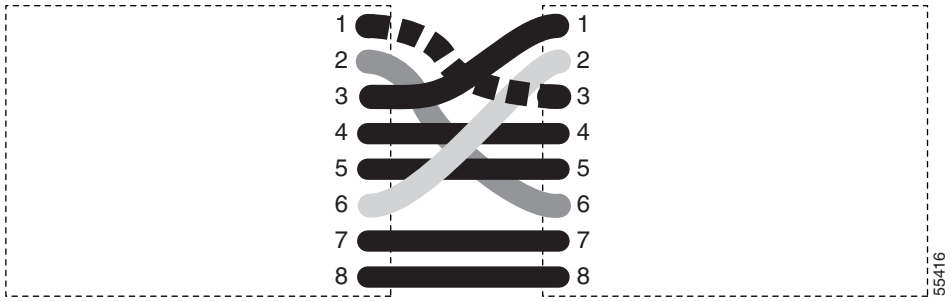


Table 1-6 Cross-Over Cable Pinout

Pin	Color	Pair	Name	Pin
1	white/orange	2	Transmit Data +	3
2	orange	2	Transmit Data –	6
3	white/green	3	Receive Data +	1
4	blue	1	—	4
5	white/blue	1	—	5
6	green	3	Receive Data –	2
7	white/brown	4	—	7
8	brown	4	—	8

Note Odd-numbered pins always connect to a white wire with a colored stripe.

1.14.2.2 Replace Faulty GBIC, SFP, or XFP Connectors

GBICs and Small Form-factor Pluggables (SFP or XFP) are hot-swappable and can be installed or removed while the card or shelf assembly is powered and running.

Warning **Class 1 laser product.** Statement 1008

Warning **Invisible laser radiation may be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments.** Statement 272

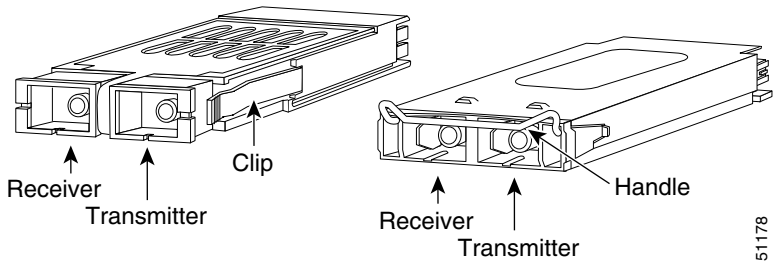
GBICs and SFPs/XFPs are input/output devices that plug into a Gigabit Ethernet card to link the port with the fiber-optic network. The type of GBIC or SFP determines the maximum distance that the Ethernet traffic can travel from the card to the next network device. For a description of GBICs and SFPs and their capabilities refer to the *Cisco ONS 15454 Reference Manual*.

Note GBICs and SFPs must be matched on either end by type: SX to SX, LX to LX, or ZX to ZX.

Note All versions of G1K-4 cards support coarse wavelength division multiplexing (CWDM) GBICs.

GBICs are available in two different models. One GBIC model has two clips (one on each side of the GBIC) that secure the GBIC in the slot on the E1000-2-G, G-Series, or G1K-4 card. The other model has a locking handle. Both models are shown in Figure 1-59.

Figure 1-59 GBICs



For a list of available GBICs and SFPs/XFPs for Ethernet cards and SAN (FC_MR-4) cards, refer to the Ethernet Cards" chapter in the *Cisco ONS 15454 Reference Manual*. For a list of available SFPs/XFPs for TXP and MXP cards, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Note GBICs are very similar in appearance. Check the GBIC label carefully before installing it.

Remove GBIC, SFP, or XFP Connectors

Warning **Invisible laser radiation may be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments.** Statement 272

Step 1 Disconnect the network fiber cable from the GBIC SC connector or XFP or SFP LC duplex connector.

Step 2 Release the GBIC or SFP/XFP from the slot by simultaneously squeezing the two plastic tab on each side.

Step 3 Slide the GBIC or SFP/XFP out of the Gigabit Ethernet module slot. A flap closes over the GBIC or SFP slot to protect the connector on the Gigabit Ethernet card.

Install a GBIC or SFP/XFP Device

Warning **Class 1 laser product.** Statement 1008

Warning **Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard.** Statement 1056

Note G-Series cards manufactured before August 2003 do not support DWDM GBICs. G1K-4 cards compatible with DWDM GBICs have a Common Language Equipment Identification (CLEI) code of WM5IRWPCAA.

Note All versions of G1K-4 cards support coarse wavelength division multiplexing (CWDM) GBICs.

Note GBICs, SFPs, and XFPs are hot-swappable and can therefore be installed/removed while the card/shelf assembly is powered and running.

Step 1 Remove the GBIC, SFP, or XFP from its protective packaging.

Step 2 Check the label to verify that the GBIC, SFP, or XFP is the correct type for your network.

Table 1-7 shows the available GBICs.

Note The GBICs are very similar in appearance. Check the GBIC label carefully before installing it.

Table 1-7 Available GBICs

GBIC	Associated Cards	Application	Fiber	Product Number
1000BaseSX	E1000-2-G G1K-4	Short reach	Multimode fiber up to 550 m long	15454E-GBIC-SX=
1000BaseLX	E1000-2-G G1K-4	Long reach	Single-mode fiber up to 5 km long	15454E-GBIC-LX=
1000BaseZX	G1K-4	Extra long reach	Single-mode fiber up to 70 km long	15454E-GBIC-ZX=
	FC_MR-4	Long reach	Single-mode fiber, 1310 nm	ONS-GX-2FC-SML=
	FC_MR-4	Intermediate reach	Multimode fiber, 850 nm	ONS-GX-2FC-MMI=

Table 1-8 shows the available SFPs and XFPs.

Table 1-8 Available SFPs and XFPs

SFP/XFP	Associated Cards	Application	Fiber	Product Number
1000BaseSX	ML1000-2	Short reach	Multimode fiber up to 550 m long	15454E-SFP-LC-SX=
1000BaseLX		Long reach	Single-mode fiber up to 5 km long	15454E-SFP-LC-LX=
1000BaseFX	ML100X-8	Short reach	1310 nm multimode fiber up to 2 km long	ONS-SE-100-FX
1000BaseLX-10		Intermediate reach	1310 nm, single mode fiber, up to 15 km long	ONS-SE-100-LX10
OC-48 SR	MRC-12	Short reach	1310-nm single-mode fiber up to 2 km long	ONS-SI-2G-S1
OC-48 IR1		Intermediate reach	1310-nm single-mode fiber, up to 15 km long	ONS-SI-2G-I1
OC-48 LR1		Long reach	1310-nm single-mode fiber up to 40 km long	ONS-SI-2G-L1
OC-48 LR2		Long reach	1550-nm single-mode fiber up to 80 km long	ONS-SI-2G-L2
OC-48 LR2 DWDM		Long reach	1530.33 to 1560.61 nm single-mode fiber up to 120 km long	ONS-SC-2G-30.3 through ONS-SC-2G-60.6
OC-3/OC-12 IR1 dual rate		Intermediate reach	1310-nm single-mode fiber up to 15 km long	ONS-SI-622-I1
OC-12 LR1		Long reach	1310-nm single-mode fiber up to 40 km long	ONS-SI-622-L1
OC-12 LR2		Long reach	1550-nm single-mode fiber up to 80 km long	ONS-SI-622-L2
OC-12 CWDM		Long reach	1470 to 1610 nm single-mode fiber up to 80 km long	ONS-SE-622-1470 through ONS-SE-622-1610
OC-3 IR1		Intermediate reach	1310-nm single-mode fiber up to 15 km long	ONS-SI-155-I1
OC-3 LR1	MRC-12 (cont.)	Long reach	1310-nm single-mode fiber up to 40 km long	ONS-SI-155-L1
OC-3 LR2		Long reach	1550-nm single-mode fiber up to 80 km long	ONS-SI-155-L2
OC-3 CWDM		Long reach	1470 to 1610 nm single-mode fiber up to 80 km long	ONS_SE-155-1470 through ONS-SE-155-1610
OC-192 SR1	OC192SR1/ STM64IO Short Reach[1]	Short reach	1310-nm single-mode fiber up to 10 km long	ONS-XC-10G-S1

Table 1-8 Available SFPs and XFPs (continued)

SFP/XFP	Associated Cards	Application	Fiber	Product Number
OC-192 SR1, IR1, LR2	OC192/ STM64 Any Reach[1]	Short reach	1310-nm single-mode fiber up to 10 km long	ONS-XC-10G-S1
		Intermediate reach	1550-nm single-mode fiber up to 15 km long	ONS-XC-10G-I2
		Long reach	1550-nm single-mode fiber up to 80 km long	ONS-XC-10G-L2

1. CTC refers to this card as OC192-XFP

Note Before you install SFPs on the MRC-12 card, refer to the MRC-12 card information in the *Cisco ONS 15454 Reference Manual* for bandwidth restrictions based on the port where you install the SFP and the cross-connect card being used.

Step 3 Verify the type of GBIC, SFP, or XFP you are using:

- If you are using a GBIC with clips, go to Step 4.
- If you are using a GBIC with a handle, go to Step 5.
- If you are using an SFP or XFP, go to Step 6.

Step 4 For GBICs with clips:

a. Grip the sides of the GBIC with your thumb and forefinger and insert the GBIC into the slot on the card.

Note GBICs are keyed to prevent incorrect installation.

b. Slide the GBIC through the flap that covers the opening until you hear a click. The click indicates the GBIC is locked into the slot.

c. When you are ready to attach the network fiber-optic cable, remove the protective plug from the GBIC, save the plug for future use, then plug the fiber connector into the GBIC.

Step 5 For GBICs with a handle:

a. Remove the protective plug from the SC-type connector.

b. Grip the sides of the GBIC with your thumb and forefinger and insert the GBIC into the slot on the card.

c. Lock the GBIC into place by closing the handle down. The handle is in the correct closed position when it does not obstruct access to an SC-type connector.

d. Slide the GBIC through the cover flap until you hear a click.

The click indicates that the GBIC is locked into the slot.

e. When you are ready to attach the network fiber-optic cable, remove the protective plug from the GBIC, save the plug for future use, then plug the fiber connector into the GBIC.

Step 6 For SFPs and XFPs:

a. Plug the LC duplex connector of the fiber into a Cisco-supported SFP or XFP.

b. If the new SFP or XFP has a latch, close the latch over the cable to secure it.

c. Plug the cabled SFP or XFP into the card port until it clicks.

SFPs and XFPs must be provisioned in CTC. If you installed a multirate PPM, refer to the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15454 Procedure Guide* for instructions to provision it. (Single-rate XFPs do not need to be provisioned in CTC.)

1.14.3 OC-N Card Transmit and Receive Levels

Each OC-N card has a transmit and receive connector on its faceplate. Table 1-9 lists these levels.

Table 1-9 Optical Card Transmit and Receive Levels

	Transmit		Receive	
Card	**Minimum**	**Maximum**	**Minimum**	**Maximum**
OC3 IR 4/STM1 SH 1310	–15 dBm	–8 dBm	–28 dBm	–8 dBm
OC3IR/STM1SH 1310-8	–15 dBm	–8 dBm	–28 dBm	–8 dBm
OC12 IR/STM4 SH 1310	–15 dBm	–8 dBm	–28 dBm	–8 dBm
OC12 LR/STM4 LH 1310	–3 dBm	+2 dBm	–28 dBm	–8 dBm
OC12 LR/STM4 LH 1550	–3 dBm	+2 dBm	–28 dBm	–8 dBm
OC12 IR/STM4 SH 1310-4	–15 dBm	–8 dBm	–30 dBm	–8 dBm
OC48 IR 1310	–5 dBm	0 dBm	–18 dBm	0 dBm
OC48 LR 1550	–2 dBm	+3 dBm	–28 dBm	–8 dBm
OC48 IR/STM16 SH AS 1310	–5 dBm	0 dBm	–18 dBm	0 dBm
OC48 LR/STM16 LH AS 1550	–2 dBm	+3 dBm	–28 dBm	–8 dBm
OC48 ELR/STM16 EH 100 GHz	–2 dBm	0 dBm	–27 dBm at 1E-12 BER	–9 dBm
OC48 ELR/STM16 EH 200 GHz	–2 dBm	0 dBm	–28 dBm	–8 dBm
OC192 SR/STM64 IO 1310	–6 dBm	–1 dBm	–11 dBm	–1 dBm
OC192 IR/STM64 SH 1550	–1 dBm	+2 dBm	–14 dBm	–1 dBm
OC192 LR/STM64 LH 1550	+7 dBm	+10 dBm	–19 dBm	–10 dBm
OC192 LR/STM64 LH ITU 15xx.xx	+3 dBm	+6 dBm	–22 dBm	–9 dBm
15454_MRC-12 (ONS-SI-2G-S1)	–10 dBm	–3 dBm	–18 dBm	–3 dBm
15454_MRC-12 (ONS-SI-2G-I1)	–5 dBm	0 dBm	–18 dBm	0 dBm
15454_MRC-12 (ONS-SI-2G-L1)	–2 dBm	3 dBm	–27 dBm	–9 dBm
15454_MRC-12 (ONS-SI-2G-L2)	–2 dBm	3 dBm	–28 dBm	–9 dBm
15454_MRC-12 (ONS-SC-2G-30.3 through ONS-SC-2G-60.6)	0 dBm	4 dBm	–28 dBm	–9 dBm
15454_MRC-12 (ONS-SI-622-I1)	–15 dBm	–8 dBm	–28 dBm	–8 dBm
15454_MRC-12 (ONS-SI-622-L1)	–3 dBm	2 dBm	–28 dBm	–8 dBm
15454_MRC-12 (ONS-SI-622-L2)	–3 dBm	2 dBm	–28 dBm	–8 dBm

Table 1-9 Optical Card Transmit and Receive Levels (continued)

Card	Transmit		Receive	
	Minimum	Maximum	Minimum	Maximum
15454_MRC-12 (ONS-SE-622-1470 through ONS-SE-622-1610)	0 dBm	5 dBm	–28 dBm	–3 dBm
15454_MRC-12 (ONS-SI-155-I1)	–15 dBm	–8 dBm	–30 dBm	–8 dBm
15454_MRC-12 (ONS-SI-155-L1)	–5 dBm	0 dBm	–34 dBm	–10 dBm
15454_MRC-12 (ONS-SI-155-L2)	–5 dBm	0 dBm	–34 dBm	–10 dBm
15454_MRC-12 (ONS_SE-155-1470 through ONS-SE-155-1610)	0 dBm	5 dBm	–34 dBm	–3 dBm
OC192SR1/STM64IO Short Reach (ONS-XC-10G-S1)	–6 dBm	–1 dBm	–11 dBm	–1 dBm
OC192/STM64 Any Reach (ONS-XC-10G-S1)	–6 dBm	–1 dBm	–11 dBm	–1 dBm
OC192/STM64 Any Reach (ONS-XC-10G-I2)	–1 dBm	2 dBm	–14 dBm	2 dBm
OC192/STM64 Any Reach (ONS-XC-10G-L2)	0 dBm	4 dBm	–24 dBm	–7dBm

1.15 Power Supply Problems

Symptom Loss of power or low voltage, resulting in a loss of traffic and causing the LCD clock to reset to the default date and time.

Possible Cause Loss of power or low voltage.

Possible Cause Improperly connected power supply.

Recommended Action The ONS 15454 requires a constant source of DC power to properly function. Input power is –48 VDC. Power requirements range from –42 VDC to –57 VDC. A newly installed ONS 15454 that is not properly connected to its power supply does not operate. Power problems can be confined to a specific ONS 15454 or affect several pieces of equipment on the site. A loss of power or low voltage can result in a loss of traffic and causes the LCD clock on the ONS 15454 to default to January 1, 1970, 00:04:15. To reset the clock, in node view click the **Provisioning > General > General** tab and change the Date and Time fields. Complete the "Isolate the Cause of Power Supply Problems" procedure on page 1-156.

Warning **Only trained and qualified personnel should be allowed to install, replace, or service this equipment.** Statement 1030

Warning **During this procedure, wear grounding wrist straps to avoid ESD damage to the card. Do not directly touch the backplane with your hand or any metal tool, or you could shock yourself.** Statement 94

Caution Operations that interrupt power supply or short the power connections to the ONS 15454 are service-affecting.

Isolate the Cause of Power Supply Problems

Step 1 If a single ONS 15454 show signs of fluctuating power or power loss:

- **a.** Verify that the –48 VDC #8 power terminals are properly connected to a fuse panel. These power terminals are located on the lower section of the backplane EIA under the clear plastic cover.
- **b.** Verify that the power cable is #12 or #14 AWG and in good condition.
- **c.** Verify that the power cable connections are properly crimped. Stranded #12 or #14 AWG does not always crimp properly with Staycon type connectors.
- **d.** Verify that 20-A fuses are used in the fuse panel.
- **e.** Verify that the fuses are not blown.
- **f.** Verify that a rack-ground cable attaches to the frame-ground terminal (FGND) on the right side of the ONS 15454 EIA. Connect this cable to the ground terminal according to local site practice.
- **g.** Verify that the DC power source has enough capacity to carry the power load.
- **h.** If the DC power source is battery-based:
  - Check that the output power is high enough. Power requirements range from –42 VDC to –57 VDC.
  - Check the age of the batteries. Battery performance decreases with age.
  - Check for opens and shorts in batteries, which might affect power output.
  - If brownouts occur, the power load and fuses might be too high for the battery plant.

Step 2 If multiple pieces of site equipment show signs of fluctuating power or power loss:

- **a.** Check the uninterruptible power supply (UPS) or rectifiers that supply the equipment. Refer to the UPS manufacturer's documentation for specific instructions.
- **b.** Check for excessive power drains caused by other equipment, such as generators.
- **c.** Check for excessive power demand on backup power systems or batteries when alternate power sources are used.

1.15.1 Power Consumption for Node and Cards

Symptom You are unable to power up a node or the cards in a node.

Possible Cause Improper power supply.

Recommended Action Refer to power information in the "Hardware Specifications" appendix in the *Cisco ONS 15454 Reference Manual*.

CHAPTER 2

Alarm Troubleshooting

Note The terms "Unidirectional Path Switched Ring" and "UPSR" may appear in Cisco literature. These terms do not refer to using Cisco ONS 15xxx products in a unidirectional path switched ring configuration. Rather, these terms, as well as "Path Protected Mesh Network" and "PPMN," refer generally to Cisco's path protection feature, which may be used in any topological network configuration. Cisco does not recommend using its path protection feature in any particular topological network configuration.

This chapter gives a description, severity, and troubleshooting procedure for each commonly encountered Cisco ONS 15454 alarm and condition. Tables 2-1 through 2-5 provide lists of ONS 15454 alarms organized by severity. Table 2-6 on page 2-9 provides a list of alarms organized alphabetically. Table 2-7 gives definitions of all ONS 15454 alarm logical objects, which are the basis of the alarm profile list in Table 2-8 on page 2-19. For a comprehensive list of all conditions and instructions for using TL1 commands, refer to the *Cisco SONET TL1 Command Guide* .

An alarm's troubleshooting procedure applies to both the Cisco Transport Controller (CTC) and TL1 version of that alarm. If the troubleshooting procedure does not clear the alarm, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call the Cisco Technical Assistance Center (1 800 553-2447).

For more information about alarm profiles, refer to the "Manage Alarms" chapter in the *Cisco ONS 15454 Procedure Guide*.

2.1 Alarm Indexes by Default Severity

The following tables group alarms and conditions by their default severities in the ONS 15454 system. These severities are the same whether they are reported in the CTC Alarms window severity (SEV) column or in TL1.

Note The CTC default alarm profile contains some alarms or conditions that are not currently implemented but are reserved for future use.

Note The CTC default alarm profile in some cases contains two severities for one alarm (for example, MJ/MN). The ONS 15454 platform default severity comes first (in this example, MJ), but the alarm can be demoted to the second severity in the presence of a higher-ranking alarm. This is in accordance with Telcordia GR-474.

2.1.1 Critical Alarms (CR)

Table 2-1 alphabetically lists ONS 15454 Critical (CR) alarms.

Table 2-1 ONS 15454 Critical Alarm List

AUTOLSROFF (OCN)	LOF (TRUNK)	OPWR-HFAIL (OTS)
AUTOLSROFF (TRUNK)	LOM (STSMON)	OPWR-LFAIL (AOTS)
AWG-FAIL (OTS)	LOM (TRUNK)	OPWR-LFAIL (OCH)
AWG-OVERTEMP (OTS)	LOP-P (STSMON)	OPWR-LFAIL (OMS)
BKUPMEMP (EQPT)	LOP-P (STSTRM)	OPWR-LFAIL (OTS)
COMIOXC (EQPT)	LOS (2R)	OTUK-LOF (TRUNK)
CONTBUS-DISABLED (EQPT)	LOS (DS3)	OTUK-TIM (TRUNK)
CTNEQPT-PBPROT (EQPT)	LOS (EC1)	PLM-P (STSMON)
CTNEQPT-PBWORK (EQPT)	LOS (ESCON)	PLM-P (STSTRM)
ENCAP-MISMATCH-P (STSTRM)	LOS (ISC)	PORT-ADD-PWR-FAIL-HIGH (OCH)
EQPT (AICI-AEP)	LOS (OCN)	PORT-ADD-PWR-FAIL-LOW (OCH)
EQPT (AICI-AIE)	LOS (OTS)	PORT-FAIL (OCH)
EQPT (EQPT)	LOS (TRUNK)	SQM (STSTRM)
EQPT (PPM)	LOS-P (OCH)	SWMTXMOD-PROT (EQPT)
EQPT-MISS (FAN)	LOS-P (OMS)	SWMTXMOD-WORK (EQPT)
FAN (FAN)	LOS-P (OTS)	TIM (OCN)
GAIN-HFAIL (AOTS)	LOS-P (TRUNK)	TIM (TRUNK)
GAIN-LFAIL (AOTS)	MEA (AIP)	TIM-P (STSTRM)
GE-OOSYNC (FC)	MEA (BIC)	TIM-S (EC1)
GE-OOSYNC (GE)	MEA (EQPT)	TIM-S (OCN)
GE-OOSYNC (ISC)	MEA (FAN)	UNEQ-P (STSMON)
GE-OOSYNC (TRUNK)	MEA (PPM)	UNEQ-P (STSTRM)
HITEMP (NE)	MFGMEM (AICI-AEP)	VOA-HFAIL (AOTS)
I-HITEMP (NE)	MFGMEM (AICI-AIE)	VOA-HFAIL (OCH)
IMPROPRMVL (EQPT)	MFGMEM (AIP)	VOA-HFAIL (OMS)
IMPROPRMVL (PPM)	MFGMEM (BPLANE)	VOA-HFAIL (OTS)
LOA (VCG)	MFGMEM (FAN)	VOA-LFAIL (AOTS)
LOF (DS3)	MFGMEM (PPM)	VOA-LFAIL (OCH)
LOF (EC1)	OPWR-HFAIL (AOTS)	VOA-LFAIL (OMS)
LOF (OCN)	OPWR-HFAIL (OCH)	VOA-LFAIL (OTS)
LOF (STSTRM)	OPWR-HFAIL (OMS)	—

2.1.2 Major Alarms (MJ)

Table 2-2 alphabetically lists ONS 15454 Major (MJ) alarms.

Table 2-2 ONS 15454 Major Alarm List

APSCM (OCN)	GFP-EX-MISMATCH (FCMR)	PRC-DUPID (OCN)
APSCNMIS (OCN)	GFP-EX-MISMATCH (GFP-FAC)	PTIM (TRUNK)
BAT-FAIL (PWR)	GFP-LFD (CE100T)	RCVR-MISS (DS1)
BLSROSYNC (OCN)	GFP-LFD (FCMR)	RCVR-MISS (E1)
BLSR-SW-VER-MISM (OCN)	GFP-LFD (GFP-FAC)	RING-ID-MIS (OCN)
CARLOSS (CE100T)	GFP-LFD (ML1000)	RING-ID-MIS (OSC-RING)
CARLOSS (E1000F)	GFP-LFD (ML100T)	RING-MISMATCH (OCN)
CARLOSS (E100T)	GFP-LFD (MLFX)	SIGLOSS (FC)
CARLOSS (EQPT)	GFP-NO-BUFFERS (FCMR)	SIGLOSS (FCMR)
CARLOSS (FC)	GFP-NO-BUFFERS (GFP-FAC)	SIGLOSS (GE)
CARLOSS (G1000)	GFP-UP-MISMATCH (CE100T)	SIGLOSS (ISC)
CARLOSS (GE)	GFP-UP-MISMATCH (FCMR)	SIGLOSS (TRUNK)
CARLOSS (ISC)	GFP-UP-MISMATCH (GFP-FAC)	SQM (VT-TERM)
CARLOSS (ML1000)	GFP-UP-MISMATCH (ML1000)	SYNCLOSS (FC)
CARLOSS (ML100T)	GFP-UP-MISMATCH (ML100T)	SYNCLOSS (FCMR)
CARLOSS (MLFX)	GFP-UP-MISMATCH (MLFX)	SYNCLOSS (GE)
CARLOSS (TRUNK)	HIBATVG (PWR)	SYNCLOSS (ISC)
DBOSYNC (NE)	INVMACADR (AIP)	SYNCLOSS (TRUNK)
DSP-COMM-FAIL (TRUNK)	LASERBIAS-FAIL (AOTS)	SYNCPRI (NE-SREF)
DSP-FAIL (TRUNK)	LOF (DS1)	SYSBOOT (NE)
EHIBATVG (PWR)	LOF (E1)	TIM-V (VT-TERM)
ELWBATVG (PWR)	LOM (STSTRM)	TPTFAIL (CE100T)
E-W-MISMATCH (OCN)	LOM (VT-TERM)	TPTFAIL (FCMR)
EXTRA-TRAF-PREEMPT (OCN)	LOP-V (VT-MON)	TPTFAIL (G1000)
FC-NO-CREDITS (FC)	LOP-V (VT-TERM)	TPTFAIL (ML1000)
FC-NO-CREDITS (FCMR)	LOS (DS1)	TPTFAIL (ML100T)
FC-NO-CREDITS (TRUNK)	LOS (E1)	TPTFAIL (MLFX)
FEC-MISM (TRUNK)	LWBATVG (PWR)	TRMT (DS1)
GFP-CSF (CE100T)	MEM-GONE (EQPT)	TRMT (E1)
GFP-CSF (FCMR)	ODUK-TIM-PM (TRUNK)	TRMT-MISS (DS1)
GFP-CSF (GFP-FAC)	OPTNTWMIS (NE)	TRMT-MISS (E1)
GFP-CSF (ML1000)	OUT-OF-SYNC (FC)	UNEQ-V (VT-MON)
GFP-CSF (ML100T)	OUT-OF-SYNC (GE)	UNEQ-V (VT-TERM)
GFP-CSF (MLFX)	OUT-OF-SYNC (TRUNK)	UT-COMM-FAIL (TRUNK)

Table 2-2 ONS 15454 Major Alarm List (continued)

GFP-DE-MISMATCH (FCMR)	PEER-NORESPONSE (EQPT)	UT-FAIL (TRUNK)
GFP-DE-MISMATCH (GFP-FAC)	PLM-V (VT-TERM)	WVL-MISMATCH (TRUNK)

2.1.3 Minor Alarms (MN)

Table 2-3 alphabetically lists ONS 15454 Minor (MN) alarms.

Table 2-3 ONS 15454 Minor Alarm List

APSB (OCN)	HI-RXPOWER (FC)	LO-TXPOWER (OCN)
APSCDFLTK (OCN)	HI-RXPOWER (GE)	LO-TXPOWER (PPM)
APSC-IMP (OCN)	HI-RXPOWER (ISC)	LO-TXPOWER (TRUNK)
APSCINCON (OCN)	HI-RXPOWER (OCN)	MEM-LOW (EQPT)
APSIMP (OCN)	HI-RXPOWER (TRUNK)	OPWR-HDEG (AOTS)
APS-INV-PRIM (OCN)	HITEMP (EQPT)	OPWR-HDEG (OCH)
APSMM (OCN)	HI-TXPOWER (2R)	OPWR-HDEG (OMS)
APS-PRIM-SEC-MISM (OCN)	HI-TXPOWER (EQPT)	OPWR-HDEG (OTS)
AUTORESET (EQPT)	HI-TXPOWER (ESCON)	OPWR-LDEG (AOTS)
AUTOSW-UNEQ (VT-MON)	HI-TXPOWER (FC)	OPWR-LDEG (OCH)
AWG-DEG (OTS)	HI-TXPOWER (GE)	OPWR-LDEG (OMS)
BPV (BITS)	HI-TXPOWER (ISC)	OPWR-LDEG (OTS)
CASETEMP-DEG (AOTS)	HI-TXPOWER (OCN)	OTUK-IAE (TRUNK)
COMM-FAIL (EQPT)	HI-TXPOWER (PPM)	PORT-ADD-PWR-DEG-HI (OCH)
CONTBUS-A-18 (EQPT)	HI-TXPOWER (TRUNK)	PORT-ADD-PWR-DEG-LOW (OCH)
CONTBUS-B-18 (EQPT)	ISIS-ADJ-FAIL (OCN)	PROTNA (EQPT)
CONTBUS-IO-A (EQPT)	KBYTE-APS-CHANNEL-FAILURE (OCN)	PROV-MISMATCH (PPM)
CONTBUS-IO-B (EQPT)	LASERBIAS-DEG (AOTS)	PWR-FAIL-A (EQPT)
DATAFLT (NE)	LASERBIAS-DEG (OTS)	PWR-FAIL-B (EQPT)
DUP-IPADDR (NE)	LASEREOL (OCN)	PWR-FAIL-RET-A (EQPT)
DUP-NODENAME (NE)	LASERTEMP-DEG (AOTS)	PWR-FAIL-RET-B (EQPT)
ENVALRM)EXT	LOF (BITS)	SFTWDOWN (EQPT)
EOC (OCN)	LO-LASERBIAS (EQPT)	SH-INS-LOSS-VAR-DEG-HIGH (OTS)
EOC (TRUNK)	LO-LASERBIAS (OCN)	SH-INS-LOSS-VAR-DEG-LOW (OTS)
EOC-L (OCN)	LO-LASERBIAS (PPM)	SNTP-HOST (NE)
EOC-L (TRUNK)	LO-LASERTEMP (EQPT)	SSM-FAIL (BITS)
ERROR-CONFIG (EQPT)	LO-LASERTEMP (OCN)	SSM-FAIL (DS1)
EXCCOL (EQPT)	LO-LASERTEMP (PPM)	SSM-FAIL (E1)
FEPRLF (OCN)	LO-RXPOWER (2R)	SSM-FAIL (OCN)

Table 2-3 ONS 15454 Minor Alarm List (continued)

FIBERTEMP-DEG (AOTS)	LO-RXPOWER (ESCON)	SSM-FAIL (TRUNK)
GAIN-HDEG (AOTS)	LO-RXPOWER (FC)	SYNCPRI (EXT-SREF)
GAIN-LDEG (AOTS)	LO-RXPOWER (GE)	SYNCSEC (EXT-SREF)
GCC-EOC (TRUNK)	LO-RXPOWER (ISC)	SYNCSEC (NE-SREF)
HELLO (OCN)	LO-RXPOWER (OCN)	SYNCTHIRD (EXT-SREF)
HI-LASERBIAS (2R)	LO-RXPOWER (TRUNK)	SYNCTHIRD (NE-SREF)
HI-LASERBIAS (EQPT)	LOS (BITS)	TIM-MON (OCN)
HI-LASERBIAS (ESCON)	LOS (FUDC)	TIM-MON (TRUNK)
HI-LASERBIAS (FC)	LOS (MSUDC)	TIM-P (STSMON)
HI-LASERBIAS (GE)	LOS-O (OCH)	UNREACHABLE-TARGET-POWER (OCH)
HI-LASERBIAS (ISC)	LOS-O (OMS)	VOA-HDEG (AOTS)
HI-LASERBIAS (OCN)	LOS-O (OTS)	VOA-HDEG (OCH)
HI-LASERBIAS (PPM)	LO-TXPOWER (2R)	VOA-HDEG (OMS)
HI-LASERBIAS (TRUNK)	LO-TXPOWER (EQPT)	VOA-HDEG (OTS)
HI-LASERTEMP (EQPT)	LO-TXPOWER (ESCON)	VOA-LDEG (AOTS)
HI-LASERTEMP (OCN)	LO-TXPOWER (FC)	VOA-LDEG (OCH)
HI-LASERTEMP (PPM)	LO-TXPOWER (GE)	VOA-LDEG (OMS)
HI-RXPOWER (2R)	LO-TXPOWER (ISC)	VOA-LDEG (OTS)
HI-RXPOWER (ESCON)	—	—

2.1.4 NA Conditions

Table 2-4 alphabetically lists ONS 15454 Not Alarmed (NA) conditions.

Table 2-4 ONS 15454 NA Conditions List

(LCAS-RX-FAIL (VT-TERM)	FORCED-REQ-SPAN (ISC)	SD-L (OCN)
)SSM-SETS (TRUNK)	FORCED-REQ-SPAN (OCN)	SD-P (STSMON)
ALS (2R)	FORCED-REQ-SPAN (TRUNK)	SD-P (STSTRM)
ALS (AOTS)	FRCDSWTOINT (NE-SREF)	SD-V (VT-MON)
ALS (ESCON)	FRCDSWTOPRI (EXT-SREF)	SD-V (VT-TERM)
ALS (FC)	FRCDSWTOPRI (NE-SREF)	SF (DS1)
ALS (GE)	FRCDSWTOSEC (EXT-SREF)	SF (DS3)
ALS (ISC)	FRCDSWTOSEC (NE-SREF)	SF (E1)
ALS (OCN)	FRCDSWTOTHIRD (EXT-SREF)	SF (TRUNK)
ALS (TRUNK)	FRCDSWTOTHIRD (NE-SREF)	SF-L (EC1)
AMPLI-INIT (AOTS)	FRNGSYNC (NE-SREF)	SF-L (OCN)
APC-CORRECTION-SKIPPED (AOTS)	FSTSYNC (NE-SREF)	SF-P (STSMON)

Table 2-4 ONS 15454 NA Conditions List (continued)

APC-CORRECTION-SKIPPED (OCH)	FULLPASSTHR-BI (OCN)	SF-P (STSTRM)
APC-CORRECTION-SKIPPED (OMS)	HI-CCVOLT (BITS)	SF-V (VT-MON)
APC-CORRECTION-SKIPPED (OTS)	HLDOVRSYNC (NE-SREF)	SF-V (VT-TERM)
APC-DISABLED (NE)	INC-ISD (DS3)	SHUTTER-OPEN (OTS)
APC-END (NE)	INHSWPR (EQPT)	SPAN-SW-EAST (OCN)
APC-OUT-OF-RANGE (AOTS)	INHSWWKG (EQPT)	SPAN-SW-WEST (OCN)
APC-OUT-OF-RANGE (OCH)	INTRUSION-PSWD (NE)	SQUELCH (OCN)
APC-OUT-OF-RANGE (OMS)	IOSCFGCOPY (EQPT)	SQUELCHED (2R)
APC-OUT-OF-RANGE (OTS)	KB-PASSTHR (OCN)	SQUELCHED (ESCON)
APS-PRIM-FAC (OCN)	LAN-POL-REV (NE)	SQUELCHED (FC)
AS-CMD (2R)	LASER-APR (AOTS)	SQUELCHED (GE)
AS-CMD (AOTS)	LCAS-CRC (STSTRM)	SQUELCHED (ISC)
AS-CMD (BPLANE)	LCAS-CRC (VT-TERM)	SQUELCHED (OCN)
AS-CMD (CE100T)	LCAS-RX-FAIL (STSTRM)	SQUELCHED (TRUNK)
AS-CMD (DS1)	LCAS-TX-ADD (STSTRM)	SSM-DUS (BITS)
AS-CMD (DS3)	LCAS-TX-ADD (VT-TERM)	SSM-DUS (DS1)
AS-CMD (E1)	LCAS-TX-DNU (STSTRM)	SSM-DUS (E1)
AS-CMD (E1000F)	LCAS-TX-DNU (VT-TERM)	SSM-DUS (OCN)
AS-CMD (E100T)	LKOUTPR-S (OCN)	SSM-DUS (TRUNK)
AS-CMD (EC1)	LOCKOUT-REQ (2R)	SSM-LNC (TRUNK)
AS-CMD (EQPT)	LOCKOUT-REQ (EQPT)	SSM-OFF (BITS)
AS-CMD (ESCON)	LOCKOUT-REQ (ESCON)	SSM-OFF (DS1)
AS-CMD (FC)	LOCKOUT-REQ (FC)	SSM-OFF (E1)
AS-CMD (FCMR)	LOCKOUT-REQ (GE)	SSM-OFF (OCN)
AS-CMD (G1000)	LOCKOUT-REQ (ISC)	SSM-OFF (TRUNK)
AS-CMD (GE)	LOCKOUT-REQ (OCN)	SSM-PRC (TRUNK)
AS-CMD (GFP-FAC)	LOCKOUT-REQ (STSMON)	SSM-PRS (BITS)
AS-CMD (ISC)	LOCKOUT-REQ (TRUNK)	SSM-PRS (DS1)
AS-CMD (ISC)	LOCKOUT-REQ (VT-MON)	SSM-PRS (E1)
AS-CMD (ML100T)	LPBKCRS (STSMON)	SSM-PRS (NE-SREF)
AS-CMD (MLFX)	LPBKCRS (STSTRM)	SSM-PRS (OCN)
AS-CMD (NE)	LPBKDS1FEAC-CMD (DS1)	SSM-PRS (TRUNK)
AS-CMD (OCH)	LPBKDS3FEAC (DS3)	SSM-RES (BITS)
AS-CMD (OCN)	LPBKDS3FEAC-CMD (DS3)	SSM-RES (DS1)
AS-CMD (OMS)	LPBKFACILITY (CE100T)	SSM-RES (E1)
AS-CMD (OTS)	LPBKFACILITY (DS1)	SSM-RES (NE-SREF)
AS-CMD (PPM)	LPBKFACILITY (DS3)	SSM-RES (OCN)

Table 2-4 ONS 15454 NA Conditions List (continued)

AS-CMD (PWR)	LPBKFACILITY (E1)	SSM-RES (TRUNK)
AS-CMD (TRUNK)	LPBKFACILITY (EC1)	SSM-SDH-TN (TRUNK)
AS-MT (2R)	LPBKFACILITY (ESCON)	SSM-SMC (BITS)
AS-MT (AOTS)	LPBKFACILITY (FC)	SSM-SMC (DS1)
AS-MT (CE100T)	LPBKFACILITY (FCMR)	SSM-SMC (E1)
AS-MT (DS1)	LPBKFACILITY (G1000)	SSM-SMC (NE-SREF)
AS-MT (DS3)	LPBKFACILITY (GE)	SSM-SMC (OCN)
AS-MT (E1)	LPBKFACILITY (ISC)	SSM-SMC (TRUNK)
AS-MT (EC1)	LPBKFACILITY (OCN)	SSM-ST2 (BITS)
AS-MT (EQPT)	LPBKFACILITY (TRUNK)	SSM-ST2 (DS1)
AS-MT (ESCON)	LPBKTERMINAL (CE100T)	SSM-ST2 (E1)
AS-MT (FC)	LPBKTERMINAL (DS1)	SSM-ST2 (NE-SREF)
AS-MT (FCMR)	LPBKTERMINAL (DS3)	SSM-ST2 (OCN)
AS-MT (G1000)	LPBKTERMINAL (E1)	SSM-ST2 (TRUNK)
AS-MT (GE)	LPBKTERMINAL (EC1)	SSM-ST3 (BITS)
AS-MT (GFP-FAC)	LPBKTERMINAL (ESCON)	SSM-ST3 (DS1)
AS-MT (ISC)	LPBKTERMINAL (FC)	SSM-ST3 (E1)
AS-MT (ISC)	LPBKTERMINAL (FCMR)	SSM-ST3 (NE-SREF)
AS-MT (ML100T)	LPBKTERMINAL (G1000)	SSM-ST3 (OCN)
AS-MT (MLFX)	LPBKTERMINAL (GE)	SSM-ST3 (TRUNK)
AS-MT (OCH)	LPBKTERMINAL (ISC)	SSM-ST3E (BITS)
AS-MT (OCN)	LPBKTERMINAL (OCN)	SSM-ST3E (DS1)
AS-MT (OMS)	LPBKTERMINAL (TRUNK)	SSM-ST3E (E1)
AS-MT (OTS)	MAN-REQ (EQPT)	SSM-ST3E (NE-SREF)
AS-MT (PPM)	MAN-REQ (STSMON)	SSM-ST3E (OCN)
AS-MT (TRUNK)	MAN-REQ (VT-MON)	SSM-ST3E (TRUNK)
AS-MT-OOG (STSTRM)	MANRESET (EQPT)	SSM-ST4 (BITS)
AS-MT-OOG (VT-TERM)	MANSWTOINT (NE-SREF)	SSM-ST4 (DS1)
AUD-LOG-LOSS (NE)	MANSWTOPRI (EXT-SREF)	SSM-ST4 (E1)
AUD-LOG-LOW (NE)	MANSWTOPRI (NE-SREF)	SSM-ST4 (NE-SREF)
AUTOSW-LOP (STSMON)	MANSWTOSEC (EXT-SREF)	SSM-ST4 (OCN)
AUTOSW-LOP (VT-MON)	MANSWTOSEC (NE-SREF)	SSM-ST4 (TRUNK)
AUTOSW-PDI (STSMON)	MANSWTOTHIRD (EXT-SREF)	SSM-STU (BITS)
AUTOSW-SDBER (STSMON)	MANSWTOTHIRD (NE-SREF)	SSM-STU (DS1)
AUTOSW-SFBER (STSMON)	MANUAL-REQ-RING (OCN)	SSM-STU (E1)
AUTOSW-UNEQ (STSMON)	MANUAL-REQ-SPAN (2R)	SSM-STU (NE-SREF)
AWG-WARM-UP (OTS)	MANUAL-REQ-SPAN (ESCON)	SSM-STU (OCN)

Table 2-4 ONS 15454 NA Conditions List (continued)

CLDRESTART (EQPT)	MANUAL-REQ-SPAN (FC)	SSM-STU (TRUNK)
CTNEQPT-MISMATCH (EQPT)	MANUAL-REQ-SPAN (GE)	SSM-TNC (BITS)
DS3-MISM (DS3)	MANUAL-REQ-SPAN (ISC)	SSM-TNC (NE-SREF)
ETH-LINKLOSS (NE)	MANUAL-REQ-SPAN (OCN)	SSM-TNC (OCN)
EXERCISE-RING-FAIL (OCN)	MANUAL-REQ-SPAN (TRUNK)	SSM-TNC (TRUNK)
EXERCISE-SPAN-FAIL (OCN)	NO-CONFIG (EQPT)	SWTOPRI (EXT-SREF)
FAILTOSW (2R)	OCHNC-INC (OCHNC-CONN)	SWTOPRI (NE-SREF)
FAILTOSW (EQPT)	ODUK-SD-PM (TRUNK)	SWTOSEC (EXT-SREF)
FAILTOSW (ESCON)	ODUK-SF-PM (TRUNK)	SWTOSEC (NE-SREF)
FAILTOSW (FC)	OOU-TPT (STSTRM)	SWTOTHIRD (EXT-SREF)
FAILTOSW (GE)	OOU-TPT (VT-TERM)	SWTOTHIRD (NE-SREF)
FAILTOSW (ISC)	OPEN-SLOT (EQPT)	SYNC-FREQ (BITS)
FAILTOSW (OCN)	OSRION (AOTS)	SYNC-FREQ (DS1)
FAILTOSW (TRUNK)	OSRION (OTS)	SYNC-FREQ (E1)
FAILTOSW-PATH (STSMON)	OTUK-SD (TRUNK)	SYNC-FREQ (OCN)
FAILTOSW-PATH (VT-MON)	OTUK-SF (TRUNK)	SYNC-FREQ (TRUNK)
FAILTOSWR (OCN)	OUT-OF-SYNC (ISC)	TEMP-MISM (NE)
FAILTOSWS (OCN)	PARAM-MISM (AOTS)	TX-RAI (DS1)
FE-AIS (DS3)	PARAM-MISM (OCH)	TX-RAI (DS3)
FE-DS1-MULTLOS (DS3)	PARAM-MISM (OMS)	TX-RAI (E1)
FE-DS1-NSA (DS3)	PARAM-MISM (OTS)	UNC-WORD (TRUNK)
FE-DS1-SA (DS3)	PDI-P (STSMON)	VCG-DEG (VCG)
FE-DS1-SNGLLOS (DS3)	PDI-P (STSTRM)	VCG-DOWN (VCG)
FE-DS3-NSA (DS3)	PORT-MISMATCH (FCMR)	VOLT-MISM (PWR)
FE-DS3-SA (DS3)	RAI (DS1)	WKSWPR (2R)
FE-EQPT-NSA (DS3)	RAI (DS3)	WKSWPR (EQPT)
FE-FRCDWKSWBK-SPAN (OCN)	RAI (E1)	WKSWPR (ESCON)
FE-FRCDWKSWPR-RING (OCN)	RING-SW-EAST (OCN)	WKSWPR (FC)
FE-FRCDWKSWPR-SPAN (OCN)	RING-SW-WEST (OCN)	WKSWPR (GE)
FE-IDLE (DS3)	ROLL (STSMON)	WKSWPR (ISC)
FE-LOCKOUTOFPR-SPAN (OCN)	ROLL (STSTRM)	WKSWPR (OCN)
FE-LOF (DS3)	ROLL (VT-MON)	WKSWPR (STSMON)
FE-LOS (DS3)	ROLL-PEND (STSMON)	WKSWPR (TRUNK)
FE-MANWKSWBK-SPAN (OCN)	ROLL-PEND (VT-MON)	WKSWPR (VT-MON)
FE-MANWKSWPR-RING (OCN)	RPRW (CE100T)	WTR (2R)
FE-MANWKSWPR-SPAN (OCN)	RPRW (ML1000)	WTR (EQPT)
FORCED-REQ (EQPT)	RPRW (ML100T)	WTR (ESCON)

Table 2-4 ONS 15454 NA Conditions List (continued)

FORCED-REQ (STSMON)	RPRW (MLFX)	WTR (FC)
FORCED-REQ (VT-MON)	RUNCFG-SAVENEED (EQPT)	WTR (GE)
FORCED-REQ-RING (OCN)	SD (DS1)	WTR (ISC)
FORCED-REQ-SPAN (2R)	SD (DS3)	WTR (OCN)
FORCED-REQ-SPAN (ESCON)	SD (E1)	WTR (STSMON)
FORCED-REQ-SPAN (FC)	SD (TRUNK)	WTR (TRUNK)
FORCED-REQ-SPAN (GE)	SD-L (EC1)	WTR (VT-MON)

2.1.5 NR Conditions

Table 2-5 alphabetically lists ONS 15454 Not Reported (NR) conditions.

Table 2-5 ONS 15454 NR Conditions List

AIS (BITS)	ERFI-P-CONN (STSMON)	OTUK-AIS (TRUNK)
AIS (DS1)	ERFI-P-CONN (STSTRM)	OTUK-BDI (TRUNK)
AIS (DS3)	ERFI-P-PAYLD (STSMON)	RFI (TRUNK)
AIS (E1)	ERFI-P-PAYLD (STSTRM)	RFI-L (EC1)
AIS (FUDC)	ERFI-P-SRVR (STSMON)	RFI-L (OCN)
AIS (MSUDC)	ERFI-P-SRVR (STSTRM)	RFI-P (STSMON)
AIS (TRUNK)	ODUK-1-AIS-PM (TRUNK)	RFI-P (STSTRM)
AIS-L (EC1)	ODUK-2-AIS-PM (TRUNK)	RFI-V (VT-TERM)
AIS-L (OCN)	ODUK-3-AIS-PM (TRUNK)	ROLL-PEND (STSTRM)
AIS-P (STSMON)	ODUK-4-AIS-PM (TRUNK)	TX-AIS (DS1)
AIS-P (STSTRM)	ODUK-AIS-PM (TRUNK)	TX-AIS (DS3)
AIS-V (VT-MON)	ODUK-BDI-PM (TRUNK)	TX-AIS (E1)
AIS-V (VT-TERM)	ODUK-LCK-PM (TRUNK)	TX-LOF (DS1)
AUTOSW-AIS (STSMON)	ODUK-OCI-PM (TRUNK)	TX-LOF (E1)
AUTOSW-AIS (VT-MON)	—	—

2.2 Alarms and Conditions Listed By Alphabetical Entry

Table 2-6 alphabetically lists all ONS 15454 alarms and conditions.

Table 2-6 ONS 15454 Alarm and Condition Alphabetical List

APSB (OCN)	GFP-LFD (ML1000)	PLM-P (STSMON)
LCAS-RX-FAIL (VT-TERM)	GFP-LFD (ML100T)	PLM-P (STSTRM)
AIS (BITS)	GFP-LFD (MLFX)	PLM-V (VT-TERM)

Table 2-6 ONS 15454 Alarm and Condition Alphabetical List (continued)

AIS (DS1)	GFP-NO-BUFFERS (FCMR)	PORT-ADD-PWR-DEG-HI (OCH)
AIS (DS3)	GFP-NO-BUFFERS (GFP-FAC)	PORT-ADD-PWR-DEG-LOW (OCH)
AIS (E1)	GFP-UP-MISMATCH (CE100T)	PORT-ADD-PWR-FAIL-HIGH (OCH)
AIS (FUDC)	GFP-UP-MISMATCH (FCMR)	PORT-ADD-PWR-FAIL-LOW (OCH)
AIS (MSUDC)	GFP-UP-MISMATCH (GFP-FAC)	PORT-FAIL (OCH)
AIS (TRUNK)	GFP-UP-MISMATCH (ML1000)	PORT-MISMATCH (FCMR)
AIS-L (EC1)	GFP-UP-MISMATCH (ML100T)	PRC-DUPID (OCN)
AIS-L (OCN)	GFP-UP-MISMATCH (MLFX)	PROTNA (EQPT)
AIS-P (STSMON)	HELLO (OCN)	PROV-MISMATCH (PPM)
AIS-P (STSTRM)	HIBATVG (PWR)	PTIM (TRUNK)
AIS-V (VT-MON)	HI-CCVOLT (BITS)	PWR-FAIL-A (EQPT)
AIS-V (VT-TERM)	HI-LASERBIAS (2R)	PWR-FAIL-B (EQPT)
ALS (2R)	HI-LASERBIAS (EQPT)	PWR-FAIL-RET-A (EQPT)
ALS (AOTS)	HI-LASERBIAS (ESCON)	PWR-FAIL-RET-B (EQPT)
ALS (ESCON)	HI-LASERBIAS (FC)	RAI (DS1)
ALS (FC)	HI-LASERBIAS (GE)	RAI (DS3)
ALS (GE)	HI-LASERBIAS (ISC)	RAI (E1)
ALS (ISC)	HI-LASERBIAS (OCN)	RCVR-MISS (DS1)
ALS (OCN)	HI-LASERBIAS (PPM)	RCVR-MISS (E1)
ALS (TRUNK)	HI-LASERBIAS (TRUNK)	RFI (TRUNK)
AMPLI-INIT (AOTS)	HI-LASERTEMP (EQPT)	RFI-L (EC1)
APC-CORRECTION-SKIPPED (AOTS)	HI-LASERTEMP (OCN)	RFI-L (OCN)
APC-CORRECTION-SKIPPED (OCH)	HI-LASERTEMP (PPM)	RFI-P (STSMON)
APC-CORRECTION-SKIPPED (OMS)	HI-RXPOWER (2R)	RFI-P (STSTRM)
APC-CORRECTION-SKIPPED (OTS)	HI-RXPOWER (ESCON)	RFI-V (VT-TERM)
APC-DISABLED (NE)	HI-RXPOWER (FC)	RING-ID-MIS (OCN)
APC-END (NE)	HI-RXPOWER (GE)	RING-ID-MIS (OSC-RING)
APC-OUT-OF-RANGE (AOTS)	HI-RXPOWER (ISC)	RING-MISMATCH (OCN)
APC-OUT-OF-RANGE (OCH)	HI-RXPOWER (OCN)	RING-SW-EAST (OCN)
APC-OUT-OF-RANGE (OMS)	HI-RXPOWER (TRUNK)	RING-SW-WEST (OCN)
APC-OUT-OF-RANGE (OTS)	HITEMP (NE)	ROLL (STSMON)
APSCDFLTK (OCN)	HITEMP (EQPT)	ROLL (STSTRM)
APSC-IMP (OCN)	HI-TXPOWER (2R)	ROLL (VT-MON)
APSCINCON (OCN)	HI-TXPOWER (EQPT)	ROLL-PEND (STSMON)
APSCM (OCN)	HI-TXPOWER (ESCON)	ROLL-PEND (STSTRM)
APSCNMIS (OCN)	HI-TXPOWER (FC)	ROLL-PEND (VT-MON)
APSIMP (OCN)	HI-TXPOWER (GE)	RPRW (CE100T)

Table 2-6 ONS 15454 Alarm and Condition Alphabetical List (continued)

APS-INV-PRIM (OCN)	HI-TXPOWER (ISC)	RPRW (ML1000)
APSMM (OCN)	HI-TXPOWER (OCN)	RPRW (ML100T)
APS-PRIM-FAC (OCN)	HI-TXPOWER (PPM)	RPRW (MLFX)
APS-PRIM-SEC-MISM (OCN)	HI-TXPOWER (TRUNK)	RUNCFG-SAVENEED (EQPT)
AS-CMD (2R)	HLDOVRSYNC (NE-SREF)	SD (DS1)
AS-CMD (AOTS)	I-HITEMP (NE)	SD (DS3)
AS-CMD (BPLANE)	IMPROPRMVL (EQPT)	SD (E1)
AS-CMD (CE100T)	IMPROPRMVL (PPM)	SD (TRUNK)
AS-CMD (DS1)	INC-ISD (DS3)	SD-L (EC1)
AS-CMD (DS3)	INHSWPR (EQPT)	SD-L (OCN)
AS-CMD (E1)	INHSWWKG (EQPT)	SD-P (STSMON)
AS-CMD (E1000F)	INTRUSION-PSWD (NE)	SD-P (STSTRM)
AS-CMD (E100T)	INVMACADR (AIP)	SD-V (VT-MON)
AS-CMD (EC1)	IOSCFGCOPY (EQPT)	SD-V (VT-TERM)
AS-CMD (EQPT)	ISIS-ADJ-FAIL (OCN)	SF (DS1)
AS-CMD (ESCON)	KB-PASSTHR (OCN)	SF (DS3)
AS-CMD (FC)	KBYTE-APS-CHANNEL-FAILURE (OCN)	SF (E1)
AS-CMD (FCMR)	LAN-POL-REV (NE)	SF (TRUNK)
AS-CMD (G1000)	LASER-APR (AOTS)	SF-L (EC1)
AS-CMD (GE)	LASERBIAS-DEG (AOTS)	SF-L (OCN)
AS-CMD (GFP-FAC)	LASERBIAS-DEG (OTS)	SF-P (STSMON)
AS-CMD (ISC)	LASERBIAS-FAIL (AOTS)	SF-P (STSTRM)
AS-CMD (ISC)	LASEREOL (OCN)	SFTWDOWN (EQPT)
AS-CMD (ML100T)	LASERTEMP-DEG (AOTS)	SF-V (VT-MON)
AS-CMD (MLFX)	LCAS-CRC (STSTRM)	SF-V (VT-TERM)
AS-CMD (NE)	LCAS-CRC (VT-TERM)	SH-INS-LOSS-VAR-DEG-HIGH (OTS)
AS-CMD (OCH)	LCAS-RX-FAIL (STSTRM)	SH-INS-LOSS-VAR-DEG-LOW (OTS)
AS-CMD (OCN)	LCAS-TX-ADD (STSTRM)	SHUTTER-OPEN (OTS)
AS-CMD (OMS)	LCAS-TX-ADD (VT-TERM)	SIGLOSS (FC)
AS-CMD (OTS)	LCAS-TX-DNU (STSTRM)	SIGLOSS (FCMR)
AS-CMD (PPM)	LCAS-TX-DNU (VT-TERM)	SIGLOSS (GE)
AS-CMD (PWR)	LKOUTPR-S (OCN)	SIGLOSS (ISC)
AS-CMD (TRUNK)	LOA (VCG)	SIGLOSS (TRUNK)
AS-MT (2R)	LOCKOUT-REQ (2R)	SNTP-HOST (NE)
AS-MT (AOTS)	LOCKOUT-REQ (EQPT)	SPAN-SW-EAST (OCN)
AS-MT (CE100T)	LOCKOUT-REQ (ESCON)	SPAN-SW-WEST (OCN)

Table 2-6 ONS 15454 Alarm and Condition Alphabetical List (continued)

AS-MT (DS1)	LOCKOUT-REQ (FC)	SQM (STSTRM)
AS-MT (DS3)	LOCKOUT-REQ (GE)	SQM (VT-TERM)
AS-MT (E1)	LOCKOUT-REQ (ISC)	SQUELCH (OCN)
AS-MT (EC1)	LOCKOUT-REQ (OCN)	SQUELCHED (2R)
AS-MT (EQPT)	LOCKOUT-REQ (STSMON)	SQUELCHED (ESCON)
AS-MT (ESCON)	LOCKOUT-REQ (TRUNK)	SQUELCHED (FC)
AS-MT (FC)	LOCKOUT-REQ (VT-MON)	SQUELCHED (GE)
AS-MT (FCMR)	LOF (DS1)	SQUELCHED (ISC)
AS-MT (G1000)	LOF (DS3)	SQUELCHED (OCN)
AS-MT (GE)	LOF (E1)	SQUELCHED (TRUNK)
AS-MT (GFP-FAC)	LOF (EC1)	SSM-DUS (BITS)
AS-MT (ISC)	LOF (OCN)	SSM-DUS (DS1)
AS-MT (ISC)	LOF (STSTRM)	SSM-DUS (E1)
AS-MT (ML100T)	LOF (TRUNK)	SSM-DUS (OCN)
AS-MT (MLFX)	LOF (BITS)	SSM-DUS (TRUNK)
AS-MT (OCH)	LO-LASERBIAS (EQPT)	SSM-FAIL (BITS)
AS-MT (OCN)	LO-LASERBIAS (OCN)	SSM-FAIL (DS1)
AS-MT (OMS)	LO-LASERBIAS (PPM)	SSM-FAIL (E1)
AS-MT (OTS)	LO-LASERTEMP (EQPT)	SSM-FAIL (OCN)
AS-MT (PPM)	LO-LASERTEMP (OCN)	SSM-FAIL (TRUNK)
AS-MT (TRUNK)	LO-LASERTEMP (PPM)	SSM-LNC (TRUNK)
AS-MT-OOG (STSTRM)	LOM (STSMON)	SSM-OFF (BITS)
AS-MT-OOG (VT-TERM)	LOM (TRUNK)	SSM-OFF (DS1)
AUD-LOG-LOSS (NE)	LOM (STSTRM)	SSM-OFF (E1)
AUD-LOG-LOW (NE)	LOM (VT-TERM)	SSM-OFF (OCN)
AUTOLSROFF (OCN)	LOP-P (STSMON)	SSM-OFF (TRUNK)
AUTOLSROFF (TRUNK)	LOP-P (STSTRM)	SSM-PRC (TRUNK)
AUTORESET (EQPT)	LOP-V (VT-MON)	SSM-PRS (BITS)
AUTOSW-AIS (STSMON)	LOP-V (VT-TERM)	SSM-PRS (DS1)
AUTOSW-AIS (VT-MON)	LO-RXPOWER (2R)	SSM-PRS (E1)
AUTOSW-LOP (STSMON)	LO-RXPOWER (ESCON)	SSM-PRS (NE-SREF)
AUTOSW-LOP (VT-MON)	LO-RXPOWER (FC)	SSM-PRS (OCN)
AUTOSW-PDI (STSMON)	LO-RXPOWER (GE)	SSM-PRS (TRUNK)
AUTOSW-SDBER (STSMON)	LO-RXPOWER (ISC)	SSM-RES (BITS)
AUTOSW-SFBER (STSMON)	LO-RXPOWER (OCN)	SSM-RES (DS1)
AUTOSW-UNEQ (STSMON)	LO-RXPOWER (TRUNK)	SSM-RES (E1)
AUTOSW-UNEQ (VT-MON)	LOS (2R)	SSM-RES (NE-SREF)

Table 2-6 ONS 15454 Alarm and Condition Alphabetical List (continued)

AWG-DEG (OTS)	LOS (DS1)	SSM-RES (OCN)
AWG-FAIL (OTS)	LOS (DS3)	SSM-RES (TRUNK)
AWG-OVERTEMP (OTS)	LOS (E1)	SSM-SDH-TN (TRUNK)
AWG-WARM-UP (OTS)	LOS (EC1)	SSM-SETS (TRUNK)
BAT-FAIL (PWR)	LOS (ESCON)	SSM-SMC (BITS)
BKUPMEMP (EQPT)	LOS (ISC)	SSM-SMC (DS1)
BLSROSYNC (OCN)	LOS (OCN)	SSM-SMC (E1)
BLSR-SW-VER-MISM (OCN)	LOS (OTS)	SSM-SMC (NE-SREF)
BPV (BITS)	LOS (TRUNK)	SSM-SMC (OCN)
CARLOSS (CE100T)	LOS (BITS)	SSM-SMC (TRUNK)
CARLOSS (E1000F)	LOS (FUDC)	SSM-ST2 (BITS)
CARLOSS (E100T)	LOS (MSUDC)	SSM-ST2 (DS1)
CARLOSS (EQPT)	LOS-O (OCH)	SSM-ST2 (E1)
CARLOSS (FC)	LOS-O (OMS)	SSM-ST2 (NE-SREF)
CARLOSS (G1000)	LOS-O (OTS)	SSM-ST2 (OCN)
CARLOSS (GE)	LOS-P (OCH)	SSM-ST2 (TRUNK)
CARLOSS (ISC)	LOS-P (OMS)	SSM-ST3 (BITS)
CARLOSS (ML1000)	LOS-P (OTS)	SSM-ST3 (DS1)
CARLOSS (ML100T)	LOS-P (TRUNK)	SSM-ST3 (E1)
CARLOSS (MLFX)	LO-TXPOWER (2R)	SSM-ST3 (NE-SREF)
CARLOSS (TRUNK)	LO-TXPOWER (EQPT)	SSM-ST3 (OCN)
CASETEMP-DEG (AOTS)	LO-TXPOWER (ESCON)	SSM-ST3 (TRUNK)
CLDRESTART (EQPT)	LO-TXPOWER (FC)	SSM-ST3E (BITS)
COMIOXC (EQPT)	LO-TXPOWER (GE)	SSM-ST3E (DS1)
COMM-FAIL (EQPT)	LO-TXPOWER (ISC)	SSM-ST3E (E1)
CONTBUS-A-18 (EQPT)	LO-TXPOWER (OCN)	SSM-ST3E (NE-SREF)
CONTBUS-B-18 (EQPT)	LO-TXPOWER (PPM)	SSM-ST3E (OCN)
CONTBUS-DISABLED (EQPT)	LO-TXPOWER (TRUNK)	SSM-ST3E (TRUNK)
CONTBUS-IO-A (EQPT)	LPBKCRS (STSMON)	SSM-ST4 (BITS)
CONTBUS-IO-B (EQPT)	LPBKCRS (STSTRM)	SSM-ST4 (DS1)
CTNEQPT-MISMATCH (EQPT)	LPBKDS1FEAC-CMD (DS1)	SSM-ST4 (E1)
CTNEQPT-PBPROT (EQPT)	LPBKDS3FEAC (DS3)	SSM-ST4 (NE-SREF)
CTNEQPT-PBWORK (EQPT)	LPBKDS3FEAC-CMD (DS3)	SSM-ST4 (OCN)
DATAFLT (NE)	LPBKFACILITY (CE100T)	SSM-ST4 (TRUNK)
DBOSYNC (NE)	LPBKFACILITY (DS1)	SSM-STU (BITS)
DS3-MISM (DS3)	LPBKFACILITY (DS3)	SSM-STU (DS1)
DSP-COMM-FAIL (TRUNK)	LPBKFACILITY (E1)	SSM-STU (E1)

Table 2-6 ONS 15454 Alarm and Condition Alphabetical List (continued)

DSP-FAIL (TRUNK)	LPBKFACILITY (EC1)	SSM-STU (NE-SREF)
DUP-IPADDR (NE)	LPBKFACILITY (ESCON)	SSM-STU (OCN)
DUP-NODENAME (NE)	LPBKFACILITY (FC)	SSM-STU (TRUNK)
EHIBATVG (PWR)	LPBKFACILITY (FCMR)	SSM-TNC (BITS)
ELWBATVG (PWR)	LPBKFACILITY (G1000)	SSM-TNC (NE-SREF)
ENCAP-MISMATCH-P (STSTRM)	LPBKFACILITY (GE)	SSM-TNC (OCN)
ENVALRM)EXT	LPBKFACILITY (ISC)	SSM-TNC (TRUNK)
EOC (OCN)	LPBKFACILITY (OCN)	SWMTXMOD-PROT (EQPT)
EOC (TRUNK)	LPBKFACILITY (TRUNK)	SWMTXMOD-WORK (EQPT)
EOC-L (OCN)	LPBKTERMINAL (CE100T)	SWTOPRI (EXT-SREF)
EOC-L (TRUNK)	LPBKTERMINAL (DS1)	SWTOPRI (NE-SREF)
EQPT (AICI-AEP)	LPBKTERMINAL (DS3)	SWTOSEC (EXT-SREF)
EQPT (AICI-AIE)	LPBKTERMINAL (E1)	SWTOSEC (NE-SREF)
EQPT (EQPT)	LPBKTERMINAL (EC1)	SWTOTHIRD (EXT-SREF)
EQPT (PPM)	LPBKTERMINAL (ESCON)	SWTOTHIRD (NE-SREF)
EQPT-MISS (FAN)	LPBKTERMINAL (FC)	SYNC-FREQ (BITS)
ERFI-P-CONN (STSMON)	LPBKTERMINAL (FCMR)	SYNC-FREQ (DS1)
ERFI-P-CONN (STSTRM)	LPBKTERMINAL (G1000)	SYNC-FREQ (E1)
ERFI-P-PAYLD (STSMON)	LPBKTERMINAL (GE)	SYNC-FREQ (OCN)
ERFI-P-PAYLD (STSTRM)	LPBKTERMINAL (ISC)	SYNC-FREQ (TRUNK)
ERFI-P-SRVR (STSMON)	LPBKTERMINAL (OCN)	SYNCLOSS (FC)
ERFI-P-SRVR (STSTRM)	LPBKTERMINAL (TRUNK)	SYNCLOSS (FCMR)
ERROR-CONFIG (EQPT)	LWBATVG (PWR)	SYNCLOSS (GE)
ETH-LINKLOSS (NE)	MAN-REQ (EQPT)	SYNCLOSS (ISC)
E-W-MISMATCH (OCN)	MAN-REQ (STSMON)	SYNCLOSS (TRUNK)
EXCCOL (EQPT)	MAN-REQ (VT-MON)	SYNCPRI (EXT-SREF)
EXERCISE-RING-FAIL (OCN)	MANRESET (EQPT)	SYNCPRI (NE-SREF)
EXERCISE-SPAN-FAIL (OCN)	MANSWTOINT (NE-SREF)	SYNCSEC (EXT-SREF)
EXTRA-TRAF-PREEMPT (OCN)	MANSWTOPRI (EXT-SREF)	SYNCSEC (NE-SREF)
FAILTOSW (2R)	MANSWTOPRI (NE-SREF)	SYNCTHIRD (EXT-SREF)
FAILTOSW (EQPT)	MANSWTOSEC (EXT-SREF)	SYNCTHIRD (NE-SREF)
FAILTOSW (ESCON)	MANSWTOSEC (NE-SREF)	SYSBOOT (NE)
FAILTOSW (FC)	MANSWTOTHIRD (EXT-SREF)	TEMP-MISM (NE)
FAILTOSW (GE)	MANSWTOTHIRD (NE-SREF)	TIM (OCN)
FAILTOSW (ISC)	MANUAL-REQ-RING (OCN)	TIM (TRUNK)
FAILTOSW (OCN)	MANUAL-REQ-SPAN (2R)	TIM-MON (OCN)
FAILTOSW (TRUNK)	MANUAL-REQ-SPAN (ESCON)	TIM-MON (TRUNK)

Table 2-6 ONS 15454 Alarm and Condition Alphabetical List (continued)

FAILTOSW-PATH (STSMON)	MANUAL-REQ-SPAN (FC)	TIM-P (STSTRM)
FAILTOSW-PATH (VT-MON)	MANUAL-REQ-SPAN (GE)	TIM-P (STSMON)
FAILTOSWR (OCN)	MANUAL-REQ-SPAN (ISC)	TIM-S (EC1)
FAILTOSWS (OCN)	MANUAL-REQ-SPAN (OCN)	TIM-S (OCN)
FAN (FAN)	MANUAL-REQ-SPAN (TRUNK)	TIM-V (VT-TERM)
FC-NO-CREDITS (FC)	MEA (AIP)	TPTFAIL (CE100T)
FC-NO-CREDITS (FCMR)	MEA (BIC)	TPTFAIL (FCMR)
FC-NO-CREDITS (TRUNK)	MEA (EQPT)	TPTFAIL (G1000)
FE-AIS (DS3)	MEA (FAN)	TPTFAIL (ML1000)
FEC-MISM (TRUNK)	MEA (PPM)	TPTFAIL (ML100T)
FE-DS1-MULTLOS (DS3)	MEM-GONE (EQPT)	TPTFAIL (MLFX)
FE-DS1-NSA (DS3)	MEM-LOW (EQPT)	TRMT (DS1)
FE-DS1-SA (DS3)	MFGMEM (AICI-AEP)	TRMT (E1)
FE-DS1-SNGLLOS (DS3)	MFGMEM (AICI-AIE)	TRMT-MISS (DS1)
FE-DS3-NSA (DS3)	MFGMEM (AIP)	TRMT-MISS (E1)
FE-DS3-SA (DS3)	MFGMEM (BPLANE)	TX-AIS (DS1)
FE-EQPT-NSA (DS3)	MFGMEM (FAN)	TX-AIS (DS3)
FE-FRCDWKSWBK-SPAN (OCN)	MFGMEM (PPM)	TX-AIS (E1)
FE-FRCDWKSWPR-RING (OCN)	NO-CONFIG (EQPT)	TX-LOF (DS1)
FE-FRCDWKSWPR-SPAN (OCN)	NOT-AUTHENTICATED	TX-LOF (E1)
FE-IDLE (DS3)	OCHNC-INC (OCHNC-CONN)	TX-RAI (DS1)
FE-LOCKOUTOFPR-SPAN (OCN)	ODUK-1-AIS-PM (TRUNK)	TX-RAI (DS3)
FE-LOF (DS3)	ODUK-2-AIS-PM (TRUNK)	TX-RAI (E1)
FE-LOS (DS3)	ODUK-3-AIS-PM (TRUNK)	UNC-WORD (TRUNK)
FE-MANWKSWBK-SPAN (OCN)	ODUK-4-AIS-PM (TRUNK)	UNEQ-P (STSMON)
FE-MANWKSWPR-RING (OCN)	ODUK-AIS-PM (TRUNK)	UNEQ-P (STSTRM)
FE-MANWKSWPR-SPAN (OCN)	ODUK-BDI-PM (TRUNK)	UNEQ-V (VT-MON)
FEPRLF (OCN)	ODUK-LCK-PM (TRUNK)	UNEQ-V (VT-TERM)
FIBERTEMP-DEG (AOTS)	ODUK-OCI-PM (TRUNK)	UNREACHABLE-TARGET-POWER (OCH)
FORCED-REQ (EQPT)	ODUK-SD-PM (TRUNK)	UT-COMM-FAIL (TRUNK)
FORCED-REQ (STSMON)	ODUK-SF-PM (TRUNK)	UT-FAIL (TRUNK)
FORCED-REQ (VT-MON)	ODUK-TIM-PM (TRUNK)	VCG-DEG (VCG)
FORCED-REQ-RING (OCN)	OOU-TPT (STSTRM)	VCG-DOWN (VCG)
FORCED-REQ-SPAN (2R)	OOU-TPT (VT-TERM)	VOA-HDEG (AOTS)
FORCED-REQ-SPAN (ESCON)	OPEN-SLOT (EQPT)	VOA-HDEG (OCH)
FORCED-REQ-SPAN (FC)	OPTNTWMIS (NE)	VOA-HDEG (OMS)

Table 2-6 ONS 15454 Alarm and Condition Alphabetical List (continued)

FORCED-REQ-SPAN (GE)	OPWR-HDEG (AOTS)	VOA-HDEG (OTS)
FORCED-REQ-SPAN (ISC)	OPWR-HDEG (OCH)	VOA-HFAIL (AOTS)
FORCED-REQ-SPAN (OCN)	OPWR-HDEG (OMS)	VOA-HFAIL (OCH)
FORCED-REQ-SPAN (TRUNK)	OPWR-HDEG (OTS)	VOA-HFAIL (OMS)
FRCDSWTOINT (NE-SREF)	OPWR-HFAIL (AOTS)	VOA-HFAIL (OTS)
FRCDSWTOPRI (EXT-SREF)	OPWR-HFAIL (OCH)	VOA-LDEG (AOTS)
FRCDSWTOPRI (NE-SREF)	OPWR-HFAIL (OMS)	VOA-LDEG (OCH)
FRCDSWTOSEC (EXT-SREF)	OPWR-HFAIL (OTS)	VOA-LDEG (OMS)
FRCDSWTOSEC (NE-SREF)	OPWR-LDEG (AOTS)	VOA-LDEG (OTS)
FRCDSWTOTHIRD (EXT-SREF)	OPWR-LDEG (OCH)	VOA-LFAIL (AOTS)
FRCDSWTOTHIRD (NE-SREF)	OPWR-LDEG (OMS)	VOA-LFAIL (OCH)
FRNGSYNC (NE-SREF)	OPWR-LDEG (OTS)	VOA-LFAIL (OMS)
FSTSYNC (NE-SREF)	OPWR-LFAIL (AOTS)	VOA-LFAIL (OTS)
FULLPASSTHR-BI (OCN)	OPWR-LFAIL (OCH)	VOLT-MISM (PWR)
GAIN-HDEG (AOTS)	OPWR-LFAIL (OMS)	WKSWPR (2R)
GAIN-HFAIL (AOTS)	OPWR-LFAIL (OTS)	WKSWPR (EQPT)
GAIN-LDEG (AOTS)	OSRION (AOTS)	WKSWPR (ESCON)
GAIN-LFAIL (AOTS)	OSRION (OTS)	WKSWPR (FC)
GCC-EOC (TRUNK)	OTUK-AIS (TRUNK)	WKSWPR (GE)
GE-OOSYNC (FC)	OTUK-BDI (TRUNK)	WKSWPR (ISC)
GE-OOSYNC (GE)	OTUK-IAE (TRUNK)	WKSWPR (OCN)
GE-OOSYNC (ISC)	OTUK-LOF (TRUNK)	WKSWPR (STSMON)
GE-OOSYNC (TRUNK)	OTUK-SD (TRUNK)	WKSWPR (TRUNK)
GFP-CSF (CE100T)	OTUK-SF (TRUNK)	WKSWPR (VT-MON)
GFP-CSF (FCMR)	OTUK-TIM (TRUNK)	WTR (2R)
GFP-CSF (GFP-FAC)	OUT-OF-SYNC (FC)	WTR (EQPT)
GFP-CSF (ML1000)	OUT-OF-SYNC (GE)	WTR (ESCON)
GFP-CSF (ML100T)	OUT-OF-SYNC (ISC)	WTR (FC)
GFP-CSF (MLFX)	OUT-OF-SYNC (TRUNK)	WTR (GE)
GFP-DE-MISMATCH (FCMR)	PARAM-MISM (AOTS)	WTR (ISC)
GFP-DE-MISMATCH (GFP-FAC)	PARAM-MISM (OCH)	WTR (OCN)
GFP-EX-MISMATCH (FCMR)	PARAM-MISM (OMS)	WTR (STSMON)
GFP-EX-MISMATCH (GFP-FAC)	PARAM-MISM (OTS)	WTR (TRUNK)
GFP-LFD (CE100T)	PDI-P (STSMON)	WTR (VT-MON)
GFP-LFD (FCMR)	PDI-P (STSTRM)	WVL-MISMATCH (TRUNK)
GFP-LFD (GFP-FAC)	PEER-NORESPONSE (EQPT)	—

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 SONET or ITU-T G.709 optical overhead bits. One alarm can appear in multiple entries. It can be raised against multiple objects. For example, the loss of signal (LOS) alarm can be raised against the optical signal (OC-N) or the optical transport layer overhead (OTN) as well as other objects. Therefore, both OCN: LOS and OTN: LOS appear in the list (as well as the other objects).

Alarm profile list objects are defined in Table 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 "OCN" logical object refers to the OC-N signal. Logical object names or industry-standard terms are used within the entries as appropriate.

Table 2-7 Alarm Logical Object Type Definitions

Logical Object	Definition
2R	Reshape and retransmit (used for transponder [TXP] cards).
AICI-AEP	Alarm Interface Controller–International/alarm expansion panel. A combination term that refers to this platform's AIC-I card.
AICI-AIE	Alarm Interface Controller-International/Alarm Interface Extension. A combination term that refers to this platform's AIC-I card.
AOTS	Amplified optical transport section.
BIC	Backplane interface connector.
BITS	Building integrated timing supply incoming references (BITS-1, BITS-2).
BPLANE	The backplane.
CE100T	CE-100T-8 card.
DS1	A DS-1 line on a DS-1 or DS-3 electrical card (DS1-14, DS3N-12E, DS3XM-6, DS3XM-12).
DS3	A DS-3 line on a DS3-12, DS3N-12, DS3-12E, DS3XM-6, DS3XM-12, DS3/EC1-48 card.
E1	An E1 line on a DS1/E1-56 card.
E1000F	An E1000 Ethernet card (E1000-2, E1000-2G).
E100T	An E100 Ethernet card (E100T-12, E100T-G).
EC1	Any EC-1 port (including EC1-12 card ports).
ENVALRM	An environmental alarm port.
EQPT	A card, its physical objects, and its logical objects as they are located in any of the eight noncommon card slots. The EQPT object is used for alarms that refer to the card itself and all other objects on the card including ports, lines, synchronous transport signals (STS), and virtual tributaries (VT).
ESCON	Enterprise System Connection fiber optic technology, referring to the following TXP cards: TXP_MR_2.5G, TXPP_MR_2.5G.

Table 2-7 Alarm Logical Object Type Definitions (continued)

Logical Object	Definition
EXT-SREF	BITS outgoing references (SYNC-BITS1, SYNC-BITS2).
FAN	Fan-tray assembly.
FC	Fibre channel data transfer architecture, referring to the following muxponder (MXP) or TXP cards: MXP_MR_2.5G, MXPP_MR_2.5G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E.
FCMR	An FC_MR-4 Fibre Channel card.
FUDC	SONET F1 byte user data channel for ONS 15454 ML-Series Ethernet cards.
G1000	A G-Series Ethernet card.
GE	Gigabit Ethernet, referring to the following MXP or TXP cards: MXP_MR_2.5G, MXPP_MR_2.5G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, TXP_MR_10G.
GFP-FAC	Generic framing procedure facility port, referring to all MXP and TXP cards.
ISC	Inter-service channel, referring to TXPP_MR_2.5G or TXP_MR_2.5G cards.
ML1000	An ML1000 Ethernet card (ML1000-2).
ML100T	An ML100 Ethernet card (ML100T-12).
MLFX	An ML100X-8 Ethernet card.
MSUDC	Multiplex section user data channel.
NE	The entire network element.
NE-SREF	The timing status of the NE.
OCH	The optical channel, referring to dense wavelength division multiplexing (DWDM) cards.
OCHNC-CONN	The optical channel network connection, referring to DWDM cards.
OCN	An OC-N line on any OC-N card.
OMS	Optical multiplex section.
OSC-RING	Optical service channel ring.
OTS	Optical transport section.
PPM	Pluggable port module (PPM), referring to MXP and TXP cards.
PWR	Power equipment.
STSMON	STS alarm detection at the monitor point (upstream from the cross-connect).
STSTRM	STS alarm detection at termination (downstream from the cross-connect).
TRUNK	The optical or DWDM card carrying the high-speed signal; referring to MXP or TXP cards.
VCG	A virtual concatenation group of VTs.
VT-MON	VT1 alarm detection at the monitor point (upstream from the cross-connect).
VT-TERM	VT1 alarm detection at termination (downstream from the cross-connect).

2.4 Alarm List by Logical Object Type

Table 2-8 lists all ONS 15454 Release 6.0 alarms and logical objects as they are given in the system alarm profile. The list entries are organized by logical object name and then by alarm or condition name. Where appropriate, the alarm entries also contain troubleshooting procedures.

Note In a mixed network containing different types of nodes (such as ONS 15310-CL, ONS 15454, and ONS 15600), the initially displayed alarm list in the Provisioning > Alarm Profiles > Alarm Profile Editor tab lists all conditions that are applicable to all nodes in the network. However, when you load the default severity profile from a node, only applicable alarms will display severity levels. Nonapplicable alarms can display "use default" or "unset."

Note In some cases this list does not follow alphabetical order, but it does reflect the order shown in CTC.

Table 2-8 Alarm List by Logical Object in Alarm Profile

2R: ALS	EXT-SREF: SYNCPRI	OCN: RFI-L
2R: AS-CMD	EXT-SREF: SYNCSEC	OCN: RING-ID-MIS
2R: AS-MT	EXT-SREF: SYNCTHIRD	OCN: RING-MISMATCH
2R: FAILTOSW	FAN: EQPT-MISS	OCN: RING-SW-EAST
2R: FORCED-REQ-SPAN	FAN: FAN	OCN: RING-SW-WEST
2R: HI-LASERBIAS	FAN: MEA	OCN: SD-L
2R: HI-RXPOWER	FAN: MFGMEM	OCN: SF-L
2R: HI-TXPOWER	FC: ALS	OCN: SPAN-SW-EAST
2R: LO-RXPOWER	FC: AS-CMD	OCN: SPAN-SW-WEST
2R: LO-TXPOWER	FC: AS-MT	OCN: SQUELCH
2R: LOCKOUT-REQ	FC: CARLOSS	OCN: SQUELCHED
2R: LOS	FC: FAILTOSW	OCN: SSM-DUS
2R: MANUAL-REQ-SPAN	FC: FCC-NO-EDITS	OCN: SSM-FAIL
2R: SQUELCHED	FC: FORCED-REQ-SPAN	OCN: SSM-OFF
2R: WKSWPR	FC: GE-OOSYNC	OCN: SSM-PRS
2R: WTR	FC: HI-LASERBIAS	OCN: SSM-RES
AICI-AEP: EQPT	FC: HI-RXPOWER	OCN: SSM-SMC
AICI-AEP: MFGMEM	FC: HI-TXPOWER	OCN: SSM-ST2
AICI-AIE: EQPT	FC: LO-RXPOWER	OCN: SSM-ST3
AICI-AIE: MFGMEM	FC: LO-TXPOWER	OCN: SSM-ST3E
AIP: INVMACADR	FC: LOCKOUT-REQ	OCN: SSM-ST4
AIP: MEA	FC: LPBKFACILITY	OCN: SSM-STU
AIP: MFGMEM	FC: LPBKTERMINAL	OCN: SSM-TNC
AOTS: ALS	FC: MANUAL-REQ-SPAN	OCN: SYNC-FREQ

Table 2-8 Alarm List by Logical Object in Alarm Profile (continued)

AOTS: AMPLI-INIT	FC: OUT-OF-SYNC	OCN: TIM
AOTS: APC-CORRECTION-SKIPPED	FC: SIGLOSS	OCN: TIM-MON
AOTS: APC-OUT-OF-RANGE	FC: SQUELCHED	OCN: TIM-S
AOTS: AS-CMD	FC: SYNCLOSS	OCN: WKSWPR
AOTS: AS-MT	FC: WKSWPR	OCN: WTR
AOTS: CASETEMP-DEG	FC: WTR	OMS: APC-CORRECTION-SKIPPED
AOTS: FIBERTEMP-DEG	FCMR: AS-CMD	OMS: APC-OUT-OF-RANGE
AOTS: GAIN-HDEG	FCMR: AS-MT	OMS: AS-CMD
AOTS: GAIN-HFAIL	FCMR: FC-NO-EDITS	OMS: AS-MT
AOTS: GAIN-LDEG	FCMR: GFP-CSF	OMS: LOS-O
AOTS: GAIN-LFAIL	FCMR: GFP-DE-MISMATCH	OMS: LOS-P
AOTS: LASER-APR	FCMR: GFP-EX-MISMATCH	OMS: OPWR-HDEG
AOTS: LASERBIAS-DEG	FCMR: GFP-LFD	OMS: OPWR-HFAIL
AOTS: LASERBIAS-FAIL	FCMR: GFP-NO-BUFFERS	OMS: OPWR-LDEG
AOTS: LASERTEMP-DEG	FCMR: GFP-UP-MISMATCH	OMS: OPWR-LFAIL
AOTS: OPWR-HDEG	FCMR: LPBKFACILITY	OMS: PARAM-MISM
AOTS: OPWR-HFAIL	FCMR: LPBKTERMINAL	OMS: VOA-HDEG
AOTS: OPWR-LDEG	FCMR: PORT-MISMATCH	OMS: VOA-HFAIL
AOTS: OPWR-LFAIL	FCMR: SIGLOSS	OMS: VOA-LDEG
AOTS: OSRION	FCMR: SYNCLOSS	OMS: VOA-LFAIL
AOTS: PARAM-MISM	FCMR: TPTFAIL	OSC-RING: RING-ID-MIS
AOTS: VOA-HDEG	FUDC: AIS	OTS: APC-CORRECTION-SKIPPED
AOTS: VOA-HFAIL	FUDC: LOS	OTS: APC-OUT-OF-RANGE
AOTS: VOA-LDEG	G1000: AS-CMD	OTS: AS-CMD
AOTS: VOA-LFAIL	G1000: AS-MT	OTS: AS-MT
BIC: MEA	G1000: CARLOSS	OTS: AWG-DEG
BITS: AIS	G1000: LPBKFACILITY	OTS: AWG-FAIL
BITS: BPV	G1000: LPBKTERMINAL	OTS: AWG-OVERTEMP
BITS: HI-CCVOLT	G1000: TPTFAIL	OTS: AWG-WARM-UP
BITS: LOF	GE: ALS	OTS: LASERBIAS-DEG
BITS: LOS	GE: AS-CMD	OTS: LOS
BITS: SSM-DUS	GE: AS-MT	OTS: LOS-O
BITS: SSM-FAIL	GE: CARLOSS	OTS: LOS-P
BITS: SSM-OFF	GE: FAILTOSW	OTS: OPWR-HDEG
BITS: SSM-PRS	GE: FORCED-REQ-SPAN	OTS: OPWR-HFAIL
BITS: SSM-RES	GE: AGE-OOSYNC	OTS: OPWR-LDEG

Table 2-8 Alarm List by Logical Object in Alarm Profile (continued)

BITS: SSM-SMC	GE: HI-LASERBIAS	OTS: OPWR-LFAIL
BITS: SSM-ST2	GE: HI-RXPOWER	OTS: OSRION
BITS: SSM-ST3	GE: HI-TXPOWER	OTS: PARAM-MISM
BITS: SSM-ST3E	GE: LO-RXPOWER	OTS: SH-INS-LOSS-VAR-DEG-HIGH
BITS: SSM-ST4	GE: LO-TXPOWER	OTS: SH-INS-LOSS-VAR-DEG-LOW
BITS: SSM-STU	GE: LOCKOUT-REQ	OTS: SHUTTER-OPEN
BITS: SSM-TNC	GE: LPBKFACILITY	OTS: VOA-HDEG
BITS: SYNC-FREQ	GE: LPBKTERMINAL	OTS: VOA-HFAIL
BPLANE: AS-CMD	GE: MANUAL-REQ-SPAN	OTS: VOA-LDEG
BPLANE: MFGMEM	GE: OUT-OF-SYNC	OTS: VOA-LFAIL
CE100T: AS-CMD	GE: SIGLOSS	PPM: AS-CMD
CE100T: AS-MT	GE: SQUELCHED	PPM: AS-MT
CE100T: CARLOSS	GE: SYNCLOSS	PPM: EQPT
CE100T: GFP-CSF	GE: WKSWPR	PPM: HI-LASERBIAS
CE100T: GFP-LFD	GE: WTR	PPM: HI-LASERTEMP
CE100T: GFP-UP-MISMATCH	GFP-FAC: AS-CMD	PPM: HI-TXPOWER
CE100T: LPBKFACILITY	GFP-FAC: AS-MT	PPM: IMPROPRMVL
CE100T: LPBKTERMINAL	GFP-FAC: GFP-CSF	PPM: LO-LASERBIAS
CE100T: RPRW	GFP-FAC: GFP-DE-MISMATCH	PPM: LO-LASERTEMP
CE100T: TPTFAIL	GFP-FAC: GFP-EX-MISMATCH	PPM: LO-TXPOWER
DS1: AIS	GFP-FAC: GFP-LFD	PPM: MEA
DS1: AS-CMD	GFP-FAC: GFP-NO-BUFFERS	PPM: MFGMEM
DS1: AS-MT	GFP-FAC: GFP-UP-MISMATCH	PPM: PROV-MISMATCH
DS1: LOF	ISC: ALS	PWR: AS-CMD
DS1: LOS	ISC: AS-CMD	PWR: BAT-FAIL
DS1: LPBKDS1FEAC-CMD	ISC: AS-MT	PWR: EHIBATVG
DS1: LPBKFACILITY	ISC: CARLOSS	PWR: ELWBATVG
DS1: LPBKTERMINAL	ISC: FAILTOSW	PWR: HIBATVG
DS1: RAI	ISC: FORCED-REQ-SPAN	PWR: LWBATVG
DS1: RCVR-MISS	ISC: GE-OOSYNC	PWR: VOLT-MISM
DS1: SD	ISC: HI-LASERBIAS	STSMON: AIS-P
DS1: SF	ISC: HI-RXPOWER	STSMON: AUTOSW-AIS
DS1: SSM-DUS	ISC: HI-TXPOWER	STSMON: AUTOSW-LOP
DS1: SSM-FAIL	ISC: LO-RXPOWER	STSMON: AUTOSW-PDI
DS1: SSM-OFF	ISC: LO-TXPOWER	STSMON: AUTOSW-SDBER
DS1: SSM-PRS	ISC: LOCKOUT-REQ	STSMON: AUTOSW-SFBER
DS1: SSM-RES	ISC: LOS	STSMON: AUTOSW-UNEQ

Table 2-8 Alarm List by Logical Object in Alarm Profile (continued)

DS1: SSM-SMC	ISC: LPBKFACILITY	STSMON: ERFI-P-CONN
DS1: SSM-ST2	ISC: LPBKTERMINAL	STSMON: ERFI-P-PAYLD
DS1: SSM-ST3	ISC: MANUAL-REQ-SPAN	STSMON: ERFI-P-SRVR
DS1: SSM-ST3E	ISC: OUT-OF-SYNC	STSMON: FAILTOSW-PATH
DS1: SSM-ST4	ISC: SIGLOSS	STSMON: FORCED-REQ
DS1: SSM-STU	ISC: SQUELCHED	STSMON: LOCKOUT-REQ
DS1: SYNC-FREQ	ISC: SYNCLOSS	STSMON: LOM
DS1: TRMT	ISC: WKSWPR	STSMON: LOP-P
DS1: TRMT-MISS	ISC: WTR	STSMON: LPBKS
DS1: TX-AIS	ML1000: AS-CMD	STSMON: MAN-REQ
DS1: TX-LOF	ML1000: AS-MT	STSMON: PDI-P
DS1: TX-RAI	ML1000: CARLOSS	STSMON: PLM-P
DS3: AIS	ML1000: GFP-CSF	STSMON: RFI-P
DS3: AS-CMD	ML1000: GFP-LFD	STSMON: ROLL
DS3: AS-MT	ML1000: GFP-UP-MISMATCH	STSMON: ROLL-PEND
DS3: DS3-MISM	ML1000: RPRW	STSMON: SD-P
DS3: FE-AIS	ML1000: TPTFAIL	STSMON: SF-P
DS3: FE-DS1-MULTLOS	ML100T: AS-CMD	STSMON: TIM-P
DS3: FE-DS1-NSA	ML100T: AS-MT	STSMON: UNEQ-P
DS3: FE-DS1-SA	ML100T: CARLOSS	STSMON: WKSWPR
DS3: FE-DS1-SNGLLOS	ML100T: GFP-CSF	STSMON: WTR
DS3: FE-DS3-NSA	ML100T: GFP-LFD	STSTRM: AIS-P
DS3: FE-DS3-SA	ML100T: GFP-UP-MISMATCH	STSTRM: AS-MT-OOG
DS3: FE-EQPT-NSA	ML100T: RPRW	STSTRM: ENCAP-MISMATCH-P
DS3: FE-IDLE	ML100T: TPTFAIL	STSTRM: ERFI-P-CONN
DS3: FE-LOF	MLFX: AS-CMD	STSTRM: ERFI-P-PAYLD
DS3: FE-LOS	MLFX: AS-MT	STSTRM: ERFI-P-SRVR
DS3: INC-ISD	MLFX: CARLOSS	STSTRM: LCAS-C
DS3: LOF	MLFX: GFP-CSF	STSTRM: LCAS-RX-FAIL
DS3: LOS	MLFX: GFP-LFD	STSTRM: LCAS-TX-ADD
DS3: LPBKDS3FEAC	MLFX: GFP-UP-MISMATCH	STSTRM: LCAS-TX-DNU
DS3: LPBKDS3FEAC-CMD	MLFX: RPRW	STSTRM: LOF
DS3: LPBKFACILITY	MLFX: TPTFAIL	STSTRM: LOM
DS3: LPBKTERMINAL	MSUDC: AIS	STSTRM: LOP-P
DS3: RAI	MSUDC: LOS	STSTRM: LPBKS
DS3: SD	NE-SREF: FRCDSWTOINT	STSTRM: OOU-TPT
DS3: SF	NE-SREF: FRCDSWTOPRI	STSTRM: PDI-P

Table 2-8 Alarm List by Logical Object in Alarm Profile (continued)

DS3: TX-AIS	NE-SREF: FRCDSWTOSEC	STSTRM: PLM-P
DS3: TX-RAI	NE-SREF: FRCDSWTOTHIRD	STSTRM: RFI-P
E1000F: AS-CMD	NE-SREF: FRNGSYNC	STSTRM: ROLL
E1000F: CARLOSS	NE-SREF: FSTSYNC	STSTRM: ROLL-PEND
E100T: AS-CMD	NE-SREF: HLDOVRSYNC	STSTRM: SD-P
E100T: CARLOSS	NE-SREF: MANSWTOINT	STSTRM: SF-P
E1: AIS	NE-SREF: MANSWTOPRI	STSTRM: SQM
E1: AS-CMD	NE-SREF: MANSWTOSEC	STSTRM: TIM-P
E1: AS-MT	NE-SREF: MANSWTOTHIRD	STSTRM: UNEQ-P
E1: LOF	NE-SREF: SSM-PRS	TRUNK: AIS
E1: LOS	NE-SREF: SSM-RES	TRUNK: ALS
E1: LPBKFACILITY	NE-SREF: SSM-SMC	TRUNK: AS-CMD
E1: LPBKTERMINAL	NE-SREF: SSM-ST2	TRUNK: AS-MT
E1: RAI	NE-SREF: SSM-ST3	TRUNK: AUTOLSROFF
E1: RCVR-MISS	NE-SREF: SSM-ST3E	TRUNK: CARLOSS
E1: SD	NE-SREF: SSM-ST4	TRUNK: DSP-COMM-FAIL
E1: SF	NE-SREF: SSM-STU	TRUNK: DSP-FAIL
E1: SSM-DUS	NE-SREF: SSM-TNC	TRUNK: EOC
E1: SSM-FAIL	NE-SREF: SWTOPRI	TRUNK: EOC-L
E1: SSM-OFF	NE-SREF: SWTOSEC	TRUNK: FAILTOSW
E1: SSM-PRS	NE-SREF: SWTOTHIRD	TRUNK: FC-NO-EDITS
E1: SSM-RES	NE-SREF: SYNCPRI	TRUNK: FEC-MISM
E1: SSM-SMC	NE-SREF: SYNCSEC	TRUNK: FORCED-REQ-SPAN
E1: SSM-ST2	NE-SREF: SYNCTHIRD	TRUNK: GCC-EOC
E1: SSM-ST3	NE: APC-DISABLED	TRUNK: GE-OOSYNC
E1: SSM-ST3E	NE: APC-END	TRUNK: HI-LASERBIAS
E1: SSM-ST4	NE: AS-CMD	TRUNK: HI-RXPOWER
E1: SSM-STU	NE: AUD-LOG-LOSS	TRUNK: HI-TXPOWER
E1: SYNC-FREQ	NE: AUD-LOG-LOW	TRUNK: LO-RXPOWER
E1: TRMT	NE: DATAFLT	TRUNK: LO-TXPOWER
E1: TRMT-MISS	NE: DBOSYNC	TRUNK: LOCKOUT-REQ
E1: TX-AIS	NE: DUP-IPADDR	TRUNK: LOF
E1: TX-LOF	NE: DUP-NODEME	TRUNK: LOM
E1: TX-RAI	NE: ETH-LINKLOSS	TRUNK: LOS
EC1: AIS-L	NE: HITEMP	TRUNK: LOS-P
EC1: AS-CMD	NE: I-HITEMP	TRUNK: LPBKFACILITY
EC1: AS-MT	NE: INTRUSION-PSWD	TRUNK: LPBKTERMINAL

Table 2-8 Alarm List by Logical Object in Alarm Profile (continued)

EC1: LOF	NE: LAN-POL-REV	TRUNK: MANUAL-REQ-SPAN
EC1: LOS	NE: OPTNTWMIS	TRUNK: ODUK-1-AIS-PM
EC1: LPBKFACILITY	NE: SNTP-HOST	TRUNK: ODUK-2-AIS-PM
EC1: LPBKTERMINAL	NE: SYSBOOT	TRUNK: ODUK-3-AIS-PM
EC1: RFI-L	NE: TEMP-MISM	TRUNK: ODUK-4-AIS-PM
EC1: SD-L	OCH: APC-CORRECTION-SKIPPED	TRUNK: ODUK-AIS-PM
EC1: SF-L	OCH: APC-OUT-OF-RANGE	TRUNK: ODUK-BDI-PM
EC1: TIM-S	OCH: AS-CMD	TRUNK: ODUK-LCK-PM
ENVALRM: EXT	OCH: AS-MT	TRUNK: ODUK-OCI-PM
EQPT: AS-CMD	OCH: LOS-O	TRUNK: ODUK-SD-PM
EQPT: AS-MT	OCH: LOS-P	TRUNK: ODUK-SF-PM
EQPT: AUTORESET	OCH: OPWR-HDEG	TRUNK: ODUK-TIM-PM
EQPT: BKUPMEMP	OCH: OPWR-HFAIL	TRUNK: OTUK-AIS
EQPT: CARLOSS	OCH: OPWR-LDEG	TRUNK: OTUK-BDI
EQPT: CLDRESTART	OCH: OPWR-LFAIL	TRUNK: OTUK-IAE
EQPT: COMIOXC	OCH: PARAM-MISM	TRUNK: OTUK-LOF
EQPT: COMM-FAIL	OCH: PORT-ADD-PWR-DEG-HI	TRUNK: OTUK-SD
EQPT: CONTBUS-A-18	OCH: PORT-ADD-PWR-DEG-LOW	TRUNK: OTUK-SF
EQPT: CONTBUS-B-18	OCH: PORT-ADD-PWR-FAIL-HIGH	TRUNK: OTUK-TIM
EQPT: CONTBUS-DISABLED	OCH: PORT-ADD-PWR-FAIL-LOW	TRUNK: OUT-OF-SYNC
EQPT: CONTBUS-IO-A	OCH: PORT-FAIL	TRUNK: PTIM
EQPT: CONTBUS-IO-B	OCH: UEACHABLE-TARGET-POWER	TRUNK: RFI
EQPT: CTNEQPT-MISMATCH	OCH: VOA-HDEG	TRUNK: SD
EQPT: CTNEQPT-PBPROT	OCH: VOA-HFAIL	TRUNK: SF
EQPT: CTNEQPT-PBWORK	OCH: VOA-LDEG	TRUNK: SIGLOSS
EQPT: EQPT	OCH: VOA-LFAIL	TRUNK: SQUELCHED
EQPT: ERROR-CONFIG	OCHNC-CONN: OCHNC-INC	TRUNK: SSM-DUS
EQPT: EXCCOL	OCN: AIS-L	TRUNK: SSM-FAIL
EQPT: FAILTOSW	OCN: ALS	TRUNK: SSM-LNC
EQPT: FORCED-REQ	OCN: APS-INV-PRIM	TRUNK: SSM-OFF
EQPT: HI-LASERBIAS	OCN: APS-PRIM-FAC	TRUNK: SSM-PRC
EQPT: HI-LASERTEMP	OCN: APS-PRIM-SEC-MISM	TRUNK: SSM-PRS
EQPT: HI-TXPOWER	OCN: APSB	TRUNK: SSM-RES
EQPT: HITEMP	OCN: APSC-IMP	TRUNK: SSM-SDH-TN
EQPT: IMPROPRMVL	OCN: APSCDFLTK	TRUNK: SSM-SETS
EQPT: INHSWPR	OCN: APSCINCON	TRUNK: SSM-SMC
EQPT: INHSWWKG	OCN: APSCM	TRUNK: SSM-ST2

Table 2-8 Alarm List by Logical Object in Alarm Profile (continued)

EQPT: IOSCFGCOPY	OCN: APSCNMIS	TRUNK: SSM-ST3
EQPT: LO-LASERBIAS	OCN: APSIMP	TRUNK: SSM-ST3E
EQPT: LO-LASERTEMP	OCN: APSMM	TRUNK: SSM-ST4
EQPT: LO-TXPOWER	OCN: AS-CMD	TRUNK: SSM-STU
EQPT: LOCKOUT-REQ	OCN: AS-MT	TRUNK: SSM-TNC
EQPT: MAN-REQ	OCN: AUTOLSROFF	TRUNK: SYNC-FREQ
EQPT: MAESET	OCN: BLSR-SW-VER-MISM	TRUNK: SYNCLOSS
EQPT: MEA	OCN: BLSROSYNC	TRUNK: TIM
EQPT: MEM-GONE	OCN: E-W-MISMATCH	TRUNK: TIM-MON
EQPT: MEM-LOW	OCN: EOC	TRUNK: UNC-WORD
EQPT: NO-CONFIG	OCN: EOC-L	TRUNK: UT-COMM-FAIL
EQPT: OPEN-SLOT	OCN: EXERCISE-RING-FAIL	TRUNK: UT-FAIL
EQPT: PEER-NORESPONSE	OCN: EXERCISE-SPAN-FAIL	TRUNK: WKSWPR
EQPT: PROT	OCN: EXTRA-TRAF-PREEMPT	TRUNK: WTR
EQPT: PWR-FAIL-A	OCN: FAILTOSW	TRUNK: WVL-MISMATCH
EQPT: PWR-FAIL-B	OCN: FAILTOSWR	VCG: LOA
EQPT: PWR-FAIL-RET-A	OCN: FAILTOSWS	VCG: VC-DEG
EQPT: PWR-FAIL-RET-B	OCN: FE-FRCDWKSWBK-SPAN	VCG: VC-DOWN
EQPT: RUNCFG-SAVENEED	OCN: FE-FRCDWKSWPR-RING	VT-MON: AIS-V
EQPT: SFTWDOWN	OCN: FE-FRCDWKSWPR-SPAN	VT-MON: AUTOSW-AIS
EQPT: SWMTXMOD-PROT	OCN: FE-LOCKOUTOFPR-SPAN	VT-MON: AUTOSW-LOP
EQPT: SWMTXMOD-WORK	OCN: FE-MANWKSWBK-SPAN	VT-MON: AUTOSW-UNEQ
EQPT: WKSWPR	OCN: FE-MANWKSWPR-RING	VT-MON: FAILTOSW-PATH
EQPT: WTR	OCN: FE-MANWKSWPR-SPAN	VT-MON: FORCED-REQ
ESCON: ALS	OCN: FEPRLF	VT-MON: LOCKOUT-REQ
ESCON: AS-CMD	OCN: FORCED-REQ-RING	VT-MON: LOP-V
ESCON: AS-MT	OCN: FORCED-REQ-SPAN	VT-MON: MAN-REQ
ESCON: FAILTOSW	OCN: FULLPASSTHR-BI	VT-MON: ROLL
ESCON: FORCED-REQ-SPAN	OCN: HELLO	VT-MON: ROLL-PEND
ESCON: HI-LASERBIAS	OCN: HI-LASERBIAS	VT-MON: SD-V
ESCON: HI-RXPOWER	OCN: HI-LASERTEMP	VT-MON: SF-V
ESCON: HI-TXPOWER	OCN: HI-RXPOWER	VT-MON: UNEQ-V
ESCON: LO-RXPOWER	OCN: HI-TXPOWER	VT-MON: WKSWPR
ESCON: LO-TXPOWER	OCN: ISIS-ADJ-FAIL	VT-MON: WTR
ESCON: LOCKOUT-REQ	OCN: KB-PASSTHR	VT-TERM: AIS-V
ESCON: LOS	OCN: KBYTE-APS-CHANNEL-FAILURE	VT-TERM: AS-MT-OOG

Table 2-8 Alarm List by Logical Object in Alarm Profile (continued)

ESCON: LPBKFACILITY	OCN: LASEREOL	VT-TERM: LCAS-C
ESCON: LPBKTERMINAL	OCN: LKOUTPR-S	VT-TERM: LCAS-RX-FAIL
ESCON: MANUAL-REQ-SPAN	OCN: LO-LASERBIAS	VT-TERM: LCAS-TX-ADD
ESCON: SQUELCHED	OCN: LO-LASERTEMP	VT-TERM: LCAS-TX-DNU
ESCON: WKSWPR	OCN: LO-RXPOWER	VT-TERM: LOM
ESCON: WTR	OCN: LO-TXPOWER	VT-TERM: LOP-V
EXT-SREF: FRCDSWTOPRI	OCN: LOCKOUT-REQ	VT-TERM: OOU-TPT
EXT-SREF: FRCDSWTOSEC	OCN: LOF	VT-TERM: PLM-V
EXT-SREF: FRCDSWTOTHIRD	OCN: LOS	VT-TERM: RFI-V
EXT-SREF: MANSWTOPRI	OCN: LPBKFACILITY	VT-TERM: SD-V
EXT-SREF: MANSWTOSEC	OCN: LPBKTERMINAL	VT-TERM: SF-V
EXT-SREF: MANSWTOTHIRD	OCN: MANUAL-REQ-RING	VT-TERM: SQM
EXT-SREF: SWTOPRI	OCN: MANUAL-REQ-SPAN	VT-TERM: TIM-V
EXT-SREF: SWTOSEC	OCN: PRC-DUPID	VT-TERM: UNEQ-V
EXT-SREF: SWTOTHIRD	—	—

2.5 DS3-12 E Line Alarms

Unlike the standard DS-3 card, which uses the unframed format exclusively, the DS3-12E card's ports provide three choices: unframed, M13, or C Bit. The choice of framing format determines the line alarms that the DS3-12E card reports. The following table lists the line alarms reported under each format.

The choice of framing format does not affect the reporting of STS alarms. Regardless of format, the DS3-12E card reports the same STS alarms and conditions, listed in Table 2-9, as the standard DS-3 card reports.

Table 2-9 DS3-12E Line Alarms

Alarm	UNFRAMED	M13	CBIT
LOS (DS1 or DS3)	Yes	Yes	Yes
AIS	Yes	Yes	Yes
LOF (DS1 or DS3)	No	Yes	Yes
FE-IDLE	No	Yes	Yes
RAI	No	Yes	Yes
Terminal Lpbk (LPBKTERMINAL for DS1 or DS3)	Yes	Yes	Yes
Facility Lpbk (LPBKFACILITY for DS1 or DS3)	Yes	Yes	Yes
LPBKDS1FEAC or LPBKDS3FEAC	No	No	Yes

Table 2-9 DS3-12E Line Alarms (continued)

Alarm	UNFRAMED	M13	CBIT
FE Common Equipment Failure-NSA (FE-DS1-NSA or FE-DS3-NSA)	No	No	Yes
FE Equipment Failure-SA (FE-DS3-SA)	No	No	Yes
FE-LOS	No	No	Yes
FE-LOF	No	No	Yes
FE-AIS	No	No	Yes
FE-IDLE	No	No	Yes
FE Equipment Failure-NSA (FE-EQPT-NSA)	No	No	Yes

2.6 Trouble Notifications

The ONS 15454 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 15454 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.

2.6.1 Alarm Characteristics

The ONS 15454 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.)

2.6.2 Condition Characteristics

Conditions include any problem detected on an ONS 15454 shelf. They can include standing or transient notifications. A snapshot of all current raised, standing conditions on the network, node, or card can be retrieved in the CTC Conditions window or using TL1's set of RTRV-COND commands. (In addition, some but not all cleared conditions are also found in the History tab.)

For a comprehensive list of all conditions, refer to the *Cisco SONET TL1 Command Guide* .

2.6.3 Severities

The ONS 15454 uses Telcordia-devised standard severities for alarms and conditions: Critical (CR), Major (MJ), Minor (MN), Not Alarmed (NA) and Not Reported (NR). These are described below:

- A Critical (CR) alarm generally indicates severe, Service-Affecting (SA) trouble that needs immediate correction. Loss of traffic on an STS-1, which can hold 28 DS-1 circuits, would be a Critical (CR), Service-Affecting (SA) alarm.
- A Major (MJ) alarm is a serious alarm, but the trouble has less impact on the network. For example, loss of traffic on more than five DS-1 circuits is Critical (CR), but loss of traffic on one to four DS-1 circuits is Major (MJ).
- Minor (MN) alarms generally are those that do not affect service. For example, the automatic protection switching (APS) byte failure (APSB) alarm indicates that line terminating equipment (LTE) detects a byte failure on the signal that could prevent traffic from properly executing a traffic switch.
- Not Alarmed (NA) conditions are information indicators, such as for free-run synchronization state (FRNGSYNC) or a forced-switch to primary (FRCSWTOPRI) timing event. They could or could not require troubleshooting, as indicated in the entries.
- Not Reported (NR) conditions occur as a secondary result of another event. For example, the alarm indication signal (AIS), with severity NR, is inserted by a downstream node when an LOS (CR or MJ) alarm occurs upstream. These conditions do not in themselves require troubleshooting, but are to be expected in the presence of primary alarms.

Severities can be customized for an entire network or for single nodes, from the network level down to the port level by changing or downloading customized alarm profiles. These custom severities are subject to the standard severity-demoting rules given in Telcordia GR-474-CORE and shown in the 2.6.4 Alarm Hierarchy section. Procedures for customizing alarm severities are located in the "Manage Alarms" chapter in the *Cisco ONS 15454 Procedure Guide*.

2.6.4 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 a path trace identifier mismatch (TIM-P) is raised on a circuit path and then a loss of pointer on the path (LOP-P) is raised on the path, the LOP-P alarm stands and the TIM-P closes. The path alarm hierarchy used in the ONS 15454 system is shown in Table 2-10.

Table 2-10 Path Alarm Hierarchy

Priority	Condition Type
Highest	AIS-P
—	LOP-P
—	UNEQ-P
Lowest	TIM-P

Facility (port) alarms also follow a hierarchy, which means that lower-ranking alarms are closed by higher-ranking alarms. The facility alarm hierarchy used in the ONS 15454 is shown in Table 2-11.

Table 2-11 Facility Alarm Hierarchy

Priority	Condition Type
Highest	LOS
—	LOF
—	AIS-L
—	SF-L
—	SD-L
—	RFI-L
—	TIM-S
—	AIS-P
—	LOP-P
—	SF-P
—	SD-P
—	UNEQ-P
—	TIM-P
Lowest	PLM-P

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 (AIS-L), path (AIS-P, etc.) or VT (AIS-V, etc.). The full hierarchy for near-end failures is shown in Table 2-12. This table is taken from Telcordia GR-253-CORE.

Table 2-12 Near-End Alarm Hierarchy

Priority	Condition Type
Highest	LOS
—	LOF
—	AIS-L
—	AIS-P[1]
—	LOP-P[2]
—	UNEQ-P
—	TIM-P
—	PLM-P
—	AIS-V[1]
—	LOP-V[2]
—	UNEQ-V
—	PLM-V
Lowest	DS-N AIS (if reported for outgoing DS-N signals)

1. Although it is not defined as a defect or failure, all-ones STS pointer relay is also higher priority than LOP-P. Similarly, all-ones VT pointer relay is higher priority than LOP-V.
2. LOP-P is also higher priority than the far-end failure RFI-P, which does not affect the detection of any near-end failures. Similarly, LOP-V is higher priority than RFI-V.

The far-end failure alarm hierarchy is shown in Table 2-13, as given in Telcordia GR-253-CORE.

Table 2-13 Far-End Alarm Hierarchy

Priority	Condition Type
Highest	RFI-L
—	RFI-P
Lowest	RFI-V

2.6.5 Service Effect

Service-Affecting (SA) alarms—those that interrupt service—could be Critical (CR), Major (MJ), or Minor (MN) severity alarms. Service-Affecting (SA) alarms indicate service is affected. Non-Service-Affecting (NSA) alarms always have a Minor (MN) default severity.

2.6.6 States

The Alarms or History tab State (ST) column indicate the disposition of the alarm or condition as follows:

- A raised (R) event is one that is active.
- A cleared (C) event is one that is no longer active.
- A transient (T) event is one that is automatically raised and cleared in CTC during system changes such as user login, logout, loss of connection to node view, etc. Transient events do not require user action. These are listed in Chapter 3, "Transients Conditions."

2.7 Safety Summary

This section covers safety considerations designed to ensure safe operation of the ONS 15454. Personnel should not perform any procedures in this chapter unless they understand all safety precautions, practices, and warnings for the system equipment. Some troubleshooting procedures require installation or removal of cards; in these instances users should pay close attention to the following caution.

Caution Hazardous voltage or energy could be present on the backplane when the system is operating. Use caution when removing or installing cards.

Some troubleshooting procedures require installation or removal of OC-192 cards; in these instances users should pay close attention to the following warnings.

Warning **On the OC-192 card, the laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. The laser is off when the safety key is off (labeled 0).** Statement 293

Warning **Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard.** Statement 1056

Warning **Use of controls, adjustments, or performing procedures other than those specified could result in hazardous radiation exposure.** Statement 1057

Warning **Class 1 laser product.** Statement 1008

Warning **Do not reach into a vacant slot or chassis while you install or remove a module or a fan. Exposed circuitry could constitute an energy hazard.** Statement 206

Warning **The power supply circuitry for the equipment can constitute an energy hazard. Before you install or replace the equipment, remove all jewelry (including rings, necklaces, and watches). Metal objects can come into contact with exposed power supply wiring or circuitry inside the DSLAM equipment. This could cause the metal objects to heat up and cause serious burns or weld the metal object to the equipment.** Statement 207

2.8 Alarm Procedures

This section list alarms alphabetically and includes some conditions commonly encountered when troubleshooting alarms. The severity, description, and troubleshooting procedure accompany each alarm and condition.

Note When you check the status of alarms for cards, ensure that the alarm filter icon in the lower right corner of the GUI is not indented. If it is, click it to turn it off. When you are done checking for alarms, you can click the alarm filter icon again to turn filtering back on. For more information about alarm filtering, refer to the "Manage Alarms" chapter in the *Cisco ONS 15454 Procedure Guide*.

Note When checking alarms, ensure that alarm suppression is not enabled on the card or port. For more information about alarm suppression, refer to the "Manage Alarms" chapter in the *Cisco ONS 15454 Procedure Guide.*

2.8.1 AIS

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

SONET Logical Objects: BITS, DS1, DS3, E1, FUDC, MSUDC

DWDM Logical Object: TRUNK

The Alarm Indication Signal (AIS) condition indicates that this node is detecting an alarm indication signal in the incoming signal SONET overhead.

Generally, any AIS is a special SONET signal that communicates to the receiving node when the transmit node does not send a valid signal. AIS is not considered an error. It is raised by the receiving node on each input when it detects the AIS instead of a real signal. In most cases when this condition is raised, an upstream node is raising an alarm to indicate a signal failure; all nodes downstream from it only raise some type of AIS. This condition clears when you resolved the problem on the upstream node.

Note ONS 15454 DS-3 terminal (inward) loopbacks do not transmit an AIS in the direction away from the loopback. Instead of AIS, a continuance of the signal transmitted into the loopback is provided. A DS3/EC1-48 card can be provisioned to transmit AIS for a terminal loopback.

Clear the AIS Condition

Step 1 Determine whether there are alarms on the upstream nodes and equipment, especially the "LOS (OCN)" alarm on page 2-147, or if there are out-of-service (OOS,MT or OOS,DSBLD) ports.

Step 2 Clear the upstream alarms using the applicable procedures in this chapter.

Step 3 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.2 AIS-L

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

SONET Logical Objects: EC1, OCN

The AIS Line condition indicates that this node is detecting line-level AIS in the incoming signal. This alarm is secondary to another alarm occurring simultaneously in an upstream node.

This condition can also be raised in conjunction with the "TIM-S" alarm on page 2-217 if AIS-L is enabled.

Note ONS 15454 DS-3 terminal (inward) loopbacks do not transmit an AIS in the direction away from the loopback. Instead of AIS, a continuance of the signal transmitted into the loopback is provided. A DS3/EC1-48 card can be provisioned to transmit AIS for a terminal loopback.

Clear the AIS-L Condition

Step 1 Complete the "Clear the AIS Condition" procedure on page 2-32.

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).

2.8.3 AIS-P

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

SONET Logical Objects: STSMON, STSTRM

The AIS Path condition means that this node is detecting AIS in the incoming path. This alarm is secondary to another alarm occurring simultaneously in an upstream node.

Clear the AIS-P Condition

Step 1 Complete the "Clear the AIS Condition" procedure on page 2-32.

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).

2.8.4 AIS-V

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

SONET Logical Objects: VT-MON, VT-TERM

The AIS VT condition means that this node is detecting AIS in the incoming VT-level path.

See the "1.13.2 AIS-V on DS3XM-6 or DS3XM-12 Unused VT Circuits" section on page 1-141 for more information.

Clear the AIS-V Condition

Step 1 Complete the "Clear the AIS Condition" procedure on page 2-32.

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).

2.8.5 ALS

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.6 AMPLI-INIT

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.7 APC-CORRECTION-SKIPPED

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.8 APC-DISABLED

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.9 APC-END

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.10 APC-OUT-OF-RANGE

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.11 APSB

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: OCN

The APS Channel Byte Failure alarm occurs when LTE detects protection switching byte failure or an invalid switching code in the incoming APS signal. Some older SONET not manufactured by Cisco send invalid APS codes if they are configured in a 1+1 protection group with newer SONET nodes, such as the ONS 15454. These invalid codes cause an APSB alarm on an ONS 15454.

Step 1 Use an optical test set to examine the incoming SONET overhead to confirm inconsistent or invalid K bytes. For specific procedures to use the test set equipment, consult the manufacturer. If corrupted K bytes are confirmed and the upstream equipment is functioning properly, the upstream equipment might not interoperate effectively with the ONS 15454.

Step 2 If the alarm does not clear and the overhead shows inconsistent or invalid K bytes, you could need to replace the upstream cards for protection switching to operate properly. Complete the "Physically Replace a Traffic Card" procedure on page 2-243.

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).

2.8.12 APSCDFLTK

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: OCN

The APS Default K Byte Received alarm occurs during bidirectional line switched ring (BLSR) provisioning or when a BLSR is not properly configured, for example, when a four-node BLSR has one node configured as a path protection. When this misconfiguration occurs, a node in a path protection or 1+1 configuration does not send the two valid K1/K2 APS bytes anticipated by a system configured for BLSR. One of the bytes sent is considered invalid by the BLSR configuration. The K1/K2 byte is monitored by receiving equipment for link-recovery information.

Troubleshooting for APSCDFLTK is often similar to troubleshooting for the "BLSROSYNC" alarm on page 2-51.

Clear the APSCDFLTK Alarm

Step 1 Complete the "Identify a BLSR Ring Name or Node ID Number" procedure on page 2-230 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 a BLSR Node ID Number" procedure on page 2-230 to change one node ID number so that each node ID is unique.

Step 4 If the alarm does not clear, verify correct configuration of east port and west port optical fibers. (See the "E-W-MISMATCH" alarm on page 2-82.) West port fibers must connect to east port fibers and east port fibers must connect to west port fibers. The "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15454 Procedure Guide* provides procedures for fibering BLSRs.

Step 5 If the alarm does not clear and the network is a four-fiber BLSR, 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 2-231.

Step 7 If nodes are not visible, complete the "Verify or Create Node Section DCC Terminations" procedure on page 2-245 to ensure that section data communications channel (SDCC) 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).

2.8.13 APSC-IMP

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: OCN

An Improper SONET 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 VT tunnel when it does not have VT 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 traffic is preempted.

Note The APSC-IMP alarm may be raised on a BLSR or MS-SPRing when a drop connection is part of a cross-connect loopback.

Note The APSC-IMP alarm may be momentarily raised on BLSR spans during PCA circuit creation or deletion across multiple nodes using CTC.

Warning **Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard.** Statement 1056

Warning **Use of controls, adjustments, or performing procedures other than those specified could result in hazardous radiation exposure.** Statement 1057

Clear the APSC-IMP Alarm

Step 1 Use an optical test set to determine the validity of the K byte signal by examining the received signal. For specific procedures to use the test set equipment, consult the manufacturer.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. 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 15454. Troubleshoot the upstream equipment using the procedures in this chapter, as applicable. If the upstream nodes are not ONS 15454s, 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 a BLSR Ring Name or Node ID Number" procedure on page 2-230.

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 a BLSR Ring Name" procedure on page 2-230.

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).

2.8.14 APSCINCON

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: OCN

An APS Inconsistent alarm means that an inconsistent APS byte is present. The SONET overhead contains K1/K2 APS bytes that notify receiving equipment, such as the ONS 15454, to switch the SONET 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 (OCN)" alarm on page 2-147, the "LOF (OCN)" alarm on page 2-135, or the "AIS" condition on page 2-32. Clearing these alarms clears the APSCINCON alarm.

Step 2 If an APSINCON alarm occurs with no other alarms, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.15 APSCM

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Object: OCN

The APS Channel Mismatch alarm occurs when the ONS 15454 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 15454 when bidirectional protection is used on OC-N cards in a 1+1 protection group configuration. The APSCM alarm does not occur in an optimized 1+1 protection configuration.

Warning **On the ONS 15454 OC-192 card, the laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. The laser is off when the safety key is off (labeled 0).** Statement 293

Warning **Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard.** Statement 1056

Warning **Use of controls, adjustments, or performing procedures other than those specified could result in hazardous radiation exposure.** Statement 1057

Clear the APSCM Alarm

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 1 Verify that the working-card channel fibers are physically connected directly to the adjoining node's working-card channel fibers.

Step 2 If the fibers are correctly connected, verify that the protection-card channel fibers are physically connected directly to the adjoining node'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) in order to report a Service-Affecting (SA) problem.

2.8.16 APSCNMIS

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Object: OCN

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 BLSR 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 a BLSR Ring Name or Node ID Number" procedure on page 2-230 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 a BLSR Node ID Number" procedure on page 2-230 to change one node ID number so that each node ID is unique.

Note If the node names shown in the network view do not correlate with the node IDs, log into each node and click the **Provisioning > BLSR** tabs. The BLSR window shows the node ID of the login node.

Note Applying and removing a lockout on a span causes the ONS node to generate a new K byte. The APSCNMIS alarm clears when the node receives a K byte containing the correct node ID.

Step 5 If the alarm does not clear, use the "Initiate a Lockout on a BLSR Protect Span" procedure on page 2-238 to lock out the span.

Step 6 Complete the "Clear a BLSR External Switching Command" procedure on page 2-239 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) in order to report a Service-Affecting (SA) problem.

2.8.17 APSIMP

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: OCN

The APS Invalid Code alarm occurs if a 1+1 protection group is not properly configured at both nodes to send or receive the correct APS byte. A node that is either configured for no protection or is configured for path protection or BLSR protection does not send the right K2 APS byte anticipated by a system configured for 1+1 protection. The 1+1 protect port monitors the incoming K2 APS byte and raises this alarm if it does not receive the byte.

The alarm is superseded by an APSCM or APSMM alarm, but not by an AIS condition. It clears when the port receives a valid code for 10 ms.

Clear the APSIMP Alarm

Step 1 Check the configuration of the other node in the 1+1 protection group. If the far end is not configured for 1+1 protection, create the group. For procedures, refer to the "Turn Up Node" chapter in the *Cisco ONS 15454 Procedure Guide*.

Step 2 If the other end of the group is properly configured or the alarm does not clear after you have provisioned the group correctly, verify that the working ports and protect ports are cabled correctly.

Step 3 Ensure that both protect ports are configured for SONET.

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).

2.8.18 APS-INV-PRIM

Default Severity: Minor (MN), Non-Service Affecting (NSA)

SONET Logical Object: OCN

The Optimized 1+1 APS Primary Facility condition occurs on OC-N cards in an optimized 1+1 protection system if the incoming primary section header does not indicate whether it is primary or secondary.

Note APS-INV-PRIM is an informational condition and does not require troubleshooting. If the APS switch is related to other alarms, troubleshoot these alarms as necessary using the procedures in this chapter.

2.8.19 APSMM

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: OCN

An APS Mode Mismatch failure alarm occurs on OC-N cards when there is a mismatch of the protection switching schemes at the two ends of the span, such as being bidirectional at one end and unidirectional at the other. Each end of a span must be provisioned the same way: bidirectional and bidirectional, or unidirectional and unidirectional. APSMM can also occur if third-party equipment is provisioned as 1:N and the ONS 15454 is provisioned as 1+1.

If one end is provisioned for 1+1 protection switching and the other is provisioned for path protection protection switching, an APSMM alarm occurs in the ONS 15454 that is provisioned for 1+1 protection switching.

Clear the APSMM Alarm

Step 1 For the reporting ONS 15454, display node view and verify the protection scheme provisioning:

a. Click the **Provisioning > Protection** tabs.

b. Click the 1+1 protection group configured for the OC-N cards.

The chosen protection group is the protection group optically connected (with data communications channel, or DCC, connectivity) to the far end.

c. Click **Edit**.

d. Record whether the Bidirectional Switching check box is checked.

Step 2 Click **OK** in the Edit Protection Group dialog box.

Step 3 Log into the far-end node and verify that the OC-N 1+1 protection group is provisioned.

Step 4 Verify that the Bidirectional Switching check box matches the checked or unchecked condition of the box recorded in Step 1. If not, change it to match.

Step 5 Click **Apply**.

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).

2.8.20 APS-PRIM-FAC

Default Severity: Not Alarmed (NA), Non-Service Affecting (NSA)

SONET Logical Object: OCN

The Optimized 1+1 APS Invalid Primary Section condition occurs on OC-N cards in an optimized 1+1 protection system if there is an APS status switch between the primary and secondary facilities to identify which port is primary.

Note APS-PRIM-FAC is an informational condition and does not require troubleshooting. If the APS switch is related to other alarms, troubleshoot these alarms as necessary using the procedures in this chapter.

Clear the APS-PRIM-FAC Condition

Step 1 This condition clears when the card receives a valid primary section indication (1 or 2).

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).

2.8.21 APS-PRIM-SEC-MISM

Default Severity: Minor (MN), Non-Service Affecting (NSA)

SONET Logical Object: OCN

The Optimized 1+1 APS Primary Section Mismatch condition occurs on OC-N cards in an optimized 1+1 protection system if there is a mismatch between the primary section of the local node facility and the primary section of the remote-node facility.

Clear the APS-PRIM-SEC-MISM Alarm

Step 1 Ensure that the local node and remote-node ports are correctly provisioned the same way. For more information about optimized 1+1 configurations, refer to the "Turn Up Node" chapter in the *Cisco ONS 15454 Procedure Guide*.

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).

2.8.22 AS-CMD

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: BPLANE, CE100T, DS1, DS3, E1, E100T, E1000F, EC1, EQPT, FCMR, G1000, GFP-FAC, ML100T, MLFX, NE, OCN, PWR

DWDM Logical Objects: 2R, AOTS, ESCON, FC, GE, ISC, OCH, OMS, OTS, PPM, TRUNK

The Alarms Suppressed by User Command condition applies to the network element (NE object), backplane, a single card, or a port on a card. It occurs when alarms are suppressed for that object and its subordinate objects. For example, suppressing alarms on a card also suppresses alarms on its ports.

Note For more information about suppressing alarms, refer to the "Manage Alarms" chapter in the *Cisco ONS 15454 Procedure Guide*.

Clear the AS-CMD Condition

Step 1 For all nodes, in node view, click the **Conditions** tab.

Step 2 Click **Retrieve**. If you have already retrieved conditions, look under the Object column and Eqpt Type column and note what entity the condition is reported against, such as a port, slot, or shelf.

- If the condition is reported against a slot and card, alarms were either suppressed for the entire card or for one of the ports. Note the slot number and continue with Step 3.
- If the condition is reported against the backplane, go to Step 7.
- If the condition is reported against the NE object, go to Step 8.

Step 3 Determine whether alarms are suppressed for a port and if so, raise the suppressed alarms:

a. Double-click the card to open the card view.

b. Click the **Provisioning > Alarm Profiles > Alarm Behavior** tabs and complete one of the following substeps:

- If the Suppress Alarms column check box is checked for a port row, deselect it and click **Apply**.
- If the Suppress Alarms column check box is not checked for a port row, from the View menu choose **Go to Previous View**.

Step 4 If the AS-CMD condition is reported for a card and not an individual port, in node view click the **Provisioning > Alarm Profiles > Alarm Behavior** tabs.

Step 5 Locate the row number for the reported card slot.

Step 6 Click the **Suppress Alarms** column check box to deselect the option for the card row.

Step 7 If the condition is reported for the backplane, the alarms are suppressed for cards such as the ONS 15454 AIP that are not in the optical or electrical slots. To clear the alarm, complete the following steps:

a. In node view, click the **Provisioning > Alarm Profiles > Alarm Behavior** tabs.

b. In the backplane row, uncheck the **Suppress Alarms** column check box.

c. Click **Apply**.

Step 8 If the condition is reported for the shelf, cards and other equipment are affected. To clear the alarm, complete the following steps:

a. In node view, click the **Provisioning > Alarm Profiles > Alarm Behavior** tabs if you have not already done so.

b. Click the **Suppress Alarms** check box located at the bottom of the window to deselect the option.

c. Click **Apply**.

Step 9 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.23 AS-MT

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: CE100T, DS1, DS3, E1, EC1, EQPT, FCMR, G1000, GFP-FAC, ML100T, MLFX, OCN

DWDM Logical Objects: 2R, AOTS, ESCON, FC, GE, ISC,OCH, OMS, OTS, PPM, TRUNK

The Alarms Suppressed for Maintenance Command condition applies to OC-N and electrical cards and occurs when a port is placed in the Out-of-Service and Management, Maintenance (OOS-MA,MT) service state for loopback testing operations.

Clear the AS-MT Condition

Step 1 Complete the "Clear an OC-N Card Facility or Terminal Loopback Circuit" procedure on page 2-245.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.24 AS-MT-OOG

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: STSTRM, VT-TERM

The Alarms Suppressed on an Out-Of-Group VCAT Member condition is raised on an STS or VT member of a VCAT group whenever the member is in the IDLE (AS-MT-OOG) admin state. This condition can be raised when a member is initially added to a group. In the IDLE (AS-MT-OOG) state, all other alarms for the STS or VT are suppressed.

The AS-MT-OOG condition clears when an STS or VT member transitions to a different state from IDLE (AS-MT-OOG) or when the member is removed completely from the VCAT group. The condition does not require troubleshooting unless it does not clear.

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).

2.8.25 AUD-LOG-LOSS

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: NE

The Audit Trail Log Loss condition occurs when the log is 100 percent full and the oldest entries are being replaced while 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).

2.8.26 AUD-LOG-LOW

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET 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 and does not require troubleshooting.

2.8.27 AU-LOF

The Administrative Unit Loss of Multiframe alarm is not supported in this platform release. It is reserved for future development.

2.8.28 AUTOLSROFF

Default Severity: Critical (CR), Service-Affecting (SA)

SONET Logical Object: OCN

DWDM Logical Object: TRUNK

The Auto Laser Shutdown alarm occurs when the OC-192 card temperature exceeds 194 degrees F (90 degrees C). The internal equipment automatically shuts down the OC-192 laser when the card temperature rises to prevent the card from self-destructing.

Warning **On the ONS 15454 OC-192 card, the laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. The laser is off when the safety key is off (labeled 0).** Statement 293

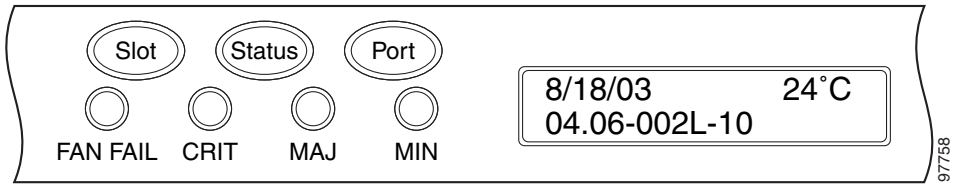
Warning **Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard.** Statement 1056

Warning **Use of controls, adjustments, or performing procedures other than those specified could result in hazardous radiation exposure.** Statement 1057

Clear the AUTOLSROFF Alarm

Step 1 View the temperature displayed on the ONS 15454 LCD front panel (Figure 2-1).

Figure 2-1 Shelf LCD Panel



Step 2 If the temperature of the shelf exceeds 194 degrees F (90 degrees C), the alarm should clear if you solve the ONS 15454 temperature problem. Complete the "Clear the HITEMP Alarm" procedure on page 2-115.

Step 3 If the temperature of the shelf is under 194 degrees F (90 degrees C), the HITEMP alarm is not the cause of the AUTOLSROFF alarm. Complete the "Physically Replace a Traffic Card" procedure on page 2-243 for the OC-192 card.

Step 4 If card replacement does not clear the alarm, call Cisco TAC (1 800 553-2447) to discuss the case and if necessary open a returned materials authorization (RMA) on the original OC-192 card.

2.8.29 AUTORESET

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: EQPT

The Automatic System Reset alarm occurs when you change an IP address or perform any other operation that causes an automatic card-level reboot.

AUTORESET typically clears after a card reboots (up to ten minutes). If the alarm does not clear, complete the following procedure.

Clear the AUTORESET Alarm

Step 1 Determine whether there are additional alarms that could have triggered an automatic reset. If there are, troubleshoot these alarms using the applicable section of this chapter.

Step 2 If the card automatically resets more than once a month with no apparent cause, complete the "Physically Replace a Traffic Card" procedure on page 2-243.

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).

2.8.30 AUTOSW-AIS

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

SONET Logical Objects: STSMON, VT-MON

The Automatic path protection Switch Caused by an AIS condition indicates that automatic path protection protection switching occurred because of an AIS condition. If the path protection is configured for revertive switching, it reverts to the working path after the fault clears. The AIS also clears when the upstream trouble is cleared.

Generally, any AIS is a special SONET signal that communicates to the receiving node when the transmit node does not send a valid signal. AIS is not considered an error. It is raised by the receiving node on each input when it detects the AIS instead of a real signal. In most cases when this condition is raised, an upstream node is raising an alarm to indicate a signal failure; all nodes downstream from it only raise some type of AIS. This condition clears when you resolved the problem on the upstream node.

Clear the AUTOSW-AIS Condition

Step 1 Complete the "Clear the AIS Condition" procedure on page 2-32.

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).

2.8.31 AUTOSW-LOP (STSMON)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: STSMON

The Automatic path protection Switch Caused by LOP condition for the STS monitor (STSMON) indicates that automatic path protection protection switching occurred because of the "LOP-P" alarm on page 2-138. If the path protection is configured for revertive switching, it reverts to the working path after the fault clears.

Clear the AUTOSW-LOP (STSMON) Condition

Step 1 Complete the "Clear the LOP-P Alarm" procedure on page 2-138.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.32 AUTOSW-LOP (VT-MON)

Default Severity: Not Alarmed (NA), Service-Affecting (SA)

SONET Logical Object: VT-MON

The AUTOSW-LOP alarm for the VT monitor (VT-MON) indicates that automatic path protection switching occurred because of the "LOP-V" alarm on page 2-139. If the path protection is configured for revertive switching, it reverts to the working path after the fault clears.

Clear the AUTOSW-LOP (VT-MON) Condition

Step 1 Complete the "Clear the LOP-V Alarm" procedure on page 2-139.

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.

2.8.33 AUTOSW-PDI

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: STSMON

The Automatic Path Protection Switch Caused by Payload Defect Indication (PDI) condition indicates that automatic path protection protection switching occurred because of a "PDI-P" alarm on page 2-174. If the path protection is configured for revertive switching, it reverts to the working path after the fault clears.

Clear the AUTOSW-PDI Condition

Step 1 Complete the "Clear the PDI-P Condition" procedure on page 2-175.

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).

2.8.34 AUTOSW-SDBER

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: STSMON

The Automatic Path Protection Switch Caused by Signal Degrade Bit Error Rate (SDBER) condition indicates that a signal degrade (SD) caused automatic path protection switching to occur. (See the "SD-L" condition on page 2-193.) If the path protection is configured for revertive switching, it reverts to the working path when the SD is resolved.

Clear the AUTOSW-SDBER Condition

Step 1 Complete the "Clear the SD (DS1, DS3) Condition" procedure on page 2-191.

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).

2.8.35 AUTOSW-SFBER

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: STSMON

The Automatic USPR Switch Caused by Signal Fail Bit Error Rate (SFBER) condition indicates that a signal failure (SF) caused automatic path protection switching to occur. If the path protection is configured for revertive switching, it reverts to the working path when the SF is resolved.

Clear the AUTOSW-SFBER Condition

Step 1 Complete the "Clear the SF (DS1, DS3) Condition" procedure on page 2-195.

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).

2.8.36 AUTOSW-UNEQ (STSMON)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: STSMON

The Automatic Path Protection Switch Caused by Unequipped condition indicates that a UNEQ alarm caused automatic path protection switching to occur. If the path protection is configured for revertive switching, it reverts to the working path after the fault clears.

Clear the AUTOSW-UNEQ (STSMON) Condition

Step 1 Complete the "Clear the UNEQ-P Alarm" procedure on page 2-223.

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).

2.8.37 AWG-DEG

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.38 AWG-FAIL

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.39 AWG-OVERTEMP

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.40 AWG-WARM-UP

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.41 BAT-FAIL

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Object: PWR

The Battery Fail alarm occurs when one of the two power supplies (A or B) is not detected. This could be because the supply is removed or is not operational. The alarm does not distinguish between the individual power supplies, so onsite information about the conditions is necessary for troubleshooting.

Clear the BAT-FAIL Alarm

Step 1 At the site, determine which battery is not present or operational.

Step 2 Remove the power cable from the faulty supply. For procedures, refer to the "Install the Shelf and Backplane Cable" chapter in the *Cisco ONS 15454 Procedure Guide*. Reverse the power cable installation procedure.

Step 3 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

2.8.42 BKUPMEMP

Default Severity: Critical (CR), Service-Affecting (SA)

SONET Logical Object: EQPT

The Primary Nonvolatile Backup Memory Failure alarm refers to a problem with the TCC2/TCC2P flash memory. The alarm occurs when the TCC2/TCC2P is in use and has one of four problems:

- Flash manager fails to format a flash partition.
- Flash manager fails to write a file to a flash partition.
- Problem at the driver level.
- Code volume fails cyclic redundancy checking (CRC, a method to verify for errors in data transmitted to the TCC2/TCC2P).

The BKUPMEMP alarm can also cause the "EQPT" alarm on page 2-77. If the EQPT alarm is caused by BKUPMEMP, complete the following procedure to clear the BKUPMEMP and the EQPT alarm.

Caution A software update on a standby TCC2/TCC2P can take up to 30 minutes.

Clear the BKUPMEMP Alarm

Step 1 Verify that both TCC2/TCC2Ps are powered and enabled by confirming lighted ACT/SBY LEDs on the TCC2/TCC2Ps.

Step 2 Determine whether the active or standbyTCC2/TCC2P has the alarm.

Step 3 If both TCC2/TCC2Ps are powered and enabled, reset the TCC2/TCC2P where the alarm is raised. If the card is the active TCC2/TCC2P, complete the "Reset an Active TCC2/TCC2P Card and Activate the Standby Card" procedure on page 2-240. If the card is the standby TCC2/TCC2P:

a. Right-click the standby TCC2/TCC2P in CTC.

b. Choose **Reset Card** from the shortcut menu.

c. Click **Yes** in the Are You Sure dialog box. The card resets, the FAIL LED blinks on the physical card.

d. Wait ten minutes to verify that the card you reset completely reboots.

Step 4 If the TCC2/TCC2P you reset does not reboot successfully, or the alarm has not cleared, call Cisco TAC (1 800 553-2447). If the Cisco TAC technician tells you to reseat the card, complete the "Remove and Reinsert (Reseat) the Standby TCC2/TCC2P Card" procedure on page 2-241. If the Cisco TAC technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Traffic Card" procedure on page 2-243.

2.8.43 BLSROSYNC

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Object: OCN

The BLSR Out Of Synchronization alarm occurs during BLSR setup when you attempt to add or delete a circuit, and a working ring node loses its DCC connection because all transmit and receive fiber has been removed. CTC cannot generate the ring table and causes the BLSROSYNC 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 could result in hazardous radiation exposure.** Statement 1057

Note This alarm can also be expected when upgrading to Release 6.0 if the ring identifier is updated.

Clear the BLSROSYNC Alarm

Step 1 Reestablish cabling continuity to the node reporting the alarm. Refer to the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15454 Procedure Guide* for cabling information to reestablish the DCC. To verify cable continuity, follow site practices.

When the DCC is established between the node and the rest of the BLSR, it becomes visible to the BLSR and should be able to function on the circuits.

Step 2 If alarms occur when you have provisioned the DCCs, see the "EOC" alarm on page 2-74.

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.

2.8.44 BLSR-SW-VER-MISM

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Object: OCN

The BLSR Software Version Mismatch alarm is raised by the TCC2/TCC2P when it checks all software versions for all nodes in a ring and discovers a mismatch in versions.

Clear the BLSR-SW-VER-MISM Alarm

Step 1 Clear the alarm by loading the correct software version on the TCC2/TCC2P 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 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) condition.

2.8.45 BPV

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: BITS

The 64K Clock Bipolar Density Violation alarm is raised on the TCC2P card if there is a frequency variation in the 8K BITS clock.

The TCC2P card contains an 8K clock and a 64K clock. Each has some bipolar variation, which is normal. This alarm is raised on the 8K clock if that variation discontinues. The BPV alarm is demoted by an LOF or LOS against the BITS clock.

Note This alarm is not raised on the TCC2 card.

Clear the BPV Alarm

Step 1 Reestablishing a normal BITS input signal clears the alarm. Clear any alarms on the incoming signal or against the BITS timing sources.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

2.8.46 CARLOSS (CE100T)

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Objects: CE100T

The Carrier Loss alarm is raised on CE-100T-8 cards in Mapper mode when there is a circuit failure due to link integrity. It does not get raised when a user simply puts the port in the In-Service and Normal (IS-NR) state. It has to be IS-NR with a circuit or loopback.

Note For more information about Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.*

Clear the CARLOSS (CE100T) Alarm

Step 1 Complete the "Clear the CARLOSS (G1000) Alarm" procedure on page 2-57. However, rather than checking for a TPTFAIL (G1000) at the end of the procedure, check for a "TPTFAIL (CE100T)" alarm on page 2-218.

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.

2.8.47 CARLOSS (E100T, E1000F)

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Objects: E100T, E1000F

A Carrier Loss alarm on the LAN E-Series Ethernet card is the data equivalent of the "LOS (OCN)" alarm on page 2-147. The Ethernet card has lost its link and is not receiving a valid signal. The most common causes of the CARLOSS alarm are a disconnected cable, an Ethernet Gigabit Interface Converter (GBIC) fiber connected to an optical card rather than an Ethernet device, or an improperly installed Ethernet card. Ethernet card ports must be enabled for CARLOSS to occur. CARLOSS is declared after no signal is received for approximately 2.5 seconds.

The CARLOSS alarm also occurs after a node database is restored. After restoration, the alarm clears in approximately 30 seconds after the node reestablishes Spanning Tree Protocol (STP).

Note For more information about Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.

Clear the CARLOSS (E100T, E1000F) Alarm

Step 1 Verify that the fiber cable is properly connected and attached to the correct port. For more information about fiber connections and terminations, refer to the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15454 Procedure Guide*.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 2 If the fiber cable is properly connected and attached to the port, verify that the cable connects the card to another Ethernet device and is not misconnected to an OC-N card. For more information about fiber connections and terminations, refer to the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15454 Procedure Guide*.

Step 3 If no misconnection to an OC-N card exists, verify that the transmitting device is operational. If not, troubleshoot the device.

Step 4 If the alarm does not clear, use an Ethernet test set to determine whether a valid signal is coming into the Ethernet port. For specific procedures to use the test set equipment, consult the manufacturer.

Step 5 If a valid Ethernet signal is not present and the transmitting device is operational, replace the fiber cable connecting the transmitting device to the Ethernet port. To do this, refer to the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15454 Procedure Guide*.

Step 6 If a valid Ethernet signal is present, complete the "Remove and Reinsert (Reseat) Any Card" procedure on page 2-242 for the Ethernet card.

Step 7 If the alarm does not clear, complete the "Physically Replace a Traffic Card" procedure on page 2-243 for the Ethernet card.

Step 8 If a CARLOSS alarm repeatedly appears and clears, use the following steps to examine the layout of your network to determine whether the Ethernet circuit is part of an Ethernet manual cross-connect.

An Ethernet manual cross-connect is used when another vendor's equipment sits between ONS 15454 nodes, and the open systems interconnect/target identifier address resolution protocol (OSI/TARP)-based equipment does not allow tunneling of the ONS 15454 TCP/IP-based DCC. To circumvent a lack of continuous DCC, the Ethernet circuit is manually cross connected to an STS channel riding through the non-ONS network.

If the reporting Ethernet circuit is part of an Ethernet manual cross-connect, complete the following steps. The reappearing alarm could be a result of mismatched STS circuit sizes in the set up of the manual cross-connect. If the Ethernet circuit is not part of a manual cross-connect, the following steps do not apply.

a. Right-click anywhere in the row of the CARLOSS alarm.

b. Click **Select Affected Circuits** in the shortcut menu that appears.

c. Record the information in the type and size columns of the highlighted circuit.

d. From the examination of the layout of your network, determine which ONS 15454 and card and card are hosting the Ethernet circuit at the other end of the Ethernet manual cross-connect and complete the following substeps:

- Log into the ONS 15454 at the other end of the Ethernet manual cross-connect.
- Double-click the Ethernet card that is part of the Ethernet manual cross-connect.
- Click the **Circuits** tab.
- Record the information in the type and size columns of the circuit that is part of the Ethernet manual cross-connect. The Ethernet manual cross-connect circuit connects the Ethernet card to an OC-N card at the same node.

e. Use the information you recorded to determine whether the two Ethernet circuits on each side of the Ethernet manual cross-connect have the same circuit size.

If one of the circuit sizes is incorrect, complete the "Delete a Circuit" procedure on page 2-244 and reconfigure the circuit with the correct circuit size. For more information, refer to the "Create Circuits and VT Tunnels" chapter in the *Cisco ONS 15454 Procedure Guide*.

Step 9 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

2.8.48 CARLOSS (EQPT)

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Object: EQPT

A Carrier Loss on the LAN Equipment alarm generally occurs on OC-N cards when the ONS 15454 and the workstation hosting CTC do not have a TCP/IP connection. The problem involves the LAN or data circuit used by the RJ-45 (LAN) connector on the TCC2/TCC2P or the LAN backplane pin connection. This CARLOSS alarm does not involve an Ethernet circuit connected to an Ethernet port. The problem is in the connection and not CTC or the node.

On TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G or MXP_2.5G_10G cards, CARLOSS is also raised against trunk ports when ITU-T G.709 monitoring is turned off.

A TXP_MR_2.5G card can raise a CARLOSS alarm when the payload is incorrectly configured for the 10 Gigabit Ethernet or 1 Gigabit Ethernet payload data types.

Warning **Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard.** Statement 1056

Warning **Use of controls, adjustments, or performing procedures other than those specified could result in hazardous radiation exposure.** Statement 1057

Note For more information about provisioning MXP or TXP PPMs, refer to the "Provision Transponder and Muxponder Cards" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For more information about the cards themselves, refer to the "Card Reference" chapter. For more information about MRC-12 and OC192-XFP/STM64-XFP cards, refer to the "Change Card Settings" chapter of the *Cisco ONS 15454 Procedure Guide*. For more information about Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.

Clear the CARLOSS (EQPT) Alarm

Step 1 If the reporting card is an MXP or TXP card in an ONS 15454 node, verify the data rate configured on the pluggable port module (PPM):

- **a.** Double-click the reporting MXP or TXP card.
- **b.** Click the **Provisioning > Pluggable Port Modules** tabs.
- **c.** View the Pluggable Port Modules area port listing in the **Actual Equipment Type** column and compare this with the contents of the Selected PPM area Rate column for the MXP or TXP multirate port.
- **d.** If the rate does not match the actual equipment, you must delete and recreate the selected PPM. Select the PPM, click **Delete**, then click **Create** and choose the correct rate for the port rate.

Step 2 If the reporting card is an OC-N card, verify connectivity by pinging the ONS 15454 that is reporting the alarm by completing the procedure in the "Verify PC Connection to the ONS 15454 (ping)" procedure on page 1-124.

Step 3 If the ping is successful, it demonstrates that an active TCP/IP connection exists. Restart CTC:

- **a.** Exit from CTC.
- **b.** Reopen the browser.

c. Log into CTC.

Step 4 Using optical test equipment, verify that proper receive levels are achieved. (For instructions to use optical test equipment, refer to the manufacturer documentation.)

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 5 Verify that the optical LAN cable is properly connected and attached to the correct port. For more information about fiber connections and terminations, refer to the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15454 Procedure Guide.*

Step 6 If the fiber cable is properly connected and attached to the port, verify that the cable connects the card to another Ethernet device and is not misconnected to an OC-N card.

Step 7 If you are unable to establish connectivity, replace the fiber cable with a new known-good cable. To do this, refer to the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15454 Procedure Guide*.

Step 8 If you are unable to establish connectivity, perform standard network or LAN diagnostics. For example, trace the IP route, verify cable continuity, and troubleshoot any routers between the node and CTC. To verify cable continuity, follow site practices.

Step 9 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

2.8.49 CARLOSS (FC)

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.50 CARLOSS (G1000)

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Object: G1000

A Carrier Loss alarm on the LAN G-Series Ethernet card is the data equivalent of the "LOS (OCN)" alarm on page 2-147. The Ethernet card has lost its link and is not receiving a valid signal.

CARLOSS on the G1000-4 card is caused by one of two situations:

- The G1000-4 port reporting the alarm is not receiving a valid signal from the attached Ethernet device. The CARLOSS can be caused by an improperly connected Ethernet cable or a problem with the signal between the Ethernet device and the G1000-4 port.
- If a problem exists in the end-to-end path (including possibly the far-end G1000-4 card), it causes the reporting card to turn off the Gigabit Ethernet transmitter. Turning off the transmitter typically causes the attached device to turn off its link laser, which results in a CARLOSS on the reporting G1000-4 card. The root cause is the problem in the end-to-end path. When the root cause is cleared, the far-end G1000-4 port turns the transmitter laser back on and clears the CARLOSS on the

reporting card. If a turned-off transmitter causes the CARLOSS alarm, other alarms such as the "TPTFAIL (G1000)" alarm on page 2-219 or OC-N alarms or conditions on the end-to-end path normally accompany the CARLOSS (G1000s) alarm.

Refer to the *Cisco ONS 15454 Reference Manual* for a description of the G1000-4 card's end-to-end Ethernet link integrity capability. Also see the "TRMT" alarm on page 2-221 for more information about alarms that occur when a point-to-point circuit exists between two cards.

Ethernet card ports must be enabled for CARLOSS to occur. CARLOSS is declared after no signal is received for approximately 2.5 seconds.

Note For more information about Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.

Clear the CARLOSS (G1000) Alarm

Step 1 Verify that the fiber cable is properly connected and attached to the correct port. For more information about fiber connections and terminations, refer to the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15454 Procedure Guide*.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 2 If the fiber cable is correctly connected and attached, verify that the cable connects the card to another Ethernet device and is not misconnected to an OC-N card.

Step 3 If no misconnection to the OC-N card exists, verify that the attached transmitting Ethernet device is operational. If not, troubleshoot the device.

Step 4 Verify that optical receive levels are within the normal range. The correct specifications are listed in the "1.14.3 OC-N Card Transmit and Receive Levels" section on page 1-154.

Step 5 If the alarm does not clear, use an Ethernet test set to determine whether a valid signal is coming into the Ethernet port. For specific procedures to use the test set equipment, consult the manufacturer.

Step 6 If a valid Ethernet signal is not present and the transmitting device is operational, replace the fiber cable connecting the transmitting device to the Ethernet port. To do this, refer to the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15454 Procedure Guide*.

Step 7 If the alarm does not clear, and link autonegotiation is enabled on the port but the autonegotiation process fails, the card turns off its transmitter laser and reports a CARLOSS alarm. If link autonegotiation has been enabled for the port, determine whether there are conditions that could cause autonegotiation to fail:

a. Confirm that the attached Ethernet device has autonegotiation enabled and is configured for compatibility with the asymmetric flow control on the card.

b. Confirm that the attached Ethernet device configuration allows reception of flow control frames.

Step 8 If the alarm does not clear, disable and reenable the Ethernet port to attempt to remove the CARLOSS condition. (The autonegotiation process restarts.)

Step 9 If the alarm does not clear and the "TPTFAIL (G1000)" alarm on page 2-219 is also reported, complete the "Clear the TPTFAIL (G1000) Alarm" procedure on page 2-219. If the TPTFAIL alarm is not raised, continue to the next step.

Note When the CARLOSS and the TPTFAIL alarms are reported, the reason for the condition could be the G1000-4 card's end-to-end link integrity feature taking action on a remote failure indicated by the TPTFAIL alarm.

Step 10 If the TPTFAIL alarm was not raised, determine whether a terminal (inward) loopback has been provisioned on the port:

a. In node view, click the card to go to card view.

b. Click the **Maintenance > Loopback tabs**.

c. If the service state is listed as OOS-MA,LPBK&MT, a loopback is provisioned. Go to Step 11.

Step 11 If a loopback was provisioned, complete the "Clear Other Electrical Card, CE-100T-8, or Ethernet Card Loopbacks" procedure on page 2-246.

On the G1000-4, provisioning a terminal (inward) loopback causes the transmit laser to turn off. If an attached Ethernet device detects the loopback as a loss of carrier, the attached Ethernet device shuts off the transmit laser to the G1000-4 card. Terminating the transmit laser could raise the CARLOSS alarm because the loopbacked G1000-4 port detects the termination.

If the does not have a loopback condition, continue to Step 12.

Step 12 If a CARLOSS alarm repeatedly appears and clears, the reappearing alarm could be a result of mismatched STS circuit sizes in the setup of the manual cross-connect. Perform the following steps if the Ethernet circuit is part of a manual cross-connect:

Note An ONS 15454 Ethernet manual cross-connect is used when another vendor's equipment sits between ONS nodes, and the OSI/TARP-based equipment does not allow tunneling of the ONS 15454 TCP/IP-based DCC. To circumvent a lack of continuous DCC, the Ethernet circuit is manually cross connected to an STS channel riding through the non-ONS network.

a. Right-click anywhere in the row of the CARLOSS alarm.

b. Right-click or left-click **Select Affected Circuits** in the shortcut menu that appears.

c. Record the information in the type and size columns of the highlighted circuit.

d. Examine the layout of your network and determine which ONS 15454 and card are hosting the Ethernet circuit at the other end of the Ethernet manual cross-connect and complete the following substeps:

- Log into the node at the other end of the Ethernet manual cross-connect.
- Double-click the Ethernet card that is part of the Ethernet manual cross-connect.
- Click the **Circuits** tab.
- Record the information in the type and size columns of the circuit that is part of the Ethernet manual cross-connect. The cross-connect circuit connects the Ethernet card to an OC-N card at the same node.

e. Determine whether the two Ethernet circuits on each side of the Ethernet manual cross-connect have the same circuit size from the circuit size information you recorded.

f. If one of the circuit sizes is incorrect, complete the "Delete a Circuit" procedure on page 2-244 and reconfigure the circuit with the correct circuit size. Refer to the "Create Circuits and VT Tunnels" chapter in the *Cisco ONS 15454 Procedure Guide* for detailed procedures to create circuits.

Step 13 If a valid Ethernet signal is present, complete the "Remove and Reinsert (Reseat) Any Card" procedure on page 2-242.

Step 14 If the alarm does not clear, complete the "Physically Replace a Traffic Card" procedure on page 2-243 for the Ethernet card.

Step 15 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.

2.8.51 CARLOSS (GE)

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.52 CARLOSS (ISC)

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.53 CARLOSS (ML100T, ML1000, MLFX)

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Objects: ML100T, ML1000, MLFX

A Carrier Loss alarm on an ML-Series Ethernet card is the data equivalent of the "LOS (OCN)" alarm on page 2-147. The Ethernet port has lost its link and is not receiving a valid signal.

A CARLOSS alarm occurs when the Ethernet port has been configured from the Cisco IOS command line interface (CLI) as a no-shutdown port and one of the following problems also occurs:

- The cable is not properly connected to the near or far port.
- Autonegotiation is failing.
- The speed (10/100 ports only) is set incorrectly.

Note For information about provisioning ML-Series Ethernet cards from the Cisco IOS interface, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.

Clear the CARLOSS (ML100T, ML1000, MLFX) Alarm

Step 1 Verify that the LAN cable is properly connected and attached to the correct port on the ML-Series card and on the peer Ethernet port. For more information about fiber connections and terminations, refer to the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15454 Procedure Guide*.

Step 2 If the alarm does not clear, verify that autonegotiation is set properly on the ML-Series card port and the peer Ethernet port.

Step 3 If the alarm does not clear, verify that the speed is set properly on the ML-Series card port and the peer Ethernet port if you are using 10/100 ports.

Step 4 If the alarm does not clear, the Ethernet signal is not valid, but the transmitting device is operational, replace the LAN cable connecting the transmitting device to the Ethernet port.

Step 5 If the alarm does not clear, disable and reenable the Ethernet port by performing a "shutdown" and then a "no shutdown" on the Cisco IOS CLI. Autonegotiation restarts.

Step 6 If the alarm does not clear, complete the "Create the Facility (Line) Loopback on the Source DS-1, DS-3, DS3N-12, DS3i-N-12, or EC1 Port" procedure on page 1-11 and test the loopback.

Step 7 If the problem persists with the loopback installed, complete the "Remove and Reinsert (Reseat) Any Card" procedure on page 2-242.

Step 8 If the alarm does not clear, complete the "Physically Replace a Traffic Card" procedure on page 2-243.

Step 9 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

2.8.54 CARLOSS (TRUNK)

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.55 CASETEMP-DEG

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.56 CLDRESTART

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: EQPT

The Cold Restart condition occurs when a card is physically removed and inserted, replaced, or when the ONS 15454 power is initialized.

Clear the CLDRESTART Condition

Step 1 Complete the "Remove and Reinsert (Reseat) the Standby TCC2/TCC2P Card" procedure on page 2-241.

Step 2 If the condition fails to clear after the card reboots, complete the "Remove and Reinsert (Reseat) Any Card" procedure on page 2-242.

Step 3 If the condition does not clear, complete the "Physically Replace a Traffic Card" procedure on page 2-243 for the card.

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).

2.8.57 COMIOXC

Default Severity: Critical (CR), Service-Affecting (SA)

SONET Logical Object: EQPT

The Input/Output Slot To Cross-Connect Communication Failure alarm is caused by the XC10G or XC-VXC-10G cross-connect card when there is a communication failure for a traffic slot.

Clear the COMIOXC Alarm

Step 1 Complete the "Reset a Traffic Card in CTC" procedure on page 2-239 on the card in which the alarm is reported. For the LED behavior, see the "2.9.2 Typical Traffic Card LED Activity During Reset" section on page 2-229.

Step 2 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

Step 3 If the CTC reset does not clear the alarm, move traffic off the reporting cross-connect card. Complete the "Side Switch the Active and Standby Cross-Connect Cards" procedure on page 2-240.

Step 4 Complete the "Remove and Reinsert (Reseat) Any Card" procedure on page 2-242 on the card in which the alarm is reported.

Step 5 If the alarm does not clear, complete the "Physically Replace an In-Service Cross-Connect Card" procedure on page 2-243 for the reporting cross-connect card or complete the "Physically Replace a Traffic Card" procedure on page 2-243 on the card in which the alarm is reported.

Step 6 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

2.8.58 COMM-FAIL

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: EQPT

The Plug-In Module (card) Communication Failure indicates that there is a communication failure between the TCC2/TCC2P and the traffic card. The failure could indicate a broken card interface.

Clear the COMM-FAIL Alarm

Step 1 Complete the "Reset a Traffic Card in CTC" procedure on page 2-239 for the reporting card.

Step 2 If the alarm does not clear, complete the "Physically Replace a Traffic Card" procedure on page 2-243 for the card.

Step 3 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.59 CONTBUS-A-18

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: EQPT

A Communication Failure from Controller Slot to Controller Slot alarm for the TCC2/TCC2P slot to TCC2/TCC2P slot occurs when the main processor on the TCC2/TCC2P in the first slot (TCC A) loses communication with the coprocessor on the same card. This applies to the TCC2/TCC2P in Slot 7.

Clear the CONTBUS-A-18 Alarm

Step 1 Complete the "Remove and Reinsert (Reseat) the Standby TCC2/TCC2P Card" procedure on page 2-241 to make the TCC2/TCC2P in Slot 11 active.

Step 2 Wait approximately 10 minutes for the TCC2/TCC2P in Slot 7 to reset as the standby TCC2/TCC2P. Verify that the ACT/SBY LED is correctly illuminated before proceeding to the next step. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

Step 3 Position the cursor over the TCC2/TCC2P in Slot 11 and complete the "Reset an Active TCC2/TCC2P Card and Activate the Standby Card" procedure on page 2-240 to return the card to the active state.

Step 4 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 an Active TCC2/TCC2P Card and Activate the Standby Card" procedure on page 2-240. If the Cisco TAC technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Traffic Card" procedure on page 2-243.

2.8.60 CONTBUS-B-18

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: EQPT

A Communication Failure from Controller Slot to Controller Slot alarm for the TCC2/TCC2P slot to TCC2/TCC2P slot occurs when the main processor on the TCC2/TCC2P in the second slot (TCC B) loses communication with the coprocessor on the same card. This applies to the Slot 11 TCC2/TCC2P.

Clear the CONTBUS-B-18 Alarm

Step 1 Complete the "Reset an Active TCC2/TCC2P Card and Activate the Standby Card" procedure on page 2-240 to make the Slot 7 TCC2/TCC2P active.

Step 2 Wait approximately 10 minutes for the Slot 11 TCC2/TCC2P to reset as the standby TCC2/TCC2P. Verify that the ACT/SBY LED is correctly illuminated before proceeding to the next step. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

Step 3 Position the cursor over the Slot 7 TCC2/TCC2P and complete the "Reset an Active TCC2/TCC2P Card and Activate the Standby Card" procedure on page 2-240 to return the Slot 11 TCC2/TCC2P to the active state.

Step 4 If the reset card has not rebooted successfully, or the alarm has not cleared, call Cisco TAC (1-800-553-2447). If the Cisco TAC technician tells you to reseat the card, complete the "Remove and Reinsert (Reseat) the Standby TCC2/TCC2P Card" procedure on page 2-241. If the Cisco TAC technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Traffic Card" procedure on page 2-243.

2.8.61 CONTBUS-DISABLED

Default Severity: Critical (CR), Service-Affecting (SA)

SONET Logical Object: EQPT

The CONTBUS-DISABLED alarm is a function of the Release 6.0 enhanced cell bus verification feature. This alarm occurs when a defective card is installed in the shelf assembly or when a card already installed in the shelf assembly becomes defective (that is, the card fails the enhanced cell bus verification test). The alarm persists as long as the defective card remains in the chassis. When the card is removed, CONTBUS-DISABLED will remain raised for a one-minute wait time. This wait time is designed as a guard period so that the system can distinguish this outage from a briefer card reset communication outage.

If no card is reinserted into the original slot during the wait time, the alarm clears. After this time, a different, nondefective card (not the original card) should be inserted.

When CONTBUS-DISABLED is raised, no message-oriented communication is allowed to or from this slot to the TCC2/TCC2P (thus avoiding node communication failure).

Caution CONTBUS-DISABLED clears only when the faulty card is removed for one minute. If any card at all is reinserted before the one-minute guard period expires, the alarm does not clear.

CONTBUS-DISABLED overrides the IMPROPRMVL alarm during the one-minute wait period, but afterward IMPROPRMVL can be raised because it is no longer suppressed. IMPROPRMVL is raised after CONTBUS-DISABLED clears if the card is in the node database. If CONTBUS-DISABLED has cleared but IMPROPRMVL is still active, inserting a card will clear the IMPROPRMVL alarm.

Clear the CONTBUS-DISABLED Alarm

Step 1 If the IMPROPRMVL alarm is raised, complete the "Physically Replace a Traffic Card" procedure on page 2-243. (For general information about card installation, refer to the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15454 Procedure Guide*.)

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.

2.8.62 CONTBUS-IO-A

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: EQPT

A TCCA to Shelf A Slot Communication Failure alarm occurs when the active Slot 7 TCC2/TCC2P (TCC A) has lost communication with another card in the shelf. The other card is identified by the Object column in the CTC alarm window.

The CONTBUS-IO-A alarm can appear briefly when the ONS 15454 switches to the protect TCC2/TCC2P. In the case of a TCC2/TCC2P protection switch, the alarm clears after the other cards establish communication with the newly active TCC2/TCC2P. If the alarm persists, the problem lies with the physical path of communication from the TCC2/TCC2P to the reporting card. The physical path of communication includes the TCC2/TCC2P, the other card, and the backplane.

Clear the CONTBUS-IO-A Alarm

Step 1 Ensure that the reporting card is physically present in the shelf. Record the card type. Click the **Inventory** tab and view the Eqpt Type column to reveal the provisioned type.

If the actual card type and the provisioned card type do not match, see the "MEA (EQPT)" alarm on page 2-165 for the reporting card.

Step 2 If the alarm object is any single card slot other than the standby Slot 11 TCC2/TCC2P, perform a CTC reset of the object card. Complete the "Reset a Traffic Card in CTC" procedure on page 2-239. For the LED behavior, see the "2.9.2 Typical Traffic Card LED Activity During Reset" section on page 2-229.

Step 3 If the alarm object is the standby Slot 11 TCC2/TCC2P, complete the "Reset a Traffic Card in CTC" procedure on page 2-239 for it. The procedure is similar.

Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card. (A reset standby card remains standby.)

If CONTBUS-IO-A is raised on several cards at the same time, complete the "Reset an Active TCC2/TCC2P Card and Activate the Standby Card" procedure on page 2-240.

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 ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

Step 5 If the CTC reset does not clear the alarm, complete the "Remove and Reinsert (Reseat) Any Card" procedure on page 2-242 for the reporting card.

Step 6 If the reset card has not rebooted successfully, or the alarm has not cleared, call Cisco TAC (1 800 553-2447). If the Cisco TAC technician tells you to reseat the card, complete the "Remove and Reinsert (Reseat) the Standby TCC2/TCC2P Card" procedure on page 2-241. If the Cisco TAC technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Traffic Card" procedure on page 2-243.

2.8.63 CONTBUS-IO-B

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: EQPT

A TCC B to Shelf Communication Failure alarm occurs when the active Slot 11 TCC2/TCC2P (TCC B) has lost communication with another card in the shelf. The other card is identified by the Object column in the CTC alarm window.

The CONTBUS-IO-B alarm could appear briefly when the ONS 15454 switches to the protect TCC2/TCC2P. In the case of a TCC2/TCC2P protection switch, the alarm clears after the other cards establish communication with the newly active TCC2/TCC2P. If the alarm persists, the problem lies with the physical path of communication from the TCC2/TCC2P to the reporting card. The physical path of communication includes the TCC2/TCC2P, the other card, and the backplane.

Clear the CONTBUS-IO-B Alarm

Step 1 Ensure that the reporting card is physically present in the shelf. Record the card type. Click the **Inventory** tab and view the Eqpt Type column to reveal the provisioned type.

If the actual card type and the provisioned card type do not match, see the "MEA (EQPT)" alarm on page 2-165 for the reporting card.

Step 2 If the alarm object is any single card slot other than the standby Slot 7 TCC2/TCC2P, perform a CTC reset of the object card. Complete the "Reset a Traffic Card in CTC" procedure on page 2-239. For the LED behavior, see the "2.9.2 Typical Traffic Card LED Activity During Reset" section on page 2-229.

Step 3 If the alarm object is the standby Slot 7 TCC2/TCC2P, complete the "Reset a Traffic Card in CTC" procedure on page 2-239 for it. The procedure is similar.

Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card. (A reset standby card remains standby.)

Step 4 If CONTBUS-IO-B is raised on several cards at the same time, complete the "Reset an Active TCC2/TCC2P Card and Activate the Standby Card" procedure on page 2-240.

Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card.

Step 5 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

Step 6 If the CTC reset does not clear the alarm, complete the "Remove and Reinsert (Reseat) Any Card" procedure on page 2-242 for the reporting card.

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 "Remove and Reinsert (Reseat) the Standby TCC2/TCC2P Card" procedure on page 2-241. If the Cisco TAC technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Traffic Card" procedure on page 2-243.

2.8.64 CTNEQPT-MISMATCH

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: EQPT

The Connection Equipment Mismatch condition is raised when there is a mismatch between the cross-connect card preprovisioned in the slot and the card actually installed in the shelf. For example, one type of cross-connect card could be preprovisioned in Slot 10, but another could be physically installed. It can also be caused by a card that is mismatched with the card. For example, CTNEQPT-MISMATCH is raised when an XCVT card is replaced with a XC10G card.

Cisco does not support configurations of unmatched cross-connect cards in Slot 8 and Slot 10, although this situation could briefly occur during the upgrade process.

The cross-connect card you are replacing should not be the active card. (It can be in SBY state or otherwise not in use.)

Note During an upgrade, this condition occurs and is raised as its default severity, Not Alarmed (NA). However, after the upgrade has occurred, if you wish to change the condition's severity so that it is Not Reported (NR), you can do this by modifying the alarm profile used at the node. For more information about modifying alarm severities, refer to the "Manage Alarms" chapter in the *Cisco ONS 15454 Procedure Guide*.

Clear the CTNEQPT-MISMATCH Condition

Step 1 Determine what kind of card is preprovisioned in the slot:

a. In node view, click the **Inventory** tab.

b. View the information for the slot in the Eqpt Type and Actual Eqpt Type columns.

The Eqpt Type column contains the equipment that is provisioned in the slot. The Actual Eqpt Type contains the equipment that is physically present in the slot. For example, Slot 8 could be provisioned for an XCVT card, which is shown in the Eqpt Type column, but an XC10G XC10G card could be physically present in the slot. The XC10G would be shown in the Actual Eqpt Type column.

Step 2 Complete the "Physically Replace a Traffic Card" procedure on page 2-243 for the mismatched card.

Step 3 If the condition does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.65 CTNEQPT-PBPROT

Default Severity: Critical (CR), Service-Affecting (SA)

SONET Logical Object: EQPT

The Interconnection Equipment Failure Protect Cross-Connect Card Payload Bus Alarm indicates a failure of the main payload between the protect ONS 15454 Slot 10 XC10G card and the reporting traffic card. The cross-connect card and the reporting card are no longer communicating through the backplane. The problem exists in the cross-connect card and the reporting traffic card, or the TCC2/TCC2P and the backplane.

Note This alarm automatically raises and clears when the Slot 8 XC10G card is reseated.

Caution A software update on a standby TCC2/TCC2P can take up to 30 minutes.

Clear the CTNEQPT-PBPROT Alarm

Step 1 If all traffic cards show CTNEQPT-PBPROT alarm, complete the following steps:

a. Complete the "Remove and Reinsert (Reseat) the Standby TCC2/TCC2P Card" procedure on page 2-241 for the standby TCC2/TCC2P.

b. If the reseat fails to clear the alarm, complete the "Physically Replace a Traffic Card" procedure on page 2-243 for the standby TCC2/TCC2P.

Caution Do not physically reseat an active TCC2/TCC2P. Doing so disrupts traffic.

Step 2 If not all cards show the alarm, perform a CTC reset on the standby XC10G card. Complete the "Reset a Traffic Card in CTC" procedure on page 2-239. For the LED behavior, see the "2.9.2 Typical Traffic Card LED Activity During Reset" section on page 2-229.

Step 3 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

If the cross-connect reset is not complete and error-free or if the TCC2/TCC2P reboots automatically, call Cisco TAC (1 800 553-2447).

Step 4 If the alarm does not clear, complete the "Remove and Reinsert (Reseat) Any Card" procedure on page 2-242 for the standby OC-192 card.

Step 5 Determine whether the card is an active card or standby card in a protection group. Click the node view **Maintenance > Protection** tabs, then click the protection group. The cards and their status are displayed in the list.

Step 6 If the reporting traffic card is the active card in the protection group, complete the "Initiate a 1:1 Card Switch Command" procedure on page 2-234. After you move traffic off the active card, or if the reporting card is standby, continue with the following steps.

Step 7 Complete the "Reset a Traffic Card in CTC" procedure on page 2-239 on the reporting card. For the LED behavior, see the "2.9.2 Typical Traffic Card LED Activity During Reset" section on page 2-229.

Step 8 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

Step 9 If the alarm does not clear, complete the "Remove and Reinsert (Reseat) Any Card" procedure on page 2-242 for the reporting card.

Step 10 Complete the "Initiate a 1:1 Card Switch Command" procedure on page 2-234 to switch traffic back.

Step 11 If the alarm does not clear, complete the "Physically Replace a Traffic Card" procedure on page 2-243 for the reporting traffic card.

Step 12 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

2.8.66 CTNEQPT-PBWORK

Default Severity: Critical (CR), Service-Affecting (SA)

SONET Logical Object: EQPT

The Interconnection Equipment Failure Working Cross-Connect Card Payload Bus alarm indicates a failure in the main payload bus between the ONS 15454 Slot 8 XC10G card and the reporting traffic card. The cross-connect card and the reporting card are no longer communicating through the backplane. The problem exists in the cross-connect card and the reporting traffic card, or the TCC2/TCC2P and the backplane.

Note This alarm automatically raises and clears when the ONS 15454 Slot 10 XC10G card is reseated.

Clear the CTNEQPT-PBWORK Alarm

Step 1 If all traffic cards show CTNEQPT-PBWORK alarm, complete the following steps:

a. Complete the "Reset an Active TCC2/TCC2P Card and Activate the Standby Card" procedure on page 2-240 for the active TCC2/TCC2P and then complete the "Remove and Reinsert (Reseat) the Standby TCC2/TCC2P Card" procedure on page 2-241.

b. If the reseat fails to clear the alarm, complete the "Physically Replace a Traffic Card" procedure on page 2-243 for the TCC2/TCC2P.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Caution Do not physically reseat an active TCC2/TCC2P; it disrupts traffic.

Step 2 If all cards do not show the alarm, complete the "Side Switch the Active and Standby Cross-Connect Cards" procedure on page 2-240 for the active XC10G card.

Step 3 Complete the "Reset a Traffic Card in CTC" procedure on page 2-239 for the reporting card. For the LED behavior, see the "2.9.2 Typical Traffic Card LED Activity During Reset" section on page 2-229.

Step 4 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

Step 5 If the alarm does not clear, complete the "Remove and Reinsert (Reseat) Any Card" procedure on page 2-242 for the standby cross-connect card.

Step 6 If the alarm does not clear and the reporting traffic card is the active card in the protection group, complete the "Initiate a 1:1 Card Switch Command" procedure on page 2-234. If the card is standby, or if you have moved traffic off the active card, proceed with the following steps.

Step 7 Complete the "Reset a Traffic Card in CTC" procedure on page 2-239 for the reporting card. For the LED behavior, see the "2.9.2 Typical Traffic Card LED Activity During Reset" section on page 2-229.

Step 8 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

Step 9 If the CTC reset does not clear the alarm, complete the "Remove and Reinsert (Reseat) Any Card" procedure on page 2-242 for the reporting card.

Step 10 If you switched traffic, complete the "Initiate a 1:1 Card Switch Command" procedure on page 2-234 to revert the traffic.

Step 11 If the alarm does not clear, complete the "Physically Replace a Traffic Card" procedure on page 2-243 for the OC-192 card.

Step 12 If the alarm does not clear, complete the "Physically Replace a Traffic Card" procedure on page 2-243 for the reporting traffic card.

Step 13 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

2.8.67 DATAFLT

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: NE

The Software Data Integrity Fault alarm occurs when the TCC2/TCC2P exceeds its flash memory capacity.

Caution When the system reboots, the last configuration entered is not saved.

Clear the DATAFLT Alarm

Step 1 Complete the "Reset an Active TCC2/TCC2P Card and Activate the Standby Card" procedure on page 2-240.

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).

2.8.68 DBOSYNC

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Object: NE

The Standby Database Out Of Synchronization alarm occurs when the standby TCC2/TCC2P database does not synchronize with the active database on the active TCC2/TCC2P.

Caution If you reset the active TCC2/TCC2P while this alarm is raised, you lose current provisioning.

Clear the DBOSYNC Alarm

Step 1 Save a backup copy of the active TCC2/TCC2P database. Refer to the "Maintain the Node" chapter in the *Cisco ONS 15454 Procedure Guide* for procedures.

Step 2 Make a minor provisioning change to the active database to see if applying a provisioning change clears the alarm:

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).

2.8.69 DS3-MISM

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: DS3

The DS-3 Frame Format Mismatch condition indicates a frame format mismatch on a signal transiting the ONS 15454 DS3XM-6, DS3XM-12, or DS3/EC1-48 card. The condition occurs when the provisioned line type and incoming signal frame format type do no match. For example, if the line type for a DS3XM-6 card is set to C Bit and the incoming signal frame format is detected as M13, then the ONS 15454 reports a DS3-MISM condition.

Clear the DS3-MISM Condition

Step 1 Display the CTC card view for the reporting DS3XM-6, DS3XM-12, or DS3/EC1-48 card.

Step 2 Click the **Provisioning > Line** tabs.

Step 3 For the row on the appropriate port, verify that the Line Type column is set to match the expected incoming signal (C Bit or M13).

Step 4 If the Line Type field does not match the expected incoming signal, select the correct Line Type in the drop-down list.

Step 5 Click **Apply**.

Step 6 If the condition does not clear after the user verifies that the provisioned line type matches the expected incoming signal, use an optical test set to verify that the actual signal coming into the ONS 15454 matches the expected incoming signal. For specific procedures to use the test set equipment, consult the manufacturer.

Step 7 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.70 DSP-COMM-FAIL

For information about this alarm or condition, refer to the “Alarm Troubleshooting” in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.71 DSP-FAIL

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.72 DUP-IPADDR

Default Severity: Minor (MN), Non-Service Affecting (NSA)

SONET 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:

- **a.** Connect to the alarmed node using the Craft port on the TCC2/TCC2P card.
- **b.** Begin a CTC session.
- **c.** In the login dialog window, uncheck the **Network Discovery** check box.

Step 2 In node view, click the **Provisioning > Network > General** tabs.

Step 3 In the IP Address field, change the IP address to a unique number.

Step 4 Click **Apply**.

Step 5 Restart any CTC sessions that are logged into either of the duplicate IP addresses. (For procedures to log in or log out, refer to the "Set Up PC and Log Into the GUI" chapter in the *Cisco ONS 15454 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).

2.8.73 DUP-NODENAME

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET 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).

2.8.74 EHIBATVG

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Object: PWR

The Extreme High Voltage Battery alarm occurs in a –48 VDC environment when a battery lead input voltage exceeds the extreme high power threshold. This threshold, with a default value of –56.5 VDC, is user-provisionable. The alarm remains raised until the voltage remains under the threshold for 120 seconds. (For information about changing this threshold, refer to the "Turn Up Node" chapter in the *Cisco ONS 15454 Procedure Guide*.)

Clear the EHIBATVG Alarm

Step 1 The problem is external to the ONS 15454. 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.

2.8.75 ELWBATVG

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Object: PWR

The Extreme Low Voltage Battery alarm occurs in a –48 VDC environment when a battery lead input voltage falls below the extreme low power threshold. This threshold, with a default value of –40.5 VDC, is user-provisionable. The alarm remains raised until the voltage remains over the threshold for 120 seconds. (For information about changing this threshold, refer to the "Turn Up Node" chapter in the *Cisco ONS 15454 Procedure Guide*.

Clear the ELWBATVG Alarm

Step 1 The problem is external to the ONS 15454. 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.

2.8.76 ENCAP-MISMATCH-P

Default Severity: Critical (CR), Service-Affecting (SA)

SONET Logical Object: STSTRM

The Encapsulation C2 Byte Mismatch Path alarm applies to ML-Series Ethernet cards. It occurs when the first three following conditions are met and one of the last two is false:

- The received C2 byte is not 0x00 (unequipped).
- The received C2 byte is not a PDI value.
- The received C2 does not match the expected C2.
- The expected C2 byte is not 0x01 (equipped unspecified).
- The received C2 byte is not 0x01 (equipped unspecified).

(This is in contrast to the "PLM-P" alarm on page 2-176, which must meet all five criteria.) For an ENCAP-MISMATCH-P to be raised, there is a mismatch between the received and expected C2 byte, with either the expected byte or received byte value being 0x01.

For example, an ENCAP-MISMATCH-P alarm is raised if a circuit created between two ML-Series cards has generic framing procedure (GFP) framing provisioned on one end and high-level data link control (HDLC) framing with LEX encapsulation provisioned on the other. The GFP framing card transmits and expects a C2 byte of 0x1B, while the HDLC framing card transmits and expects a C2 byte of 0x01.

A mismatch between the transmit and receive cards on any of the following parameters can cause the alarm:

- Mode (HDLC, GFP-F)
- Encapsulation (LEX, HDLC, PPP)
- CRC size (16 or 32)
- Scrambling state (on or off)

This alarm is demoted by a PLM-P or PLM-V condition.

Note By default, an ENCAP-MISMATCH-P alarm causes an ML-Series card data link to go down. This behavior can be modified using the command line interface (CLI) command **no pos trigger defect encap**.

Note For more information about the ML-Series Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.*

Clear the ENCAP-MISMATCH-P Alarm

Step 1 Ensure that the correct framing mode is in use on the receive card:

a. In node view, double-click the receive ML-Series card to open the card view.

b. Click the **Provisioning > Card** tabs.

c. In the Mode drop-down list, ensure that the same mode (GFP or HDLC) is selected. If it is not, choose it and click **Apply**.

Step 2 Ensure that the correct framing mode is in use on the transmit card, and that it is identical to the receiving card:

a. In node view, double-click the transmit ML-Series card to open the card view.

b. Click the **Provisioning > Card** tabs.

c. In the Mode drop-down list, ensure that the same mode (GFP or HDLC) is selected. If it is not, choose it and click **Apply**.

Step 3 If the alarm does not clear, use the CLI to ensure that the remaining settings are correctly configured on the ML-Series card:

- Encapsulation
- CRC size
- Scrambling state

To open the interface, click the **IOS** tab and click **Open IOS Command Line Interface (CLI)**. Refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327* entries on all three of these topics to obtain the full configuration command sequences.

Step 4 If the alarm does not clear, log into the 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.

2.8.77 EOC

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: OCN

DWDM Logical Object: TRUNK

The SONET DCC Termination Failure alarm occurs when the ONS 15454 loses its DCC. Although this alarm is primarily SONET, it can apply to DWDM. For example, the OSCM card can raise this alarm on its OC-3 section overhead.

The SDCC consists of three bytes, D1 through D3, in the SONET overhead. The bytes convey information about operation, administration, maintenance, and provisioning (OAM&P). The ONS 15454 uses the DCC on the SONET section layer to communicate network management information.

Warning **On the ONS 15454 OC-192 card, the laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. The laser is off when the safety key is off (labeled 0).** Statement 293

Warning **Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard.** Statement 1056

Warning **Use of controls, adjustments, or performing procedures other than those specified could result in hazardous radiation exposure.** Statement 1057

Note If a circuit shows a partial 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 (DS1)" alarm on page 2-141 is also reported, complete the "Clear the LOS (OCN) Alarm" procedure on page 2-148.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 2 If the "SF-L" condition on page 2-196 is reported, complete the "Clear the SF-L Condition" procedure on page 2-196.

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 SDCC traffic. For more information about fiber connections and terminations, refer to the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15454 Procedure Guide*.

If the physical connections are correct and configured to carry DCC traffic, ensure that both ends of the fiber span have in-service (IS-NR) ports. Verify that the ACT/SBY LED on each OC-N card is green.

Step 4 When the LEDs on the OC-N cards are correctly illuminated, complete the "Verify or Create Node Section DCC Terminations" procedure on page 2-245 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:

a. Confirm that the OC-N card shows a green LED in CTC or on the physical card.

   A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

b. To determine whether the port is in service, double-click the card in CTC to open the card view.

c. Click the **Provisioning > Line** tabs.

d. Verify that the Admin State column lists the port as **IS**.

e. If the Admin State column lists the port as OOS,MT or OOS,DSBLD, click the column and click **IS** in the drop-down list. Click **Apply**.

Step 7 For all nodes, if the card is in service, use an optical test set to determine whether signal failures are present on fiber terminations. For specific procedures to use the test set equipment, consult the manufacturer.

Caution Using an optical test set disrupts service on the OC-N card. It could be necessary to manually switch traffic carrying circuits over to a protection path. Refer to the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-231 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 "1.14.3 OC-N Card Transmit and Receive Levels" section on page 1-154 for non-DWDM card levels.

Step 9 If budget loss is within parameters, ensure that fiber connectors are securely fastened and properly terminated. For more information refer to the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15454 Procedure Guide*.

Step 10 If fiber connectors are properly fastened and terminated, complete the "Reset an Active TCC2/TCC2P Card and Activate the Standby Card" procedure on page 2-240.

Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card.

Resetting the active TCC2/TCC2P switches control to the standby TCC2/TCC2P. If the alarm clears when the ONS 15454 node switches to the standby TCC2/TCC2P, the user can assume that the previously active card is the cause of the alarm.

Step 11 If the TCC2/TCC2P reset does not clear the alarm, delete the problematic SDCC termination:

a. From the View menu in card view, choose **Go to Previous View** if you have not already done so.

b. Click the **Provisioning > Comm Channels > SDCC** tabs.

c. Highlight the problematic DCC termination.

d. Click **Delete**.

e. Click **Yes** in the Confirmation Dialog box.

Step 12 Recreate the SDCC termination. Refer to the "Turn Up Network" chapter in the *Cisco ONS 15454 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, call Cisco TAC (1 800 553-2447). If the Cisco TAC technician tells you to reseat the card, complete the "Remove and Reinsert (Reseat) the Standby TCC2/TCC2P Card" procedure on page 2-241. If the Cisco TAC technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Traffic Card" procedure on page 2-243.

2.8.78 EOC-L

Default Severity: Minor (MN), Non-Service-Affecting (NSA) for OCN

SONET Logical Object: OCN

DWDM Logical Object: TRUNK

The Line DCC (LDCC) Termination Failure alarm occurs when the ONS 15454 loses its line data communications channel (LDCC) termination. For example, the OSCM card can raise this alarm on its OC-3 line overhead.

The LDCC consists of nine bytes, D4 through D12, in the SONET overhead. The bytes convey information about OAM&P. The ONS 15454 uses the LDCCs on the SONET line layer to communicate network management information.

Warning **On the OC-192 card, the laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. The laser is off when the safety key is off (labeled 0).** Statement 293

Warning **Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard.** Statement 1056

Warning **Use of controls, adjustments, or performing procedures other than those specified could result in hazardous radiation exposure.** Statement 1057

Note If a circuit shows a partial status when the EOC or EOC-L alarm is raised, it occurs when the logical circuit is in place. The circuit is able to carry traffic when the DCC termination issue is resolved. You do not need to delete the circuit when troubleshooting this alarm.

Clear the EOC-L Alarm

Step 1 Complete the "Clear the EOC Alarm" procedure on page 2-75.

Step 2 If the alarm has not cleared, call Cisco TAC (1 800 553-2447). If the Cisco TAC technician tells you to reseat the card, complete the "Remove and Reinsert (Reseat) the Standby TCC2/TCC2P Card" procedure on page 2-241. If the Cisco TAC technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Traffic Card" procedure on page 2-243.

2.8.79 EQPT

Default Severity: Critical (CR), Service-Affecting (SA)

SONET Logical Objects: AICI-AEP, AICI-AIE, EQPT

DWDM Logical Object: PPM

An Equipment Failure alarm indicates that a hardware failure has occurred on the reporting card. If the EQPT alarm occurs with a BKUPMEMP alarm, refer to the "2.8.42 BKUPMEMP" section on page 2-50. 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 and a"PROTNA" alarm on page 2-180 is raised. The standby path generates a path-type alarm.

Clear the EQPT Alarm

Step 1 If traffic is active on the alarmed port, you could need to switch traffic away from it. See the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-231 for commonly used traffic-switching procedures.

Step 2 Complete the "Reset a Traffic Card in CTC" procedure on page 2-239 for the reporting card. For the LED behavior, see the "2.9.2 Typical Traffic Card LED Activity During Reset" section on page 2-229.

Step 3 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. Verify the LED status. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

Step 4 If the CTC reset does not clear the alarm, complete the "Remove and Reinsert (Reseat) Any Card" procedure on page 2-242 for the reporting card.

Step 5 If the physical reseat of the card fails to clear the alarm, complete the "Physically Replace a Traffic Card" procedure on page 2-243 for the reporting card.

Step 6 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

2.8.80 EQPT-DIAG

Default Severity: Critical (CR), Service-Affecting (SA)

SONET Logical Object: EQPT

An Equipment-Diagnostic Failure alarm indicates that a software or hardware failure has occurred on the reporting card. This alarm can be raised against a traffic card or a cross-connect card.

Clear the EQPT-DIAG Alarm

Step 1 If traffic is active on the alarmed card, you could need to switch traffic away from it. Refer to the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-231 for procedures.

Step 2 Complete the "Remove and Reinsert (Reseat) Any Card" procedure on page 2-242 for the alarmed card

Step 3 If the alarm does not clear, complete the "Physically Replace a Traffic Card" procedure on page 2-243 if it is raised against a traffic card, or complete the "Physically Replace an In-Service Cross-Connect Card" procedure on page 2-243 if the alarm is raised against the cross-connect card.

Step 4 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.81 EQPT-MISS

Default Severity: Critical (CR), Service-Affecting (SA)

SONET Logical Object: FAN

The Replaceable Equipment or Unit Missing alarm is reported against the fan-tray assembly unit. It indicates that the replaceable fan-tray assembly is missing or not fully inserted. It could also indicate that the ribbon cable connecting the AIP to the system board is bad.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Clear the EQPT-MISS Alarm

Step 1 If the alarm is reported against the fan, verify that the fan-tray assembly is present.

Step 2 If the fan-tray assembly is present, complete the "Replace the Fan-Tray Assembly" procedure on page 2-249.

Step 3 If no fan-tray assembly is present, obtain a fan-tray assembly and refer to the "Install the Fan-Tray Assembly," procedure in the *Cisco ONS 15454 Procedure Guide*.

Step 4 If the alarm does not clear, replace the ribbon cable from the AIP to the system board with a known-good ribbon cable.

Step 5 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

2.8.82 ERFI-P-CONN

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

SONET Logical Objects: STSMON, STSTRM

The Three-Bit (Enhanced) Remote Failure Indication (ERFI) Path Connectivity condition is triggered on DS-1, DS-3, or VT circuits when the "UNEQ-P" alarm on page 2-223 and the "TIM-P" alarm on page 2-216 are raised on the transmission signal.

Clear the ERFI-P-CONN Condition

Step 1 Complete the "Clear the UNEQ-P Alarm" procedure on page 2-223. This should clear the ERFI condition.

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).

2.8.83 ERFI-P-PAYLD

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

SONET Logical Objects: STSMON, STSTRM

The Three-Bit ERFI Path Payload condition is triggered on DS-1, DS-3, or VT circuits when the "PLM-P" alarm on page 2-176 is raised on the transmission signal.

Clear the ERFI-P-PAYLD Condition

Step 1 Complete the "Clear the PLM-P Alarm" procedure on page 2-177. This should clear the ERFI condition.

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).

2.8.84 ERFI-P-SRVR

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

SONET Logical Objects: STSMON, STSTRM

The Three-Bit ERFI Path Server condition is triggered on DS-1, DS-3, or VT circuits when the "AIS-P" condition on page 2-33 or the "LOP-P" alarm on page 2-138 is raised on the transmission signal.

Clear the ERFI-P-SRVR Condition

Step 1 Complete the "Clear the LOP-P Alarm" procedure on page 2-138. This should clear the ERFI condition.

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).

2.8.85 ERROR-CONFIG

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: EQPT

The Error in Startup Configuration alarm applies to the ML-Series Ethernet cards. These cards process startup configuration files line by line. If one or more lines cannot be executed, the error causes the ERROR-CONFIG alarm. ERROR-CONFIG is not caused by hardware failure.

The typical reasons for an errored startup file are:

- The user stored the configuration for one type of ML-Series card in the database and then installed another type in its slot.
- The configuration file contained a syntax error on one of the lines.

Note For information about provisioning the ML-Series Ethernet cards from the Cisco IOS interface, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.*

Clear the ERROR-CONFIG Alarm

Step 1 If you have a different type of ML-Series card specified in the startup configuration file than what you have installed, create the correct startup configuration.

Follow the card provisioning instructions in the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.

Step 2 Upload the configuration file to the TCC2/TCC2P:

a. In node view, right-click the ML-Series card graphic.

b. Choose **IOS Startup Config** from the shortcut menu.

c. Click **Local > TCC** and navigate to the file location in the Open dialog box.

Step 3 Complete the "Reset a Traffic Card in CTC" procedure on page 2-239.

Step 4 If the alarm does not clear or if your configuration file was correct according to the installed card, start a Cisco IOS CLI for the card:

a. Right click the ML-Series card graphic in node view.

b. Choose **Open IOS Connection** from the shortcut menu.

Note Open IOS Connection is not available unless the ML-Series card is physically installed in the shelf.

Follow the card provisioning instructions in the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327* to correct the errored configuration file line.

Step 5 Execute the CLI command:

```
copy run start
```

The command copies the new card configuration into the database and clears the alarm.

Step 6 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.86 ETH-LINKLOSS

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: NE

The Rear Panel Ethernet Link Removed condition, if enabled in the network defaults, is raised under the following conditions:

- The node.network.general.AlarmMissingBackplaneLAN field in NE default is enabled.
- The node is configured as a gateway network element (GNE).
- The backplane LAN cable is removed.

Note For more information about Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.

Clear the ETH-LINKLOSS Condition

Step 1 To clear this condition, reconnect the backplane LAN cable. Refer to the "Install the Shelf and Backplane Cable" chapter in the *Cisco ONS 15454 Procedure Guide* for procedures to install this cable.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.87 E-W-MISMATCH

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Object: OCN

A Procedural Error Misconnect East/West Direction alarm occurs during BLSR 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, Slot 6 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 Click the circuit and click **Edit**. The network map detailed view window appears. This window contains the node name, slot, and port for each end of each span.

Step 4 Label each of the nodes on the diagram with the same name that appears on the network map.

Step 5 Label the span ends on the diagram with the same information. For example, with Node 1/Slot 12/Port 1—Node 2/Slot 6/Port 1 (2F BLSR OC48, ring name=0), label the end of the span that connects Node 1 and Node 2 at the Node 1 end as Slot 12/Port 1. Label the Node 2 end of that same span Slot 6/Port 1.

Step 6 Repeat Steps 4 and 5 for each span on your diagram.

Step 7 Label the highest slot at each node east and the lowest slot at each node west.

Step 8 Examine the diagram. You should see a clockwise pattern of west slots connecting to east slots for each span. Refer to the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15454 Procedure Guide* for more information about cabling the system.

Step 9 If any span has an east-to-east or west-to-west connection, physically switching the fiber connectors from the card that does not fit the pattern to the card that continues the pattern should clear the alarm.

Warning **On the OC-192 card, the laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. The laser is off when the safety key is off (labeled 0).** Statement 293

Warning **Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard.** Statement 1056

Warning **Use of controls, adjustments, or performing procedures other than those specified could result in hazardous radiation exposure.** Statement 1057

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.

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 > BLSR** tabs.

Step 3 From the row of information for the fiber span, complete the "Identify a BLSR Ring Name or Node ID Number" procedure on page 2-230 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 BLSR:

a. Click the **Provisioning > BLSR** 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 > BLSR** tabs.

Step 7 Change the West Line field to the slot you recorded for the East Line in Step 3.

Step 8 Change the East Line field 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) in order to report a Service-Affecting (SA) problem.

2.8.88 EXCCOL

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: EQPT

The Excess Collisions on the LAN alarm indicates that too many collisions are occurring between data packets on the network management LAN, and communications between the ONS 15454 and CTC could be affected. The network management LAN is the data network connecting the workstation running the CTC software to the TCC2/TCC2P. The problem causing the alarm is external to the ONS 15454.

Troubleshoot the network management LAN connected to the TCC2/TCC2P for excess collisions. You might need to contact the system administrator of the network management LAN to accomplish the following steps.

Clear the EXCCOL Alarm

Step 1 Verify that the network device port connected to the TCC2/TCC2P has a flow rate set to 10 Mb, half-duplex.

Step 2 If the port has the correct flow rate and duplex setting, troubleshoot the network device connected to the TCC2/TCC2P and the network management LAN.

Step 3 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.89 EXERCISE-RING-FAIL

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: OCN

The Exercise Ring command issues ring protection switching of the requested channel without completing the actual bridge and switch. The EXERCISE-RING-FAIL condition is raised if the command was issued and accepted but the exercise did not take place.

Note If the exercise command gets rejected due to the existence of a higher-priority condition in the ring, EXERCISE-RING-FAIL is Not Reported (NR).

Clear the EXERCISE-RING-FAIL Condition

Step 1 Look for and clear, if present, the "LOF (OCN)" alarm on page 2-135, the "LOS (OCN)" alarm on page 2-147, or a BLSR alarm.

Step 2 Complete the "Initiate an Exercise Ring Switch on a BLSR" procedure on page 2-238.

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).

2.8.90 EXERCISE-SPAN-FAIL

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: OCN

The Exercise Span command issues span switching of the requested channel without completing the actual bridge and switch. The EXERCISE-SPAN-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 span or ring, EXERCISE-SPAN-FAIL is Not Reported (NR).

Clear the EXERCISE-SPAN-FAIL Condition

Step 1 Look for and clear, if present, the "LOF (OCN)" alarm on page 2-135, the "LOS (OCN)" alarm on page 2-147, or a BLSR alarm.

Step 2 Complete the "Initiate an Exercise Ring Switch on a BLSR" procedure on page 2-238.

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).

2.8.91 EXT

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: ENVALRM

A Failure Detected External to the NE alarm occurs because an environmental alarm is present. For example, a door could be open or flooding could have occurred.

Clear the EXT Alarm

Step 1 In node view double-click the AIC-I card to open the card view.

Step 2 Double-click the **Maintenance > External Alarms** tab.

Step 3 Follow your standard operating procedure to remedy environmental conditions that cause alarms. The alarm clears when the situation is remedied.

Step 4 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.92 EXTRA-TRAF-PREEMPT

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Object: OCN

An Extra Traffic Preempted alarm occurs on OC-N cards in two-fiber and four-fiber BLSRs 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 "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-231 or the "Maintain the Node" chapter in the *Cisco ONS 15454 Procedure Guide*.

Step 3 If the alarm occurred on a four-fiber BLSR and the span switch occurred on this OC-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) in order to report a Service-Affecting (SA) problem.

2.8.93 FAILTOSW

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: EQPT, OCN

DWDM Logical Objects: 2R, ESCON, FC, GE, ISC, TRUNK

The Failure to Switch to Protection Facility condition occurs when a working or protect electrical or optical facility switches to its companion port by using a MANUAL command. For example, if you attempt to manually switch traffic from an unused protect port to an in-service working port, the switch will fail (because traffic is already present on the working port) and you will see the FAILTOSW condition.

Clear the FAILTOSW Condition

Step 1 Look up and troubleshoot the higher-priority alarm. Clearing the higher-priority condition frees the card and clears the FAILTOSW.

Note A higher-priority alarm is an alarm raised on the working DS-N card using the 1:N card protection group. The working DS-N card is reporting an alarm but not reporting a FAILTOSW condition.

Step 2 If the condition does not clear, replace the working electrical or optical card that is reporting the higher-priority alarm by following the "Physically Replace a Traffic Card" procedure on page 2-243. This card is the working electrical or optical card using the protect card and not reporting FAILTOSW.

Replacing the working electrical or optical card that is reporting the higher-priority alarm allows traffic to revert to the working slot and the card reporting the FAILTOSW to switch to the protect card.

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).

2.8.94 FAILTOSW-PATH

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: STSMON, VT-MON

The Fail to Switch to Protection Path condition occurs when the working circuit does not switch to the protection circuit on a path protection. Common causes of the FAILTOSW-PATH alarm include a missing or defective protect port, a lockout set on one of the path protection nodes, or path-level alarms that would cause a path protection switch to fail including the "AIS-P" condition on page 2-33, the "LOP-P" alarm on page 2-138, the "SD-P" condition on page 2-194, the "SF-P" condition on page 2-197, and the "UNEQ-P" alarm on page 2-223.

The "LOF (OCN)" alarm on page 2-135, the "LOS (OCN)" alarm on page 2-147, the "SD-L" condition on page 2-193, or the "SF-L" condition on page 2-196 can also occur on the failed path.

Clear the FAILTOSW-PATH Condition in a Path Protection Configuration

Step 1 Look up and clear the higher-priority alarm. Clearing this alarm frees the standby card and clears the FAILTOSW-PATH condition. If the "AIS-P" condition on page 2-33, the "LOP-P" alarm on page 2-138, the "UNEQ-P" alarm on page 2-223, the "SF-P" condition on page 2-197, the "SD-P" condition on page 2-194, the "LOF (OCN)" alarm on page 2-135, the "LOS (OCN)" alarm on page 2-147, the "SD-L" condition on page 2-193, or the "SF-L" condition on page 2-196 are also occurring on the reporting port, complete the applicable alarm clearing procedure.

Note A higher-priority alarm is an alarm raised on the working electrical card using the 1:N card protection group. The working DS-N card is reporting an alarm but not reporting a FAILTOSW condition.

Step 2 If the condition does not clear, replace the active OC-N card that is reporting the higher-priority alarm. Complete the "Physically Replace a Traffic Card" procedure on page 2-243. Replacing the active OC-N card that is reporting the higher-priority alarm allows traffic to revert to the active slot. Reverting frees the standby card, which can then take over traffic from the card reporting the lower-priority alarm and the FAILTOSW-PATH condition.

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).

2.8.95 FAILTOSWR

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: OCN

The Fail to Switch to Protection Ring condition occurs when a ring switch did not complete because of internal APS problems.

FAILTOSWR clears in any of the following situations:

- A physical card pull of the active TCC2/TCC2P (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 "SD (DS1, DS3)" condition on page 2-190 or the "SF (DS1, DS3)" condition on page 2-195) clears.

Warning **On the OC-192 card, the laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. The laser is off when the safety key is off (labeled 0).** Statement 293

Warning **Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard.** Statement 1056

Warning **Use of controls, adjustments, or performing procedures other than those specified could result in hazardous radiation exposure.** Statement 1057

Clear the FAILTOSWR Condition in a BLSR Configuration

Step 1 Perform the Exercise Ring command on the reporting card:

a. Click the **Maintenance > BLSR** tabs.

b. Click the row of the affected ring under the West Switch column.

c. Select **Exercise Ring** in the drop-down list.

Step 2 If the condition does not clear, from the view menu, choose **Go to Network View**.

Step 3 Look for alarms on OC-N cards that make up the ring or span and troubleshoot these alarms.

Step 4 If clearing other alarms does not clear the FAILTOSWR condition, log into the near-end node.

Step 5 Click the **Maintenance > BLSR** tabs.

Step 6 Record the OC-N cards listed under West Line and East Line. Ensure that these OC-N cards and ports are active and in service:

- **a.** Verify the LED status: A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.
- **b.** Double-click the card in CTC to open the card view.
- **c.** Click the **Provisioning > Line** tabs.
- **d.** Verify that the Admin State column lists the port as IS.
- **e.** If the Admin State column lists the port as OOS,MT or OOS,DSBLD, click the column and choose **IS**. Click **Apply**.

Step 7 If the OC-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 OC-N card. It could be necessary to manually switch traffic carrying circuits over to a protection path. Refer to the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-231 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 15454 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 OC-N card receiver specifications. The "1.14.3 OC-N Card Transmit and Receive Levels" section on page 1-154 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 OC-N cards is within specifications, complete the "Physically Replace a Traffic Card" procedure on page 2-243 for the protect standby OC-N card.

Step 13 If the condition does not clear after you replace the BLSR 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).

2.8.96 FAILTOSWS

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: OCN

The Failure to Switch to Protection Span condition signals an APS span switch failure. For a four-fiber BLSR, a failed span switch initiates a ring switch. If the ring switch occurs, the FAILTOSWS condition does not appear. If the ring switch does not occur, the FAILTOSWS condition appears. FAILTOSWS clears when one of the following situations occurs:

- A physical card pull of the active TCC2/TCC2P 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 "SD (DS1, DS3)" condition on page 2-190 or the "SF (DS1, DS3)" condition on page 2-195) clears.

Clear the FAILTOSWS Condition

Step 1 Perform the Exercise Span command on the reporting card:

a. Click the **Maintenance > BLSR** 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 OC-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 > BLSR** tabs.

Step 6 Record the OC-N cards listed under West Line and East Line. Ensure that these OC-N cards are active and in service:

a. Verify the LED status: A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

b. To determine whether the OC-N port is in service, double-click the card in CTC to open the card view.

c. Click the **Provisioning > Line** tabs.

d. Verify that the Admin State column lists the port as IS.

e. If the Admin State column lists the port as OOS,MT or OOS,DSBLD, click the column and choose **IS**. Click **Apply**.

Step 7 If the OC-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 OC-N card. It could be necessary to manually switch traffic carrying circuits over to a protection path. Refer to the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-231 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 15454 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 OC-N card receiver specifications. The "1.14.3 OC-N Card Transmit and Receive Levels" section on page 1-154 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 OC-N cards is within specifications, complete the "Physically Replace a Traffic Card" procedure on page 2-243 for the protect standby OC-N card.

Step 13 If the condition does not clear after you replace the BLSR 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).

2.8.97 FAN

Default Severity: Critical (CR), Service-Affecting (SA)

SONET Logical Object: FAN

The Fan Failure alarm indicates a problem with the fan-tray assembly. When the fan-tray assembly is not fully functional, the temperature of the ONS 15454 can rise above its normal operating range.

The fan-tray assembly contains six fans and needs a minimum of five working fans to properly cool the shelf. However, even with five working fans, the fan-tray assembly could need replacement because a sixth working fan is required for extra protection against overheating.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Clear the FAN Alarm

Step 1 Determine whether the air filter needs replacement. Complete the "Inspect, Clean, and Replace the Reusable Air Filter" procedure on page 2-247.

Step 2 If the filter is clean, complete the "Remove and Reinsert a Fan-Tray Assembly" procedure on page 2-249.

Step 3 If the fan does not run or the alarm persists, complete the "Replace the Fan-Tray Assembly" procedure on page 2-249. The fan should run immediately when correctly inserted.

Step 4 If the replacement fan-tray assembly does not operate correctly, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC to report a Service-Affecting (SA) problem (1 800 553-2447).

2.8.98 FC-NO-CREDITS

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Object: FCMR

DWDM Logical Objects: FC, TRUNK

The Fibre Channel Distance Extension Credit Starvation alarm occurs on storage access networking (SAN) Fibre Channel/Fiber Connectivity (FICON) FC_MR-4 cards when the congestion prevents the GFP transmitter from sending frames to the FC_MR-4 card port. For example, the alarm can be raised when an operator configures a card to autodetect framing credits but the card is not connected to an interoperable FC-SW-standards-based Fibre Channel/FICON port.

FC-NO-CREDITS is raised only if transmission is completely prevented. (If traffic is slowed but still passing, this alarm is not raised.) The alarm is raised in conjunction with the GFP-NO-BUFFERS alarm. For example, if the FC-NO-CREDITS alarm is generated at an FC_MR-4 data port, a GFP-NO-BUFFERS alarm could be raised at the upstream remote FC_MR-4 data port.

Clear the FC-NO-CREDITS Alarm

Step 1 If the port is connected to a Fibre Channel/FICON switch, make sure it is configured for interoperation mode using the manufacturer's instructions.

Step 2 If the port is not connected to a switch, turn off Autodetect Credits:

a. Double-click the FC_MR-4 card.

b. Click **Provisioning > Port > General.**

c. Under Admin State, click the cell and choose **OOS,MT**.

d. Click **Apply**.

e. Click the **Provisioning > Port > Distance Extension** tabs.

f. Uncheck the **Autodetect Credits** column check box.

g. Click **Apply**.

h. Click **Provisioning > Port > General.**

i. Under Admin State, click the cell and choose **IS**.

j. Click **Apply**.

Step 3 Program the Credits Available value based on the buffers available on the connected equipment:

Note The NumCredits must be provisioned to a value smaller than or equal to the receive buffers or credits available on the connected equipment.

a. Double-click the FC_MR-4 card.

b. Click the **Provisioning > Port > Distance Extension** tabs.

c. Enter a new value in the Credits Available column.

d. Click **Apply**.

Step 4 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) to report a Service-Affecting (SA) problem.

2.8.99 FE-AIS

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: DS3

The Far-End AIS condition occurs when an AIS has occurred at the far-end node. FE-AIS usually occurs in conjunction with a downstream LOS alarm (see the "LOS (OCN)" alarm on page 2-147).

Generally, any AIS is a special SONET signal that communicates to the receiving node when the transmit node does not send a valid signal. AIS is not considered an error. It is raised by the receiving node on each input when it detects the AIS instead of a real signal. In most cases when this condition is raised, an upstream node is raising an alarm to indicate a signal failure; all nodes downstream from it only raise some type of AIS. This condition clears when you resolved the problem on the upstream node.

Clear the FE-AIS Condition

Step 1 Complete the "Clear the AIS Condition" procedure on page 2-32.

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).

2.8.100 FEC-MISM

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.101 FE-DS1-MULTLOS

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: DS3

The Far-End Multiple DS-1 LOS Detected condition occurs when multiple DS-1 signals are lost on a far-end DS-1 card.

The prefix FE means the main alarm is occurring at the far-end node and not at the node reporting the FE-DS1-MULTLOS condition. Troubleshoot the FE alarm or condition by troubleshooting the main alarm at its source. The secondary alarms or conditions clear when the main alarm clears.

Clear the FE-DS1-MULTLOS Condition

Step 1 To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE condition. For example, an ONS 15454 FE condition on a card in Slot 12 of Node 1 could relate to a main alarm from a card in Slot 6 of Node 2.

Step 2 Log into the node that links directly to the card reporting the FE condition.

Step 3 Clear the main alarm. Refer to the appropriate alarm section in this chapter for troubleshooting instructions.

Step 4 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.102 FE-DS1-NSA

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: DS3

The Far End DS-1 Equipment Failure Non-Service-Affecting (NSA) condition occurs when a far-end DS-1 equipment failure occurs, but does not affect service because the port is protected and traffic is able to switch to the protect port.

Clear the FE-DS1-NSA Condition

Step 1 To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE alarm. For example, an alarm from a card in an ONS 15454 Slot 12 of Node 1 could link to an alarm from a card in Slot 6 of Node 2.

Step 2 Log into the node that links directly to the card reporting the FE condition.

Step 3 Clear the main alarm. Refer to the appropriate alarm section in this chapter for troubleshooting instructions.

Step 4 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.103 FE-DS1-SA

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: DS3

The Far End DS-1 Equipment Failure Service Affecting condition occurs when there is a far-end equipment failure on a DS-1 card that affects service because traffic is unable to switch to the protect port.

Clear the FE-DS1-SA Condition

Step 1 To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE alarm. For example, an alarm from a card in Slot 12 of Node 1 could link to an alarm from a card in Slot 6 of Node 2.

Step 2 Log into the node that links directly to the card reporting the FE condition.

Step 3 Clear the main alarm. Refer to the appropriate alarm section in this chapter for troubleshooting instructions.

Step 4 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.104 FE-DS1-SNGLLOS

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: DS3

The Far-End Single DS-1 LOS condition occurs when a single DS-1 signal is lost on far-end DS-1 equipment (within a DS3). Signal loss also causes the "LOS (OCN)" alarm on page 2-147.

Clear the FE-DS1-SNGLLOS Condition

Step 1 To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE condition. For example, an FE condition on a card in Slot 12 of Node 1 could link to an alarm from a card in Slot 6 of Node 2.

Step 2 Log into the node that links directly to the card reporting the FE condition.

Step 3 Clear the main alarm. Refer to the appropriate alarm section in this chapter for troubleshooting instructions.

Step 4 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.105 FE-DS3-NSA

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: DS3

The Far End DS-3 Equipment Failure Non-Service-Affecting (NSA) condition occurs when a far-end ONS 15454 DS-3 equipment failure occurs in C-bit framing mode, but does not affect service because the port is protected and traffic is able to switch to the protect port.

Clear the FE-DS3-NSA Condition

Step 1 To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE alarm. For example, an alarm from a card in Slot 12 of Node 1 could link to an alarm from a card in Slot 6 of Node 2.

Step 2 Log into the node that links directly to the card reporting the FE condition.

Step 3 Clear the main alarm. Refer to the appropriate alarm section in this chapter for troubleshooting instructions.

Step 4 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.106 FE-DS3-SA

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: DS3

The Far End DS-3 Equipment Failure Service Affecting condition occurs when there is a far-end equipment failure on an ONS 15454 DS-3 card in C-bit framing mode that affects service because traffic is unable to switch to the protect port.

Clear the FE-DS3-SA Condition

Step 1 To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE alarm. For example, an alarm from a card in Slot 12 of Node 1 could link to an alarm from a card in Slot 6 of Node 2.

Step 2 Log into the node that links directly to the card reporting the FE condition.

Step 3 Clear the main alarm. Refer to the appropriate alarm section in this chapter for troubleshooting instructions.

Step 4 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.107 FE-EQPT-NSA

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: DS3

The Far End Common Equipment Failure condition occurs when a Non-Service-Affecting (NSA) equipment failure is detected on far-end DS-3 equipment.

Clear the FE-EQPT-NSA Condition

Step 1 To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE condition. For example, an FE condition on a card in Slot 12 of Node 1 could relate to a main alarm from a card in Slot 6 of Node 2.

Step 2 Log into the node that links directly to the card reporting the FE condition.

Step 3 Clear the main alarm. Refer to the appropriate alarm section in this chapter for troubleshooting instructions.

Step 4 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.108 FE-FRCDWKSWBK-SPAN

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: OCN

The Far End Forced Switch Back to Working—Span condition is raised on a far-end 1+1 working port when it is Force switched to the working port.

Note WKSWBK-type conditions apply only to revertive circuits.

Clear the FE-FRCDWKSWBK-SPAN Condition

Step 1 Complete the "Clear a 1+1 Force or Manual Switch Command" procedure on page 2-232 for the far-end port.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.109 FE-FRCDWKSWPR-RING

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: OCN

The Far End Ring Working Facility Forced to Switch to Protection condition occurs from a far-end node when a BLSR is forced from working to protect using the Force Ring command. This condition is only visible on the network view Conditions tab.

Clear the FE-FRCDWKSWPR-RING Condition

Step 1 To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE alarm. For example, an FE-AIS condition from the OC-48 card in Slot 12 of Node 1 could link to the main AIS condition from an OC-48 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 BLSR External Switching Command" procedure on page 2-239.

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).

2.8.110 FE-FRCDWKSWPR-SPAN

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: OCN

The Far End Working Facility Forced to Switch to Protection Span condition occurs from a far-end node when a span on a four-fiber BLSR is forced from working to protect using the Force Span command. This condition is only visible on the network view Conditions tab. The port where the Force Switch occurred is indicated by an "F" on the network view detailed circuit map. This condition is accompanied by WKSWPR.

Clear the FE-FRCDWKSWPR-SPAN Condition

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 OC-48 card in Slot 12 of Node 1 could link to the main AIS condition from an OC-48 card in Slot 6 of Node 2.

Step 2 Log into the node that links directly to the card reporting the FE condition.

Step 3 Clear the main alarm.

Step 4 If the FE-FRCDWKSWPR-SPAN condition does not clear, complete the "Clear a BLSR External Switching Command" procedure on page 2-239 for procedures.

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).

2.8.111 FE-IDLE

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: DS3

The Far End Idle condition occurs when a far-end node detects an idle DS-3 signal in C-bit framing mode.

Clear the FE-IDLE Condition

Step 1 To troubleshoot the FE condition, determine which node and card link directly to the card reporting the FE condition. For example, an FE condition on a card in Slot 12 of Node 1 could relate to a main alarm from a card in Slot 6 of Node 2.

Step 2 Log into the node that links directly to the card reporting the FE condition.

Step 3 Clear the main alarm by clearing the protection switch. See the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-231 for commonly used traffic-switching procedures.

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).

2.8.112 FE-LOCKOUTOFPR-SPAN

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: OCN

The Far-End Lock Out of Protection Span condition occurs when a BSLR span is locked out of the protection system from a far-end node using the Lockout Protect Span command. This condition is only seen on the network view Conditions tab and is accompanied by LKOUTPR-S. The port where the lockout originated is marked by an "L" on the network view detailed circuit map.

Clear the FE-LOCKOUTOFPR-SPAN Condition

Step 1 To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE alarm. For example, an FE-AIS condition from the OC-48 card in Slot 12 of Node 1 could link to the main AIS condition from an OC-48 card in Slot 6 of Node 2.

Step 2 Log into the node that links directly to the card reporting the FE condition.

Step 3 Ensure there is no lockout set. Complete the "Clear a BLSR External Switching Command" procedure on page 2-239.

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).

2.8.113 FE-LOF

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: DS3

The Far End LOF condition occurs when a far-end node reports the "LOF (DS3)" alarm on page 2-133 in C-bit framing mode.

Clear the FE-LOF Condition

Step 1 To troubleshoot an FE condition, determine which node and card link directly to the card reporting the FE condition. For example, an FE condition on a card in Slot 12 of Node 1 could relate to a main alarm from a card in Slot 6 of Node 2.

Step 2 Log into the node that links directly to the card reporting the FE condition.

Step 3 Complete the "Clear the LOF (DS1) Alarm" procedure on page 2-132. It also applies to FE-LOF.

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).

2.8.114 FE-LOS

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: DS3

The Far End LOS condition occurs in C-bit framing mode when a far-end node reports the "LOS (DS3)" alarm on page 2-143.

Clear the FE-LOS Condition

Step 1 To troubleshoot the FE condition, determine which node and card link directly to the card reporting the FE condition. For example, an FE condition on a card in Slot 12 of Node 1 could relate to a main alarm from a card in Slot 6 of Node 2.

Step 2 Log into the node that links directly to the card reporting the FE condition.

Step 3 Complete the "Clear the LOS (DS1) Alarm" procedure on page 2-141.

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).

2.8.115 FE-MANWKSWBK-SPAN

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: OCN

The Far End Manual Switch Back to Working—Span condition occurs when a far-end span with a Manual switch reverts to working.

Note WKSWBK-type conditions apply only to nonrevertive circuits.

Clear the FE-MANWKSWBK-SPAN Condition

Step 1 To troubleshoot the FE condition, determine which node and card link directly to the card reporting the FE condition. For example, an FE condition on a card in Slot 12 of Node 1 could relate to a main alarm from a card in Slot 6 of Node 2.

Step 2 Log into the node that links directly to the card reporting the FE condition.

Step 3 Complete the "Clear a BLSR External Switching Command" procedure on page 2-239.

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).

2.8.116 FE-MANWKSWPR-RING

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: OCN

The Far End Ring Manual Switch of Working Facility to Protect condition occurs when a BLSR 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 OC-48 card in Slot 12 of Node 1 could link to the main AIS condition from an OC-48 card in Slot 6 of Node 2.

Step 2 Log into the node that links directly to the card reporting the FE condition.

Step 3 Complete the "Clear a BLSR External Switching Command" procedure on page 2-239.

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).

2.8.117 FE-MANWKSWPR-SPAN

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: OCN

The Far-End Span Manual Switch Working Facility to Protect condition occurs when a four-fiber BLSR span is switched from working to protect at the far-end node using the Manual Span command. This condition is only visible on the network view Conditions tab and is accompanied by WKSWPR. The port where the Manual Switch occurred is indicated by an "M" on the network view detailed circuit map.

Clear the FE-MANWKSWPR-SPAN Condition

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 OC-48 card in Slot 12 of Node 1 could link to the main AIS condition from an OC-48 card in Slot 6 of Node 2.

Step 2 Log into the node that links directly to the card reporting the FE condition.

Step 3 Complete the "Clear a BLSR External Switching Command" alarm on page 2-239.

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).

2.8.118 FEPRLF

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: OCN

The Far End Protection Line Failure alarm occurs when an APS channel "SF-L" condition on page 2-196 occurs on the protect card coming into the node.

Note The FEPRLF alarm occurs when bidirectional protection is used on optical cards in a 1+1 protection group configuration or four-fiber BLSR configuration.

Clear the FEPRLF Alarm on a Four-Fiber BLSR

Step 1 To troubleshoot the FE alarm, determine which node and card link directly to the card reporting the FE alarm. For example, an FE condition on a card in Slot 12 of Node 1 could relate to a main alarm from a card in Slot 6 of Node 2.

Step 2 Log into the node that links directly to the card reporting the FE condition.

Step 3 Clear the main alarm. Refer to the appropriate alarm section in this chapter in this chapter for procedures.

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).

2.8.119 FIBERTEMP-DEG

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.120 FORCED-REQ

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: EQPT, STSMON, VT-MON

The Force Switch Request on Facility or Port condition occurs when you enter the Force command on a port to force traffic from a working port to a protect port or protection span (or from a protect port to a working port or span). You do not need to clear the condition if you want the Force switch to remain.

Clear the FORCED-REQ Condition

Step 1 Complete the "Clear a 1+1 Force or Manual Switch Command" procedure on page 2-232.

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).

2.8.121 FORCED-REQ-RING

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: OCN

The Force Switch Request Ring condition applies to optical trunk cards when the Force Ring command is applied to BLSRs 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 BLSR External Switching Command" procedure on page 2-239.

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).

2.8.122 FORCED-REQ-SPAN

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: OCN

DWDM Logical Objects: 2R, ESCON, FC, GE, ISC, TRUNK

The Force Switch Request Span condition applies to optical trunk cards in two-fiber or four-fiber BLSRs when the Force Span command is applied to a BLSR 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 BLSR External Switching Command" procedure on page 2-239.

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).

2.8.123 FRCDSWTOINT

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET 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.

2.8.124 FRCDSWTOPRI

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: EXT-SREF, NE-SREF

The Force Switch to Primary Timing Source condition occurs when the user issues a Force command to switch to the primary timing source.

Note FRCDSWTOPRI is an informational condition and does not require troubleshooting.

2.8.125 FRCDSWTOSEC

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: EXT-SREF, NE-SREF

The Force Switch to Second Timing Source condition occurs when the user issues a Force command to switch to the second timing source.

Note FRCDSWTOSEC is an informational condition and does not require troubleshooting.

2.8.126 FRCDSWTOTHIRD

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: EXT-SREF, NE-SREF

The Force Switch to Third Timing Source condition occurs when the user issues a Force command to switch to a third timing source.

Note FRCDSWTOTHIRD is an informational condition and does not require troubleshooting.

2.8.127 FRNGSYNC

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: NE-SREF

The Free Running Synchronization Mode condition occurs when the reporting ONS 15454 is in free-run synchronization mode. External timing sources have been disabled and the node is using its internal clock, or the node has lost its designated building integrated timing supply (BITS) timing source. After the 24-hour holdover period expires, timing slips could begin to occur on an ONS 15454 node relying on an internal clock.

Note If the ONS 15454 is configured to operate from its internal clock, disregard the FRNGSYNC condition.

Clear the FRNGSYNC Condition

Step 1 If the ONS 15454 is configured to operate from an external timing source, verify that the BITS timing source is valid. Common problems with a BITS timing source include reversed wiring and bad timing cards. Refer to the "Timing" chapter in the *Cisco ONS 15454 Reference Manual* for more information.

Step 2 If the BITS source is valid, clear alarms related to the failures of the primary and secondary reference sources, such as the "SYNCPRI" alarm on page 2-212 and the "SYNCSEC" alarm on page 2-212.

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).

2.8.128 FSTSYNC

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: NE-SREF

A Fast Start Synchronization Mode condition occurs when the node is choosing a new timing reference. The previous timing reference has failed.

The FSTSYNC alarm disappears after approximately 30 seconds. If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

Note FSTSYNC is an informational condition. It does not require troubleshooting.

2.8.129 FULLPASSTHR-BI

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: OCN

The Bidirectional Full Pass-Through Active condition occurs on a nonswitching node in a BLSR when the protect channels on the node are active and carrying traffic and there is a change in the receive K byte from No Request.

Clear the FULLPASSTHR-BI Condition

Step 1 Complete the "Clear a BLSR External Switching Command" procedure on page 2-239.

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).

2.8.130 GAIN-HDEG

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.131 GAIN-HFAIL

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.132 GAIN-LDEG

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.133 GAIN-LFAIL

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.134 GCC-EOC

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.135 GE-OOSYNC

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.136 GFP-CSF

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Objects: CE100T, FCMR, GFP-FAC, ML100T, ML1000, MLFX

The GFP Client Signal Fail Detected alarm is a secondary alarm raised on local GFP data ports when a remote Service-Affecting (SA) alarm causes invalid data transmission. The alarm is raised locally on FC_MR-4, ML100T, ML1000, ML100X-8, MXP_MR_25G, and MXPP_MR_25G GFP data ports and does not indicate that a Service-Affecting (SA) failure is occurring at the local site, but that a CARLOSS, LOS, or SYNCLOSS alarm caused by an event such as a pulled receive cable is affecting a remote data port's transmission capability. This alarm can be demoted when a facility loopback is placed on the FC_MR-4 port.

Note For more information about Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.

Clear the GFP-CSF Alarm

Step 1 Clear the Service-Affecting (SA) alarm at the remote data port.

Step 2 If the GFP-CSF alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) to report a Service-Affecting (SA) problem.

2.8.137 GFP-DE-MISMATCH

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Objects: FCMR, GFP-FAC

The GFP Fibre Channel Distance Extension Mismatch alarm indicates that a port configured for Distance Extension is connected to a port that is not operating in Cisco's proprietary Distance Extension mode. It is raised on Fibre Channel and FICON card GFP ports supporting distance extension. The alarm occurs when distance extension is enabled on one side of the transport but not on the other. To clear, distance extension must be enabled on both ports connected by a circuit.

Note For more information about Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.

Clear the GFP-DE-MISMATCH Alarm

Step 1 Ensure that the distance extension protocol is configured correctly on both sides:

a. Double-click the card to open the card view.

b. Click the **Provisioning > Port > General** tabs.

c. Under Admin State, click the cell and choose **OOS,MT**.

d. Click **Apply**.

e. Click the **Provisioning > Port > Distance Extension** tabs.

f. Check the check box in the **Enable Distance Extension** column.

g. Click **Apply**.

h. Click the **Provisioning > Port > General** tabs.

i. Under Admin State, click the cell and choose **IS-NR**.

j. Click **Apply**.

Step 2 If the GFP-DE-MISMATCH alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) to report a Service-Affecting (SA) problem.

2.8.138 GFP-EX-MISMATCH

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Objects: FCMR, GFP-FAC

The GFP Extension Header Mismatch alarm is raised on Fibre Channel/FICON cards when it receives frames with an extension header that is not null. The alarm occurs when a provisioning error causes all GFP frames to be dropped for 2.5 seconds.

Ensure that both end ports are sending a null extension header for a GFP frame. The FC_MR-4 card always sends a null extension header, so if the equipment is connected to other vendors' equipment, those need to be provisioned appropriately.

Note For more information about Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.

Clear the GFP-EX-MISMATCH Alarm

Step 1 Ensure that the vendor equipment is provisioned to send a null extension header in order to interoperate with the FC_MR-4 card. (The FC_MR-4 card always sends a null extension header.)

Step 2 If the GFP-EX-MISMATCH alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) to report a Service-Affecting (SA) problem.

2.8.139 GFP-LFD

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Objects: CE100T, FCMR, GFP-FAC, ML100T, ML1000, MLFX

The GFP Loss of Frame Delineation alarm applies to Fibre Channel, FICON GFP, and Ethernet ports. This alarm occurs if there is a bad SONET connection, if SONET path errors cause GFP header errors in the check sum calculated over payload length (PLI/cHEC) combination, or if the GFP source port sends an invalid PLI/cHEC combination. The loss causes traffic stoppage.

Note For more information about Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.

Clear the GFP-LFD Alarm

Step 1 Look for and clear any associated SONET path errors such as LOS or AIS-L originating at the transmit node.

Step 2 If the GFP-LFD alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) to report a Service-Affecting (SA) problem.

2.8.140 GFP-NO-BUFFERS

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Objects: FCMR, GFP-FAC

The GFP Fibre Channel Distance Extension Buffer Starvation alarm is raised on Fibre Channel/FICON card ports supporting GFP and the distance extension protocol when the GFP transmitter cannot send GFP frames due to lack of remote GFP receiver buffers. This occurs when the remote GFP-T receiver experiences congestion and is unable to send frames over the Fibre Channel/FICON link.

This alarm could be raised in conjunction with the FC-NO-CREDITS alarm. For example, if the FC-NO-CREDITS alarm is generated at an FC_MR-4 data port, a GFP-NO-BUFFERS alarm could be raised at the upstream remote FC_MR-4 data port.

Note For more information about Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.

Clear the GFP-NO-BUFFERS Alarm

Step 1 Complete the "Clear the FC-NO-CREDITS Alarm" procedure on page 2-92.

Step 2 If the GFP-CSF alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) to report a Service-Affecting (SA) problem.

2.8.141 GFP-UP-MISMATCH

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Objects: CE100T, FCMR, GFP-FAC, ML100T, ML1000, MLFX

The GFP User Payload Mismatch is raised against Fibre Channel/FICON ports supporting GFP. It occurs when the received frame user payload identifier (UPI) does not match the transmitted UPI and all frames are dropped. The alarm is caused by a provisioning error, such as the port media type not matching the remote port media type. For example, the local port media type could be set to Fibre Channel—1 Gbps ISL or Fibre Channel—2 Gbps ISL and the remote port media type could be set to FICON—1 Gbps ISL or FICON—2 Gbps ISL.

Note For more information about Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.

Clear the GFP-UP-MISMATCH Alarm

Step 1 Ensure that the transmit port and receive port are identically provisioned for distance extension by completing the following steps:

a. Double-click the card to open the card view.

b. Click the **Provisioning > Port > Distance Extension** tabs.

c. Check the check box in the **Enable Distance Extension** column.

d. Click **Apply**.

Step 2 Ensure that both ports are set for the correct media type. For each port, complete the following steps:

a. Double-click the card to open the card view (if you are not already in card view).

b. Click the **Provisioning > Port > General** tabs.

c. Choose the correct media type (**Fibre Channel - 1Gbps ISL**, **Fibre Channel - 2 Gbps ISL**, **FICON - 1 Gbps ISL**, or **FICON - 2 Gbps ISL**) from the drop-down list.

d. Click **Apply**.

Step 3 If the GFP-UP-MISMATCH alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) to report a Service-Affecting (SA) problem.

2.8.142 HELLO

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: OCN

The Open Shortest Path First (OSPF) Hello alarm is raised when the two end nodes cannot bring an OSPF neighbor up to the full state. Typically, this problem is caused by an area ID mismatch, and/or an OSPF HELLO packet loss over the DCC.

Clear the HELLO Alarm

Step 1 Ensure that the area ID is correct on the missing neighbor:

a. In node view, click the **Provisioning > Network > OSPF** tabs.

b. Ensure that the IP address in the Area ID column matches the other nodes.

c. If the address does not match, click the incorrect cell and correct it.

d. Click **Apply**.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.143 HIBATVG

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Object: PWR

The High Voltage Battery alarm occurs in a –48 VDC environment when a battery lead input voltage exceeds the high power threshold. This threshold, with a default value of –52 VDC, is user-provisionable. The alarm remains raised until the voltage remains under the threshold for 120 seconds. (For information about changing this threshold, refer to the "Turn Up Node" chapter in the *Cisco ONS 15454 Procedure Guide*.

Clear the HIBATVG Alarm

Step 1 The problem is external to the ONS 15454. 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.

2.8.144 HI-CCVOLT

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: BITS

The 64K Composite Clock High NE Voltage alarm occurs when the 64K signal peak voltage exceeds 1.1 VDC.

Clear the HI-CCVOLT Condition

Step 1 Lower the source voltage to the clock.

Step 2 If the condition does not clear, add more cable length or add a 5 dBm attenuator to the cable.

Step 3 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

2.8.145 HI-LASERBIAS

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Objects: EQPT, OCN

DWDM Logical Objects: 2R, ESCON, FC, GE, ISC, PPM, TRUNK

The Equipment High Transmit Laser Bias Current alarm is raised against TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, MXP_2.5G_10G, and OC192-XFP card laser performance. The alarm indicates that the card laser has reached the maximum laser bias tolerance.

Laser bias typically starts at about 30 percent of the manufacturer maximum laser bias specification and increases as the laser ages. If the HI-LASERBIAS alarm threshold is set at 100 percent of the maximum, the laser usability has ended. If the threshold is set at 90 percent of the maximum, the card is still usable for several weeks or months before it needs to be replaced.

Note For more information about provisioning MXP or TXP PPMs, refer to the "Provision Transponder and Muxponder Cards" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For more information about the cards themselves, refer to the "Card Reference" chapter.

Clear the HI-LASERBIAS Alarm

Step 1 Complete the "Clear the LASEREOL Alarm" procedure on page 2-127, which can include replacing the card. Replacement is not urgent and can be scheduled during a maintenance window.

Caution Removing an active card can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-231 for commonly used traffic-switching procedures.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.146 HI-LASERTEMP

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Objects: EQPT, OCN

DWDM Logical Object: PPM

The Equipment High Laser Optical Transceiver Temperature alarm applies to the TXP and MXP cards. HI-LASERTEMP occurs when the internally measured transceiver temperature exceeds the card setting by 35.6 degrees F (2 degrees C). A laser temperature change affects the transmitted wavelength.

When the TXP or MXP card raises this alarm, the laser is automatically shut off. The "LOS (OCN)" alarm on page 2-147 is raised at the far-end node and the "DUP-IPADDR" alarm on page 2-71 is raised at the near end.

Note For more information about provisioning MXP or TXP PPMs, refer to the "Provision Transponder and Muxponder Cards" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For more information about the cards themselves, refer to the "Card Reference" chapter.

Clear the HI-LASERTEMP Alarm

Step 1 In node view, double-click the TXP or MXP card to open the card view.

Step 2 Click the **Performance > Optics PM > Current Values** tabs.

Step 3 Verify the card laser temperature levels. Maximum, minimum, and average laser temperatures are shown in the Current column entries in the Laser Temp rows.

Step 4 Complete the "Reset a Traffic Card in CTC" procedure on page 2-239 for the MXP or TXP card.

Step 5 If the alarm does not clear, complete the "Physically Replace a Traffic Card" procedure on page 2-243 for the reporting MXP or TXP card.

Step 6 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.147 HI-RXPOWER

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: OCN

DWDM Logical Objects: 2R, ESCON, FC, GE, ISC, TRUNK

The Equipment High Receive Power alarm is an indicator of the optical signal power that is transmitted to the TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, MXP_2.5G_10G, or OC192-XFP card. HI-RXPOWER occurs when the measured optical power of the received signal exceeds the threshold. The threshold value is user-provisionable.

Note For more information about MXP or TXP cards, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Note When you upgrade a node to Software Release 6.0 or later, this enables received optical power PMs for the OC3-8, OC192-SR, OC192-IR, OC192-ITU, OC-192-XFP, MRC-12, and MRC25G-4 cards. The newly enabled HI-RXPOWER and LO-RXPOWER alarms require that you initialize a site-accepted optical power (OPR0) nominal value after the upgrade. (To do this, refer to the procedure in the "Turn Up a Node" chapter in the *Cisco ONS 15454 Procedure Guide*.) When you apply the value change, CTC uses the new OPR0 value to calculate PM percentage values. If you do not change the nominal value, the HI-RXPOWER or LO-RXPOWER may be raised in response to the unmodified setting.

Clear the HI-RXPOWER Alarm

Step 1 Find out whether gain (the amplification power) of any amplifiers has been changed. This change also causes channel power to need adjustment.

Step 2 Find out whether channels have been dropped from the fiber. Increasing or decreasing channels can affect power. If channels have been dropped, the power levels of all channels have to be adjusted.

Note If the card is part of an amplified DWDM system, dropping channels on the fiber affects the transmission power of each channel more than it would in an unamplified system.

Step 3 At the transmit end of the errored circuit, decrease the transmit power level within safe limits.

Step 4 If neither of these problems cause the HI-RXPOWER alarm, there is a slight possibility that another wavelength is drifting on top of the alarmed signal. In this case, the receiver gets signals from two transmitters at the same time and data alarms would be present. If wavelengths are drifting, the data is garbled and receive power increases by about +3 dBm.

Step 5 If the alarm does not clear, add fiber attenuators to the receive ports. Start with low-resistance attenuators and use stronger ones as needed, depending on factors such as the transmission distance, according to standard practice.

Step 6 If the alarm does not clear and no faults are present on the other port(s) of the transmit or receive card, use a known-good loopback cable to complete the "Perform a Facility (Line) Loopback on a Source-Node MXP/TXP/FC_MR-4 Port" procedure on page 1-90 and test the loopback.

Step 7 If a port is bad and you need to use all the port bandwidth, complete the "Physically Replace a Traffic Card" procedure on page 2-243. If the port is bad but you can move the traffic to another port, replace the card at the next available maintenance window.

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).

2.8.148 HITEMP

Default Severity: Critical (CR), Service-Affecting (SA) for NE; Default Severity: Minor (MN), Non-Service-Affecting (NSA) for EQPT

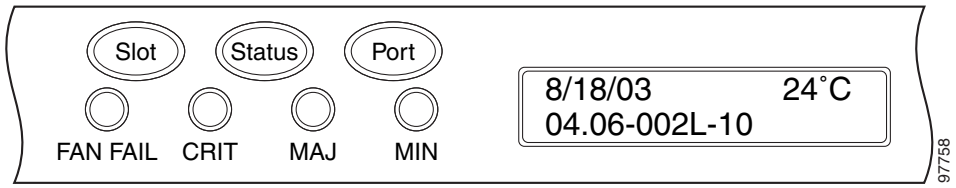
SONET Logical Objects: EQPT, NE

The High Temperature alarm occurs when the temperature of the ONS 15454 is above 122 degrees F (50 degrees C).

Clear the HITEMP Alarm

Step 1 View the temperature displayed on the ONS 15454 LCD front panel (Figure 2-2).

Figure 2-2 Shelf LCD Panel



Step 2 Verify that the environmental temperature of the room is not abnormally high.

Step 3 If the room temperature is not abnormal, physically ensure that nothing prevents the fan-tray assembly from passing air through the ONS 15454 shelf.

Step 4 If airflow is not blocked, physically ensure that blank faceplates fill the ONS 15454 shelf empty slots. Blank faceplates help airflow.

Step 5 If faceplates fill the empty slots, determine whether the air filter needs replacement. Refer to the "Inspect, Clean, and Replace the Reusable Air Filter" procedure on page 2-247.

Step 6 If the fan does not run or the alarm persists, complete the "Replace the Fan-Tray Assembly" procedure on page 2-249.

Note The fan should run immediately when correctly inserted.

Step 7 If the replacement fan-tray assembly does not operate correctly, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC to report a Service-Affecting (SA) problem (1 800 553-2447) if it applies to the NE, or a Non-Service-Affecting (NSA) problem if it applies to equipment.

2.8.149 HI-TXPOWER

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Objects: EQPT, OCN

DWDM Logical Objects: 2R, ESCON, FC, GE, ISC, PPM, TRUNK

The Equipment High Transmit Power alarm is an indicator on the TXP_MR_E, TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, MXP_2.5G_10G, or OC192-XFP card transmitted optical signal power. HI-TXPOWER occurs when the measured optical power of the transmitted signal exceeds the threshold.

Note For more information about provisioning MXP or TXP PPMs, refer to the "Provision Transponder and Muxponder Cards" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For more information about the cards themselves, refer to the "Card Reference" chapter.

Clear the HI-TXPOWER Alarm

Step 1 In node view, double-click the card view for the TXP_MR_10E, TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, MXP_2.5G_10G, or OC192-XFP card.

Step 2 Click the **Provisioning > Optics Thresholds > Current Values** tabs.

Step 3 Decrease (change toward the negative direction) the OPT-HIGH column value by 0.5 dBm.

Step 4 If the card transmit power setting cannot be lowered without disrupting the signal, complete the "Physically Replace a Traffic Card" section on page 2-243.

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).

2.8.150 HLDOVRSYNC

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: NE-SREF

The Holdover Synchronization Mode condition is caused by loss of the primary and second timing references in the node. Timing reference loss occurs when line coding on the timing input is different from the configuration on the node, and it often occurs during the selection of a new node reference clock. The condition clears when primary or second timing is reestablished. After the 24-hour holdover period expires, timing slips could begin to occur on an ONS 15454 relying on an internal clock.

Clear the HLDOVRSYNC Condition

Step 1 Clear additional alarms that relate to timing, such as:

- 2.8.127 FRNGSYNC, page 2-105
- 2.8.128 FSTSYNC, page 2-105
- 2.8.175 LOF (BITS), page 2-131
- 2.8.190 LOS (BITS), page 2-141
- 2.8.236 MANSWTOINT, page 2-161
- 2.8.237 MANSWTOPRI, page 2-162
- 2.8.238 MANSWTOSEC, page 2-162
- 2.8.239 MANSWTOTHIRD, page 2-162
- 2.8.354 SWTOPRI, page 2-210
- 2.8.355 SWTOSEC, page 2-210
- 2.8.356 SWTOTHIRD, page 2-210
- 2.8.357 SYNC-FREQ, page 2-211
- 2.8.359 SYNCPRI, page 2-212
- 2.8.360 SYNCSEC, page 2-212
- 2.8.361 SYNCTHIRD, page 2-213

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 15454 Procedure Guide.*

Step 3 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

2.8.151 I-HITEMP

Default Severity: Critical (CR), Service-Affecting (SA)

SONET Logical Object: NE

The Industrial High Temperature alarm occurs when the temperature of the ONS 15454 is above 149 degrees F (65 degrees C) or below –40 degrees F (–40 degrees C). This alarm is similar to the HITEMP alarm but is used for the industrial environment. If this alarm is used, you can customize your alarm profile to ignore the lower-temperature HITEMP alarm.

Clear the I-HITEMP Alarm

Step 1 Complete the "Clear the HITEMP Alarm" procedure on page 2-115.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call TAC (1-800-553-2447) in order to report a Service-Affecting (SA) problem.

2.8.152 IMPROPRMVL

Default Severity: Critical (CR), Service-Affecting (SA)

SONET Logical Object: EQPT

DWDM Logical Object: PPM

The Improper Removal equipment alarm can occur in the following situations:

- A card is physically removed from its slot before being deleted from CTC
- A card is not completely plugged into the backplane
- A card has an electrical or circuit failure
- A PPM is provisioned without first being inserted

If the alarm is caused by card removal, the card does not need to be in service; it only needs to be recognized by CTC. (IMPROPRMVL does not appear if you delete the card from CTC before physically removing the card from the node.) The alarm can also be raised if the card is physically present but not fully plugged into the backplane.

An IMPROPRMVL alarm can also occur if a card is failing because of a shorted circuit or an electrical component failure. This kind of failure can only be resolved by card replacement. In an MSTP network, such an electrical failure (on an amplifier, multiplexer, demultiplexer, or 32WSS card) and the resulting

IMRPROPRMVL alarm can be the root cause of many subsequent circuit alarms. If an alarm storm occurs on an MSTP network, finding an IMPROPRMVL equipment alarm within the generated alarms is a good indicator for troubleshooting purposes.

For PPMs, the alarm occurs if you provision a PPM but no physical module is inserted on the port.

Caution Do not remove a card during a card reboot. If CTC begins to reboot a card before you remove 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. When you delete the card, CTC loses connection with the node view and go to network view.

Note CTC gives the user approximately 15 seconds to physically remove the card before CTC begins a card reboot.

Note It can take up to 30 minutes for software to be updated on a standby TCC2/TCC2P.

Clear the IMPROPRMVL Alarm

Step 1 In node view, right-click the card reporting the IMPROPRMVL.

Step 2 Choose **Delete** from the shortcut menu.

Note CTC does not allow you to delete the reporting card if the card is in service, does have circuits mapped to it, is paired in a working protection scheme, has DCC enabled, or is used as a timing reference.

Step 3 If any ports on the card are in service, place them out of service (OOS,MT):

Caution Before placing a port out of service (OOS,MT or OOS,DSBLD), ensure that no live traffic is present.

a. In node view, double-click the reporting card to open the card view.
b. Click the **Provisioning > Line** tab.
c. Click the Admin State column of any in-service (IS) ports.
d. Choose **OOS,MT** to take the ports out of service.

Step 4 If a circuit has been mapped to the card, complete the "Delete a Circuit" procedure on page 2-244.

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:

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:

a. Click the ONS 15454 **Provisioning > Comm Channels > SDCC** 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:

a. Click the **Provisioning > Timing > General** tabs.

b. Under NE Reference, click the drop-down arrow for **Ref-1**.

c. Change Ref-1 from the listed OC-N 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. If the TAC technician tells you to, complete the following procedures:

Step 9 Under TAC's supervision, complete the "Remove and Reinsert (Reseat) Any Card" procedure on page 2-242.

Step 10 If the alarm does not clear, under TAC's supervision complete the "Physically Replace a Traffic Card" procedure on page 2-243.

Step 11 With TAC's direction, determine whether to RMA the faulty card.

2.8.153 INC-ISD

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: DS3

The DS-3 Idle condition indicates that the DS-3 card is receiving an idle signal, meaning that the payload of the signal contains a repeating pattern of bits. The INC-ISD condition occurs when the transmitting port has an OOS-MA,MT service state. It is resolved when the OOS-MA,MT state ends.

Note INC-ISD is a condition and not an alarm. It is for information only and does not require troubleshooting.

2.8.154 INHSWPR

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: EQPT

The Inhibit Switch To Protect Request on Equipment condition occurs on traffic cards when the ability to switch to protect has been disabled. If the card is part of a 1:1 or 1+1 protection scheme, traffic remains locked onto the working system. If the card is part of a 1:N protection scheme, traffic can be switched between working cards when the switch to protect is disabled.

Clear the INHSWPR Condition

Step 1 If the condition is raised against a 1+1 port, complete the "Initiate a 1+1 Manual Switch Command" section on page 2-232.

Step 2 If the condition is raised against a 1:1 card, complete the "Initiate a 1:1 Card Switch Command" procedure on page 2-234 to switch it back.

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).

2.8.155 INHSWWKG

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: EQPT

The Inhibit Switch To Working Request on Equipment condition occurs on traffic cards when the ability to switch to working has been disabled. If the card is part of a 1:1 or 1+1 protection scheme, traffic remains locked onto the protect system. If the card is part of a 1:N protection scheme, traffic can be switched between protect cards when the switch to working is disabled.

Clear the INHSWWKG Condition

Step 1 If the condition is raised against a 1+1 port, complete the "Initiate a 1+1 Manual Switch Command" section on page 2-232.

Step 2 If it is raised against a 1:1 card, complete the "Initiate a 1:1 Card Switch Command" procedure on page 2-234 to switch traffic back.

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).

2.8.156 INTRUSION-PSWD

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: NE

The Security Intrusion Incorrect Password condition occurs after a user attempts a provisionable (by Superuser) number of unsuccessful logins, a login with an expired password, or an invalid password. The alarmed user is locked out of the system, and INTRUSION-PSWD condition is raised. This condition is only shown in Superuser login sessions, not in login sessions for lower-level users. The INTRUSION-PSWD condition is automatically cleared when a provisionable lockout timeout expires, or it can be manually cleared in CTC by the Superuser if the lockout is permanent.

Clear the INTRUSION-PSWD Condition

Step 1 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).

2.8.157 INVMACADR

Default Severity: Major (MJ), Non-Service Affecting (NSA)

SONET Logical Object: AIP

The Equipment Failure Invalid MAC Address alarm occurs when the ONS 15454 MAC address is invalid. Each ONS 15454 has a unique, permanently assigned MAC address. The address resides on an AIP EEPROM. The TCC2/TCC2P reads the address value from the AIP chip during boot-up and keeps this value in its synchronous dynamic RAM (SDRAM).

Under normal circumstances, the read-only MAC address can be viewed in the Provisioning/Network tab in CTC.

The ONS 15454 uses both IP and MAC addresses for circuit routing. When an INVMACADR alarm exists on a node, you see a PARTIAL circuit in the CTC circuit status column. The circuit works and is able to carry traffic, but CTC cannot logically display the circuit end-to-end information.

An invalid MAC address can be caused when:

- There is a read error from the AIP during bootup; in this case, the reading TCC2/TCC2P uses the default MAC address (00-10-cf-ff-ff-ff).
- There is a read error occurring on one of the redundant TCC2/TCC2Ps that read the address from the AIP; these cards read the address independently and could therefore each read different address values.
- An AIP component failure causes a read error.
- The ribbon cable connecting the AIP card to the backplane is bad.

Clear the INVMACADR Alarm

Step 1 Check for any outstanding alarms that were raised against the active and standby TCC2/TCC2P and resolve them.

Step 2 If the alarm does not clear, determine whether the LCD display on the fan tray (Figure 2-2 on page 2-115) is blank or if the text is garbled. If so, proceed to Step 8. If not, continue with Step 3.

Step 3 At the earliest maintenance window, reset the standby TCC2/TCC2P:

Note The reset requires approximately five minutes. Do not perform any other step until the reset is complete.

a. Log into a node on the network. If you are already logged in, continue with Step b.

b. Identify the active TCC2/TCC2P.

   A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

c. Right-click the standby TCC2/TCC2P in CTC.

d. Choose **Reset Card** from the shortcut menu.

e. Click **Yes** in the Are You Sure dialog box.

   The card resets, the FAIL LED blinks on the physical card, and connection to the node is lost. CTC switches to network view.

f. Verify that the reset is complete and error-free, and that no new related alarms appear in CTC. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

g. Double-click the node and ensure that the reset TCC2/TCC2P is still in standby mode and that the other TCC2/TCC2P is active.

   A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

h. Ensure that no new alarms associated with this reset appear in the CTC Alarms window.

If the standby TCC2/TCC2P fails to boot into standby mode and reloads continuously, the AIP is probably defective. In this case, the standby TCC2/TCC2P is unsuccessfully attempting to read the EEPROM located on the AIP. The TCC2/TCC2P reloads until it reads the EEPROM. Proceed to Step 8.

Step 4 If the standby TCC2/TCC2P rebooted successfully into standby mode, complete the "Remove and Reinsert (Reseat) the Standby TCC2/TCC2P Card" procedure on page 2-241.

Resetting the active TCC2/TCC2P causes the standby TCC2/TCC2P to become active. The standby TCC2/TCC2P keeps a copy of the chassis MAC address. If its stored MAC address is valid, the alarm should clear.

Step 5 After the reset, note whether or not the INVMACADR alarm has cleared or is still present.

Step 6 Complete the "Reset an Active TCC2/TCC2P Card and Activate the Standby Card" procedure on page 2-240 again to place the standby TCC2/TCC2P back into active mode.

After the reset, note whether or not the INVMACADR alarm has cleared or is still present. If the INVMACADR alarm remains standing through both TCC2/TCC2P resets, this indicates that the AIP is probably defective. Proceed to Step 8.

If the INVMACADR was raised during one TCC2/TCC2P reset and cleared during the other, the TCC2/TCC2P that was active while the alarm was raised needs to be replaced. Continue with Step 7.

Step 7 If the faulty TCC2/TCC2P is currently in standby mode, complete the "Physically Replace a Traffic Card" procedure on page 2-243 for this card. If the faulty TCC2/TCC2P is currently active, during the next available maintenance window complete the "Reset an Active TCC2/TCC2P Card and Activate the Standby Card" procedure on page 2-240 and then complete the "Physically Replace a Traffic Card" procedure on page 2-243.

Note If the replacement TCC2/TCC2P is loaded with a different software version from the current TCC2/TCC2P, the card bootup could take up to 30 minutes. During this time, the card LEDs flicker between Fail and Act/Sby as the active TCC2/TCC2P version software is copied to the new standby card.

Step 8 Open a case with Cisco TAC (1 800 553-2447) for assistance with determining the node's previous MAC address.

Step 9 Replace the ribbon cable between the system board and the AIP with a known-good cable.

Step 10 If the alarm persists, complete the "Replace the Alarm Interface Panel" procedure on page 2-251.

Step 11 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.158 IOSCFGCOPY

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: EQPT

The IOS Configuration Copy in Progress condition occurs on ML-Series Ethernet cards when a Cisco IOS startup configuration file is being uploaded or downloaded to or from an ML-Series card. (This condition is very similar to the "SFTWDOWN" condition on page 2-197 but it applies to ML-Series Ethernet cards rather than to the TCC2/TCC2P.)

The condition clears after the copy operation is complete. (If it does not complete correctly, the "NO-CONFIG" condition on page 2-169 could be raised.)

Note IOSCFGCOPY is an informational condition.

Note For more information about the ML-Series Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.*

2.8.159 ISIS-ADJ-FAIL

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: OCN

The Open System Interconnection (OSI) Intermediate System to Intermediate-System (IS-IS) Adjacency Failure alarm is raised by an intermediate system (node routing IS Level 1 or Level 1 and 2) when no IS or end system (ES) adjacency is established on a point-to-point subnet. The Intermediate-System Adjacency Failure alarm is not supported by ES. It is also not raised by IS for disabled routers.

The alarm is typically caused by a misconfigured router manual area adjacency (MAA) address. For more information about IS-IS OSI routing and MAA configuration, refer to the "Management Network Connectivity" chapter in the *Cisco ONS 15454 Reference Manual*. For more information about configuring OSI, refer to the "Turn Up Node" chapter in the *Cisco ONS 15454 Procedure Guide*.

Clear the ISIS-ADJ-FAIL Alarm

Step 1 Ensure that both ends of the communication channel are using the correct Layer 2 protocol and settings (LAPD or PPP). To do this, complete the following steps:

a. At the local node, in node view, click the **Provisioning > Comm Channels > SDCC** tabs.

b. Click the row of the circuit. Click **Edit**.

c. In the Edit SDCC 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. Login to the remote node and follow the same steps, also recording the same information for this node.

Step 2 If both nodes do not use the same Layer 2 settings, you will have to delete the incorrect termination and recreate it. To delete it, click the termination and click **Delete**. To recreate it, refer to the "Turn Up Node" chapter in the *Cisco ONS 15454 Procedure Guide* for the procedure.

Step 3 If the nodes use PPP Layer 2, complete the "Clear the EOC Alarm" procedure on page 2-75. 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 SDCC 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 SDCC 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 SDCC dialog box and click **OK**.

Step 7 If all of the preceding settings are correct, ensure that OSI routers are enabled for the communications channels at both ends:

a. Click **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 communications channel have a common MAA:

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 15454 Procedure Guide* for procedures.

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).

2.8.160 KB-PASSTHR

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: OCN

The K Bytes Pass Through Active condition occurs on a nonswitching node in a BLSR 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 BLSR ring is being exercised using the Exercise Ring command.

Clear the KB-PASSTHR Condition

Step 1 Complete the "Clear a BLSR External Switching Command" procedure on page 2-239.

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).

2.8.161 KBYTE-APS-CHANNEL-FAILURE

Default Severity: Minor (MN), Non-Service Affecting (NSA)

SONET Logical Object: OCN

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 the "AIS-P" alarm on page 2-33, the "LOF (OCN)" alarm on page 2-135, the "LOS (OCN)" alarm on page 2-147 or the "SF-P" alarm on page 2-197.

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 "Turn Up Network" chapter in the *Cisco ONS 15454 Procedure Guide*.

Step 2 If the error is not caused by misprovisioning, it is due to checksum errors within an OC-N, cross-connect, or TCC2/TCC2P. In this case, complete the "Side Switch the Active and Standby Cross-Connect Cards" procedure on page 2-240 to allow CTC to resolve the issue.

Step 3 If third-party equipment is involved, ensure that it is configured for the same APS channel as the Cisco ONS equipment.

Step 4 If the 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).

2.8.162 LAN-POL-REV

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: NE

The LAN Connection Polarity Reversed condition is not raised in shelves that contain TCC2 cards. It is raised during a software upgrade when the card detects that a connected Ethernet cable has reversed receive wire pairs. The card automatically compensates for this reversal, but LAN-POL-REV stays active.

Note For more information about Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.

Clear the LAN-POL-REV Condition

Step 1 Replace the connected Ethernet cable with a cable that has the correct pinout. For correct pin mapping, refer to the "Maintain the Node" chapter in the *Cisco ONS 15454 Procedure Guide*.

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).

2.8.163 LASER-APR

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.164 LASERBIAS-DEG

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.165 LASERBIAS-FAIL

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.166 LASEREOL

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: OCN

The Laser Approaching End of Life alarm applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G cards. It is typically accompanied by the "HI-LASERBIAS" alarm on page 2-112. It is an indicator that the laser in the card must be replaced. How soon the replacement must happen depends upon the HI-LASERBIAS threshold. If the threshold is set under 100 percent, the laser replacement can usually be done during a maintenance window. But if the HI-LASERBIAS threshold is set at 100 percent and is accompanied by data errors, the card must be replaced sooner.

Note For more information about MXP or TXP cards, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Clear the LASEREOL Alarm

Step 1 Complete the "Physically Replace a Traffic Card" procedure on page 2-243.

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).

2.8.167 LASERTEMP-DEG

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.168 LCAS-CRC

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: STSTRM, VT-TERM

The Link Capacity Adjustment Scheme (LCAS) Control Word CRC Failure condition is raised against ML-Series Ethernet cards and CE-series cards. It occurs when there is an equipment, path, or provisioning error on the virtual concatenation group (VCG) that causes consecutive 2.5 second CRC failures in the LCAS control word.

Transmission errors would be reflected in CV-P, ES-P, or SES-P performance monitoring statistics. If these errors do not exist, an equipment failure is indicated.

If LCAS is not supported on the peer node, the condition does not clear.

LCAS-CRC can also occur if the VCG source node is not LCAS-enabled, but the receiving node does have the capability enabled. Both source and destination nodes must have LCAS enabled. Otherwise, the LCAS-CRC condition persists on the VCG.

Note For more information about the ML-Series Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.*

Clear the LCAS-CRC Condition

Step 1 Look for and clear any associated equipment failures, such as the EQPT alarm, on the receive node or transmit node.

Step 2 Look for and clear any bit error rate alarms at the transmit node.

Step 3 If no equipment or SONET path errors exist, ensure that the remote node has LCAS enabled on the circuit:

a. In node view, click the **Circuits** tab.

b. Choose the VCAT circuit and click **Edit**.

c. In the Edit Circuit window, click the **General** tab.

d. Verify that the Mode column says **LCAS**.

Step 4 If the column does not say LCAS, complete the "Delete a Circuit" procedure on page 2-244 and recreate it in LCAS mode using the instructions in the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.

Step 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).

2.8.169 LCAS-RX-FAIL

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: STSTRM, VT-TERM

The LCAS VCG Member Receive-Side-In Fail condition is raised against CE-series cards, FC_MR-4 cards and ML-Series Ethernet cards with LCAS-enabled VCG.

LCAS VCGs treat failures unidirectionally, meaning that failures of the transmit or receive points occur independently of each other. The LCAS-RX-FAIL condition can occur on the receive side of an LCAS VCG member for the following reasons:

- SONET path failure (a unidirectional failure as seen by the receive side)
- VCAT member is set out of group at the transmit side, but is set in group at the receive side
- VCAT member does not exist at the transmit side but does exist and is in group at the receive side

The condition can be raised during provisioning operations on LCAS VCGs but should clear when the provisioning is completed.

Software-enabled LCAS VCGs treat failure bidirectionally, meaning that both directions of a VCG member are considered failed if either transmit or receive fails. The LCAS-RX-FAIL condition is raised on these VCG members when a member receive side fails due to a SONET path failure.

Note For more information about the ML-Series Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.*

Note ML-Series cards are LCAS-enabled. ML-Series and FC_MR-4 cards are SW-LCAS enabled.

Clear the LCAS-RX-FAIL Condition

Step 1 Check for and clear any line or path alarms.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.170 LCAS-TX-ADD

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: STSTRM, VT-TERM

The LCAS VCG Member Transmit-Side-In Add State condition is raised against ML-Series Ethernet cards and CE-series cards when the transmit side of an LCAS VCG member is in the add state. The condition clears after provisioning is completed. The remote likely reports a path condition such as the "AIS-P" condition on page 2-33 or the "UNEQ-P" alarm on page 2-223.

Note LCAS-TX-ADD is an informational condition and does not require troubleshooting.

Note For more information about the ML-Series Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.

2.8.171 LCAS-TX-DNU

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: STSTRM, VT-TERM

The LCAS VCG Member Transmit-Side-In Do Not Use condition is raised on FC_MR-4 cards, ML-Series Ethernet cards, and CE-series cards when the transmit side of an LCAS VCG member is in the do-not use state. For a unidirectional failure, this condition is only raised at the source node. The LCAS-TX-DNU condition is raised when the cable is unplugged.

The node reporting this condition likely reports an "RFI-P" alarm on page 2-185, and the remote node likely reports a path alarm such as the "AIS-P" alarm on page 2-33 or the "UNEQ-P" alarm on page 2-223.

Note LCAS-TX-DNU is an informational condition and does not require troubleshooting.

Note For more information about the ML-Series Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.

2.8.172 LKOUTPR-S

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: OCN

The Lockout of Protection Span condition occurs when span traffic is locked out of a protect span using the Lockout of Protect command. This condition is visible on the 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 BLSR External Switching Command" procedure on page 2-239.

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).

2.8.173 LOA

Default Severity: Critical (CR), Service-Affecting (SA)

SONET Logical Object: VCG

The Loss of Alignment on a VCG is a VCAT member alarm. (VCAT member circuits are independent circuits that are concatenated from different time slots into a higher-rate signal.) The alarm occurs when members of a VCG travel over different paths in the network (due to initial operator provisioning or to protection or restoration events) and the differential delays between the paths cannot be recovered by terminating hardware buffers.

Note This alarm occurs only if you provision circuits outside of CTC, such as by using TL1.

Clear the LOA Alarm

Step 1 In network view, click the **Circuits** tab.

Step 2 Click the alarmed VCG and then click **Edit**.

Step 3 In the Edit Circuit window, view the source and destination circuit slots, ports, and STSs.

Step 4 Identify whether the STS travels across different fibers. If it does, complete the "Delete a Circuit" procedure on page 2-244.

Step 5 Recreate the circuit using the procedure in the "Create Circuits and VT Tunnels" chapter in the *Cisco ONS 15454 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) in order to report a Service-Affecting (SA) problem.

2.8.174 LOCKOUT-REQ

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: EQPT, OCN, STSMON, VT-MON

DWDM Logical Objects: 2R, ESCON, FC, GE, ISC, TRUNK

The Lockout Switch Request on Facility or Equipment condition occurs when a user initiates a lockout switch request for an OC-N port in a 1+1 facility protection group. This can be accomplished by locking traffic onto the working port with the LOCK ON command (thus locking it off the protect port), or locking it off the protect port with the LOCK OUT command. In either case, the protect port will show "Lockout of Protection," and the Conditions window will show the LOCKOUT-REQ condition.

A lockout prevents protection switching. Clearing the lockout again allows protection switching and clears the LOCKOUT-REQ condition.

Clear the LOCKOUT-REQ Condition

Step 1 Complete the "Clear a Lock-On or Lockout Command" procedure on page 2-234.

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).

2.8.175 LOF (BITS)

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: BITS

The Loss of Frame (LOF) BITS alarm occurs when a port on theTCC2/TCC2P BITS input detects an LOF on the incoming BITS timing reference signal. LOF indicates that the receiving ONS 15454 has lost frame delineation in the incoming data.

Note The procedure assumes that the BITS timing reference signal is functioning properly. It also assumes the alarm is not appearing during node turn-up.

Clear the LOF (BITS) Alarm

Step 1 Verify that the line framing and line coding match between the BITS input and the TCC2/TCC2P:

a. In node or card view, note the slot and port reporting the alarm.

b. Find the coding and framing formats of the external BITS timing source. The formats should be in the user documentation for the external BITS timing source or on the timing source itself.

c. Click the **Provisioning > Timing > BITS Facilities** tabs.

d. Verify that the Coding setting matches the coding of the BITS timing source, either B8ZS or AMI.

e. If the coding does not match, click **Coding** and choose the appropriate coding from the drop-down list.

f. Verify that Framing matches the framing of the BITS timing source, either ESF or SF (D4).

g. If the framing does not match, click **Framing** and choose the appropriate framing from the drop-down list.

Note On the timing subtab, the B8ZS coding field is normally paired with ESF in the Framing field and the AMI coding field is normally paired with SF (D4) in the Framing field.

Step 2 If the alarm does not clear when the line framing and line coding match between the BITS input and the TCC2/TCC2P, complete the "Physically Replace a Traffic Card" procedure on page 2-243 for the TCC2/TCC2P.

Step 3 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

2.8.176 LOF (DS1)

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Object: DS1

The DS-1 LOF alarm indicates that the receiving ONS 15454 has lost frame delineation in an incoming DS-1 data stream.

Clear the LOF (DS1) Alarm

Step 1 Verify that the line framing and line coding match between the DS1 port and the signal source:

a. In CTC, note the slot and port reporting the alarm.

b. Find the coding and framing formats of the signal source for the card reporting the alarm. You could need to contact your network administrator for the format information.

c. Display the card view of the reporting card.

d. Click the **Provisioning > Line** tabs.

e. Verify that the line type of the reporting port matches the line type of the signal source (DS4 and DS4, unframed and unframed, or ESF and ESF). If the signal source line type does not match the reporting port, click the **Line Type** cell to reveal a drop-down list and choose the matching type.

f. Verify that the reporting Line Coding matches the signal source line coding (AMI and AMI or B8ZS and B8ZS). If the signal source line coding does not match the reporting port, click the **Line Coding** cell and choose the correct type from the drop-down list.

g. Click **Apply**.

Note On the Line tab, the B8ZS coding field is normally paired with ESF in the Framing field. AMI coding is normally paired with SF (D4) in the Framing field.

Note When you replace a card with the identical type of card, you do not need to make any changes to the database.

Step 2 If the alarm does not clear, log into the 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.

2.8.177 LOF (DS3)

Default Severity: Critical (CR), Service-Affecting (SA)

SONET Logical Object: DS3

The DS-3 LOF alarm indicates that the receiving ONS 15454 has lost frame delineation in the incoming DS-3 data stream on DS3XM-6, DS3XM-12, or add DS3/EC1-48 cards. The framing of the transmitting equipment could be set to a format that differs from the receiving system. On DS3XM-6 cards, the alarm occurs only on cards with the provisionable framing format set to C Bit or M13 and not on cards with the provisionable framing format is set to unframed.

Clear the LOF (DS3) Alarm

Step 1 Change the line type of the non-ONS equipment attached to the reporting card to C Bit:

a. Display the card view of the reporting card.

b. Click the **Provisioning > Line** tabs.

c. Verify that the line type of the reporting port matches the line type of the signal source.

d. If the signal source line type does not match the reporting port, click **Line Type** and choose **C Bit** from the drop-down list.

e. Click **Apply**.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

2.8.178 LOF (E1)

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Object: E1

The E1 LOF alarm appears on the DS1/E1-56 card when the card is placed in All E1 mode. It indicates that the receiving ONS 15454 has lost frame delineation in an incoming E1 data stream. The transmitting equipment could possibly have its framing set to a format that differs from the receiving node. For more information about the DS1/E1-56 card, refer to the "Electrical Cards" chapter in the *Cisco ONS 15454 Reference Manual*.

Note The DS1/E1-56 card only carries an E1 signal within an STS-3c/VT2 circuit.

Clear the LOF (E1) Alarm

Step 1 Verify that the line framing and line coding match between the DS1/E1-56 port and the signal source:

a. In CTC, note the slot and port reporting the alarm.

b. Find the coding and framing formats of the signal source for the card reporting the alarm. You could need to contact your network administrator for this information.

c. Double-click the DS1/E1-56 card to open the card view.

d. Click the **Provisioning > Line** tabs.

e. Verify that the line type of the reporting port matches the line type (E1_MF, E1_CRCMF, AUTOFRAMED, UNFRAMED) of the signal source. If the signal source line type does not match the reporting port, click the **Line Type** cell to reveal a drop-down list and choose the matching type.

f. Verify that the reporting Line Coding matches the signal source line coding. If the signal source line coding does not match the reporting port, click the **Line Coding** cell and choose the correct type from the drop-down list.

g. Click **Apply**.

Note When you replace a card with the identical type of card, you do not need to make any changes to the database.

Step 2 If the alarm does not clear, log into the 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.

2.8.179 LOF (EC1)

Default Severity: Critical (CR), Service-Affecting (SA)

SONET Logical Object: EC1

The EC1/EC1-12 LOF alarm occurs when a port on the reporting EC1/EC1-12 or DS3/EC1-48 card has an LOF condition. LOF indicates that the receiving ONS 15454 has lost frame delineation in the incoming data. LOF occurs when the SONET overhead loses a valid framing pattern for 3 milliseconds. Receiving two consecutive valid A1/A2 framing patterns clears the alarm.

Clear the LOF (EC1) Alarm

Step 1 Verify cabling continuity to the port reporting the alarm. To verify cable continuity, follow site practices.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 2 If cabling continuity is good, 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 15454 Procedure Guide*.

Step 3 If the alarm does not clear, see the loopback procedures in Chapter 1, "General Troubleshooting" to isolate the fault causing the LOF alarm.

Step 4 If the alarm does not clear, or if you need assistance conducting network troubleshooting tests, call Cisco TAC to report a Service-Affecting (SA) problem (1 800 553-2447).

2.8.180 LOF (OCN)

Default Severity: Critical (CR), Service-Affecting (SA)

SONET Logical Object: OCN

The LOF alarm occurs when a port on the reporting card has an LOF condition. It can also occur on ONS 15454 MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G,TXP_MR_10E, or TXPP_MR_2.5G cards reporting LOF. The alarm indicates that the receiving ONS 15454 has lost frame delineation in the incoming data. LOF occurs when the SONET overhead loses a valid framing pattern for 3 milliseconds. Receiving two consecutive valid A1/A2 framing patterns clears the alarm.

When the alarm is raised on an OC-N card, it is sometimes an indication that the OC-N card expects a specific line rate and the input line rate source does not match the input line rate of the optical receiver.

Note For information about MXP or TXP cards, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Clear the LOF (OCN) Alarm

Step 1 Verify cabling continuity to the port reporting the alarm.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly. To verify cable continuity, follow site practices.

Step 2 If cabling continuity is good, clean the fiber according to site practice. If no site practice exists, complete the procedure in the "Maintain the Node" chapter of the *Cisco ONS 15454 Procedure Guide*.

Step 3 If the alarm does not clear, see the loopback procedures in Chapter 1, "General Troubleshooting" to isolate the fault causing the LOF alarm.

Step 4 If the alarm does not clear, or if you need assistance conducting network troubleshooting tests, call Cisco TAC to report a Service-Affecting (SA) problem (1 800 553-2447).

2.8.181 LOF (STSTRM)

Default Severity: Critical (CR), Service-Affecting (SA)

SONET Logical Object: STSTRM

A Loss of Frame alarm for an STS circuit termination indicates that the LOF has occurred at the terminating point of the circuit (such as an OC-N port). It is similar to the "LOF (OCN)" alarm on page 2-135.

Clear the LOF (STSTRM) Alarm

Step 1 Complete the "Clear the LOF (OCN) Alarm" alarm on page 2-135.

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.

2.8.182 LOF (TRUNK)

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.183 LO-LASERBIAS

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Objects: EQPT, OCN

DWDM Logical Object: PPM

The Equipment Low Transmit Laser Bias Current alarm is raised against the TXP and MXP card laser performance. The alarm indicates that the card laser has reached the minimum laser bias tolerance.

If the LO-LASERBIAS alarm threshold is set at 0 percent (the default), the laser's usability has ended. If the threshold is set at 5 percent to10 percent, the card is still usable for several weeks or months before you need to replace it.

Note For more information about provisioning MXP or TXP PPMs, refer to the "Provision Transponder and Muxponder Cards" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For more information about the cards themselves, refer to the "Card Reference" chapter.

Clear the LO-LASERBIAS Alarm

Step 1 Complete the "Physically Replace a Traffic Card" procedure on page 2-243.

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).

2.8.184 LO-LASERTEMP

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Objects: EQPT, OCN

DWDM Logical Object: PPM

The Equipment Low Laser Optical Transceiver Temperature alarm applies to the TXP and MXP cards. LO-LASERTEMP occurs when the internally measured transceiver temperature falls below the card setting by35.6 degrees F or 2 degrees C. A laser temperature change affects the transmitted wavelength. (Two degrees Celsius is equivalent to about 200 picometers in the wavelength.)

When the TXP or MXP card raises this alarm, the laser is automatically shut off. The "LOS (OCN)" alarm on page 2-147 is raised at the far-end node and the "DUP-IPADDR" alarm on page 2-71 is raised at the near end. To verify the card laser temperature level, double-click the card in node view and click the **Performance > Optics PM > Current Values** tabs. Maximum, minimum, and average laser temperatures are shown in the Current column entries in the Laser Temp rows.

Note For more information about provisioning MXP or TXP PPMs, refer to the "Provision Transponder and Muxponder Cards" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For more information about the cards themselves, refer to the "Card Reference" chapter.

Clear the LO-LASERTEMP Alarm

Step 1 Complete the "Reset a Traffic Card in CTC" procedure on page 2-239 for the reporting MXP or TXP card.

Step 2 If the alarm does not clear, complete the "Physically Replace a Traffic Card" procedure on page 2-243 for the reporting MXP or TXP card.

Step 3 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.185 LOM

Default Severity: Critical (CR), Service-Affecting (SA) for STSMON, TRUNK; Major (MJ) for STSTRM, VT-TERM

SONET Logical Objects: STSMON, STSTRM, VT-TERM

DWDM Logical Object: TRUNK

The Optical Transport Unit (OTU) Loss of Multiframe is a VCAT member alarm. (VCAT member circuits are independent circuits that are concatenated from different time slots into a higher-rate signal.) The alarm applies to MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, TXP_MR_10E, or TXPP_MR_2.5G cards when the Multi Frame Alignment Signal (MFAS) overhead field is errored for more than five frames and persists for more than 3 milliseconds.

Note For more information about MXP or TXP cards, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Clear the LOM Alarm

Step 1 Complete the "Clear the SD-L Condition" procedure on page 2-193.

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.

2.8.186 LOP-P

Default Severity: Critical (CR), Service-Affecting (SA)

SONET Logical Objects: STSMON, STSTRM

A Loss of Pointer Path alarm indicates that the SONET path pointer in the overhead has been lost. LOP occurs when valid H1/H2 pointer bytes are missing from the overhead. Receiving equipment monitors the H1/H2 pointer bytes to locate the SONET payload. An LOP-P alarm occurs when eight, nine, or ten consecutive frames do not have valid pointer values. The alarm clears when three consecutive valid pointers are received.

The LOP-P alarm can occur when the received payload does not match the provisioned payload. The alarm is caused by a circuit type mismatch on the concatenation facility. For example, if an STS-1 is sent across a circuit provisioned for STS-3c, an LOP-P alarm occurs.

For the FC_MR-4 card, an LOP-P is raised if a port is configured for a SONET signal but receives an SONET signal instead. (This information is contained in the H1 byte bits 5 and 6.)

Clear the LOP-P Alarm

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 1 In node view, click the **Circuits** tab and view the alarmed circuit.

Step 2 Verify the circuit size listed in the Size column. If the size is different from what is expected, such as an STS3c instead of an STS1, this causes the alarm.

Step 3 If you have been monitoring the circuit with optical test equipment, a mismatch between the provisioned circuit size and the size expected by the test set can cause this alarm. For specific procedures to use the test set equipment, consult the manufacturer. Ensure that the test set monitoring is set up for the same size as the circuit provisioning.

Refer to the manufacturer's instructions for test-set use.

Step 4 If the error is not due to an incorrectly configured test set, the error is in the provisioned CTC circuit size. Complete the "Delete a Circuit" procedure on page 2-244.

Step 5 Recreate the circuit for the correct size. For procedures, refer to the "Create Circuits and VT Tunnels" chapter in the *Cisco ONS 15454 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) in order to report a Service-Affecting (SA) problem.

2.8.187 LOP-V

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Objects: VT-MON, VT-TERM

The LOP VT alarm indicates a loss of pointer at the VT level.

The LOP-V alarm can occur when the received payload does not match the provisioned payload. LOP-V is caused by a circuit size mismatch on the concatenation facility.

Clear the LOP-V Alarm

Step 1 Complete the "Clear the LOP-P Alarm" procedure on page 2-138.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. 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, 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.

2.8.188 LO-RXPOWER

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: OCN

DWDM Logical Objects: 2R, ESCON, FC, GE, ISC, TRUNK

The Equipment Low Receive Power alarm is an indicator for TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, MXP_2.5G_10G and OC192-XFP card received optical signal power. LO-RXPOWER occurs when the measured optical power of the received signal falls below the threshold value, which is user-provisionable.

Note For more information about MXP or TXP cards, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Note When you upgrade a node to Software Release 6.0 or later, this enables received optical power PMs for the OC3-8, OC192-SR, OC192-IR, OC192-ITU, OC-192-XFP, MRC-12, and MRC25G-4 cards. The newly enabled HI-RXPOWER and LO-RXPOWER alarms require that you initialize a site-accepted optical power (OPR0) nominal value after the upgrade. (To do this, refer to the procedure in the "Turn

Up a Node" chapter in the *Cisco ONS 15454 Procedure Guide*.) When you apply the value change, CTC uses the new OPR0 value to calculate PM percentage values. If you do not change the nominal value, the HI-RXPOWER or LO-RXPOWER may be raised in response to the unmodified setting.

Clear the LO-RXPOWER Alarm

Step 1 At the transmit end of the errored circuit, increase the transmit power level within safe limits.

Step 2 Find out whether new channels have been added to the fiber. Up to 32 channels can be transmitted on the same fiber, but the number of channels affects power. If channels have been added, power levels of all channels need to be adjusted.

Note If the card is part of an amplified DWDM system, adding channels on the fiber affects the transmission power of each channel more than it would in an unamplified system.

Step 3 Find out whether gain (the amplification power) of any amplifiers has been changed. Changing amplification also causes channel power to need adjustment.

Step 4 If the alarm does not clear, remove any receive fiber attenuators or replace them with lower-resistance attenuators.

Step 5 If the alarm does not clear, inspect and clean the receive and transmit node fiber connections according to site practice. If no site practice exists, complete the procedure in the "Maintain the Node" chapter in the *Cisco ONS 15454 Procedure Guide*.

Step 6 If the alarm does not clear, ensure that the fiber is not broken or damaged by testing it with an optical test set. If no test set is available, use the fiber for a facility (line) loopback on a known-good port. The error reading you get is not as precise, but you generally know whether the fiber is faulty. For specific procedures to use the test set equipment, consult the manufacturer.

Step 7 If the alarm does not clear, and no faults are present on the other port(s) of the transmit or receive card, do a facility loopback on the transmit and receive ports with known-good loopback cable. Complete the "Perform a Facility (Line) Loopback on a Source-Node Optical Port" procedure on page 1-49 or the "Perform a Facility (Line) Loopback on an Intermediate-Node Optical Port" procedure on page 1-58 to test the loopback.

Step 8 If a port is bad and you need to use all the port bandwidth, complete the "Physically Replace a Traffic Card" procedure on page 2-243. If the port is bad but you can move the traffic to another port, replace the card at the next available maintenance window.

Step 9 If no ports are shown bad and the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.189 LOS (2R)

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.190 LOS (BITS)

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: BITS

The LOS (BITS) alarm indicates that the TCC2/TCC2P has an LOS from the BITS timing source. The LOS (BITS) means the BITS clock or the connection to it failed.

Clear the LOS (BITS) Alarm

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 1 Verify the wiring connection from the BITS clock pin fields on the ONS 15454 backplane to the timing source.

Step 2 If wiring is good, verify that the BITS clock is operating properly.

Step 3 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

2.8.191 LOS (DS1)

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Object: DS1

A LOS (DS1) alarm for a DS-1 port occurs when the port on the card is in service but no signal is being received. A cabling issue or a configuration issue could cause this alarm. If an upstream equipment failure causes a transmission failure, the LOS (DS1) will likely be demoted by a card-level alarm (to the DS1/E1-56).

Clear the LOS (DS1) Alarm

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 1 Verify that the fiber cable is properly connected and attached from the correct transmitting port to the correct receiving port. For more information about fiber connections and terminations, refer to the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15454 Procedure Guide*.

Step 2 Clean the cable ends using site practices or, if none exists, complete the procedure in the "Maintain the Node" chapter of the *Cisco ONS 15454 Procedure Guide*.

Step 3 If the alarm is raised on a DS1/E1-56 card, verify that the card is placed in the correct service mode by completing the following steps:

a. Double-click the card to open the card view.

b. Click the **Provisioning > Card** tabs.

c. Verify that the **Operating Mode** column says All DS1 for your errored circuit.

Step 4 For any other DS-1 or DS-3 card, consult site records to determine whether the port raising the alarm has been assigned.

Step 5 If the port is not currently assigned, place the port out of service using the following steps:

a. Double-click the card to open the card view.

b. For a DS-1 card, click the **Maintenance > Loopback** tabs. For a DS-1 line on a DS3XM-6 or DS3XM-12 card, click the **Maintenance > DS1** tabs.

c. Under Admin State, click **OOS,DSBLD**.

d. Click **Apply**.

Step 6 For any card, if the port is assigned, verify that the correct one is in service:

a. To confirm this physically, confirm that the LED is correctly illuminated on the physical card.

A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

b. To determine this virtually, double-click the card in CTC to open the card view and complete the following substeps:

- Click the **Provisioning > Line** tabs.
- Verify that the Admin State column lists the port as IS.
- If the Admin State column lists the port as OOS,MT or OOS,DSBLD, click the column and choose **IS**. Click **Apply**.

Step 7 Use a test set to confirm that a valid signal exists on the line. Test the line as close to the receiving card as possible. For specific procedures to use the test set equipment, consult the manufacturer.

Step 8 Ensure that the transmit and receive outputs from the DSx patch panel to your equipment are properly connected. For more information about cable connections and terminations, refer to the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15454 Procedure Guide*.

Step 9 If there is a valid signal but the alarm does not clear, replace the electrical connector on the ONS 15454.

Step 10 If a valid electrical signal is not present and the transmitting device is operational, replace the fiber cable connecting the transmitting device to the Ethernet port. To do this, refer to the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15454 Procedure Guide*.

Step 11 Repeat Steps 1 to 10 for any other port on the card that reports the LOS.

Step 12 If the alarm does not clear, check for any card-level alarm that could affect this port.

Step 13 If the alarm does not clear, complete the "Physically Replace a Traffic Card" procedure on page 2-243 for the reporting card.

Step 14 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.

2.8.192 LOS (DS3)

Default Severity: Critical (CR), Service-Affecting (SA)

SONET Logical Object: DS3

The LOS (DS3) for a DS-3 port occurs when the port on a DS3XM-6, DS3XM-12, or DS3/EC1-48 card is in service but no signal is being received. The alarm is caused by incorrect or dirty cabling, a fiber break, or upstream equipment failure.

Note If a circuit shows a partial status when this alarm is raised, the logical circuit is in place. The circuit is able to carry traffic when the connection issue is resolved. You do not need to delete the circuit when troubleshooting this alarm.

Clear the LOS (DS3) Alarm

Step 1 Check for any upstream failures in the transmitting equipment.

Step 2 Verify that the cable is properly connected from the transmitting port and attached to the correct receiving port at the node with the LOS. For more information about fiber connections and terminations, refer to the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15454 Procedure Guide*.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 3 Clean the cable ends using site practices or, if none exists, complete the procedure in the "Maintain the Node" chapter in the *Cisco ONS 15454 Procedure Guide*.

Step 4 Consult site records to determine whether the port raising the alarm has been assigned.

Step 5 If the port is not currently assigned, place the port out of service using the following steps:

a. Double-click the card to open the card view.

b. Click the **Maintenance > DS3** tabs.

c. Under Admin State, click **OOS,DSBLD**.

d. Click **Apply**.

Step 6 If the port is assigned, verify that the correct one is in service:

a. To confirm this physically, confirm that the LED is correctly illuminated on the physical card.

   A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

b. To determine this virtually, double-click the card in CTC to open the card view and complete the following substeps:

   - Click the **Provisioning > Line** tabs.
   - Verify that the Admin State column lists the port as IS.
   - If the Admin State column lists the port as OOS,MT or OOS,DSBLD, click the column and choose **IS**. Click **Apply**.

Step 7 Use a test set to confirm that a valid signal exists on the line. Test the line as close to the receiving card as possible. (For specific procedures to use the test set equipment, consult the manufacturer.)

Step 8 Ensure that the transmit and receive outputs from the DSx patch panel to your equipment are properly connected. For more information about cable connections and terminations, refer to the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15454 Procedure Guide*.

Step 9 If there is a valid signal but the alarm does not clear, replace the electrical connector on the ONS 15454.

Step 10 If the test set shows signal errors but the cabling is correctly installed and the transmitting device is operational, the existing cabling could still be faulty. Use the test set to locate the bad cable and replace it. To do this, refer to the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15454 Procedure Guide*.

Step 11 Repeat Steps 1 to 10 for any other port on the card that reports the LOS.

Step 12 If the alarm does not clear, complete the "Physically Replace a Traffic Card" procedure on page 2-243 for the reporting card.

Step 13 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

2.8.193 LOS (E1)

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Object: E1

An LOS (E1) alarm for a DS1/E1-56 card port occurs when the card is placed in All E1 mode and is in service, but the alarmed port is not receiving a signal due to a physical or provisioning problem. The physical causes for the alarm could be incorrectly connected or faulty cabling. The software causes could be improperly configured card or circuit size.

For more information about the DS1/E1-56 card, refer to the "Electrical Cards" chapter in the *Cisco ONS 15454 Reference Manual*.

Clear the LOS (E1) Alarm

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 1 Verify that the cable is properly connected and attached to the correct port. For more information about connecting cable, refer to the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15454 Procedure Guide*. Also refer to site records for your specific cabling scheme.

Step 2 Ensure that the transmit and receive outputs from the patch panel to your equipment are properly connected. For more information about cable connections and terminations, refer to the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15454 Procedure Guide*.

Step 3 Clean the cable using your site practices. If none exists, complete the procedure in the "Maintain the Node" chapter in the *Cisco ONS 15454 Procedure Guide*.

Step 4 Confirm that the card is properly provisioned to carry the E1 payload:

a. Double-click the card to open the card view.

b. Click the **Provisioning > Card** tabs.

c. Under the **Operating Mode** column, you should see "All E1." If you see "All DS1," click the drop-down to change it and click **Apply**.

Step 5 Use a test set to confirm that a valid E1 signal exists on the line. Test the line as close to the receiving card as possible. (For specific procedures to use the test set equipment, consult the manufacturer.) If the test set shows errors, the cabling could still be faulty despite being correctly installed. Use the tester to isolate the bad section of cable and replace it. Refer to the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15454 Procedure Guide* for procedures.

Step 6 Repeat Steps 1 to 5 for any other port on the card that reports the LOS (E1).

Step 7 If the alarm does not clear, look for any card-level alarm that could cause this alarm.

Step 8 If the alarm does not clear, complete the "Physically Replace a Traffic Card" procedure on page 2-243 for the reporting card.

Step 9 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

2.8.194 LOS (EC1)

Default Severity: Critical (CR), Service-Affecting (SA)

SONET Logical Object: EC1

LOS on an EC1/EC1-12 or DS3/EC1-48 port occurs when a SONET receiver detects an all-zero pattern for 10 microseconds or longer. An LOS (EC1) most likely means that the upstream transmitter has failed. If an EC1 LOS alarm is not accompanied by additional alarms, a cabling problem (such as an incorrect attachment, fiber cut, or other fiber error) usually causes this alarm. The condition clears when the problem is corrected, allowing two consecutive valid frames to be received.

Note If a circuit shows a partial status when this alarm is raised, the logical circuit is in place. The circuit is able to carry traffic when the connection issue is resolved. You do not need to delete the circuit when troubleshooting this alarm.

Clear the LOS (EC1) Alarm

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 1 Check for any upstream equipment failures that could cause the LOS (EC1) in this node.

Step 2 If there is no cause upstream, verify cabling continuity from the transmitting port to the receiving port reporting LOS (EC1) To verify cable continuity, follow site practices.

If the continuity is good, clean the fiber according to site practice. If none exists, complete the procedure in the "Maintain the Node" chapter in the *Cisco ONS 15454 Procedure Guide*.

Step 3 If the cabling is good, verify that the correct EC1-12 port is in service:

a. Confirm that the LED is correctly lit on the physical card.

A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

b. To determine whether the port is in service, double-click the card in CTC to open the card view.

c. Click the **Provisioning > Line** tabs.

d. Verify that the Admin State column lists the port as IS.

e. If the Admin State column lists the port as OOS,MT or OOS,DSBLD, click the column and choose **IS**. Click **Apply**.

Step 4 If the correct port is in service, use an optical test set to confirm that a valid signal exists on the line. For specific procedures to use the test set equipment, consult the manufacturer. Test the line as close to the receiving card as possible.

Step 5 If the signal is valid, ensure that the transmit and receive outputs from the patch panel to your equipment are properly connected. For more information about fiber connections and terminations, refer to the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15454 Procedure Guide*.

Step 6 If a valid signal exists but the alarm does not clear, replace the cable connector on the ONS 15454.

Step 7 Repeat Steps 2 through 6 for any other port on the card that reports the LOS (EC1).

Step 8 If the alarm does not clear, the cabling could still be faulty despite correct attachments. Use the test set to locate the bad cable and replace it using the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15454 Procedure Guide*.

Step 9 If the alarm does not clear, look for any card-level alarm that could cause this port alarm.

Step 10 If the alarm does not clear, complete the "Physically Replace a Traffic Card" procedure on page 2-243 for the reporting card.

Step 11 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

2.8.195 LOS (ESCON)

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.196 LOS (FUDC)

Default Severity: Minor (MN), Non-Service Affecting (NSA)

SONET Logical Object: FUDC

The LOS (FUDC) alarm is raised if there is a UDC circuit created on an AIC-I UDC port but the port is not receiving signal input. The downstream node has an AIS condition raised against the AIC-I port transmitting the UDC. FUDC refers to the 64-kb user data channel using the F1 byte.

Clear the LOS (FUDC) Alarm

Step 1 Verify cable continuity to the AIC-I UDC port. To verify cable continuity, follow site practices.

Step 2 Verify that there is a valid input signal using a test set. For specific procedures to use the test set equipment, consult the manufacturer.

Step 3 If there is a valid signal, clean the fiber according to site practice. If no site practice exists, complete the procedure in the "Maintain the Node" chapter in the *Cisco ONS 15454 Procedure Guide*.

Step 4 If the alarm does not clear, verify that the UDC is provisioned:

a. At the network view, click the **Provisioning > Overhead Circuits** tabs.

b. If no UDC circuit exists, create one. Refer to the "Create Circuits and VT Tunnels" chapter in the *Cisco ONS 15454 Procedure Guide.*

c. If a user data circuit exists (shown as User Data F1 under the Type column), check the source and destination ports. These must be located on AIC-I cards to function.

Step 5 If the alarm does not clear, look for and troubleshoot any other alarm that could identify the source of the problem.

Step 6 If no other alarms exist that could be the source of the LOS (FUDC), or if clearing another alarm did not clear the LOS, complete the "Physically Replace a Traffic Card" procedure on page 2-243 for the reporting card.

Step 7 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.197 LOS (ISC)

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.198 LOS (MSUDC)

The LOS (MSUDC) alarm is not used in this platform in this release. It is reserved for future development.

2.8.199 LOS (OCN)

Default Severity: Critical (CR), Service-Affecting (SA)

SONET Logical Object: OCN

An LOS alarm on an OC-N port occurs when a SONET receiver detects an all-zero pattern for 10 microseconds or longer. An LOS alarm means the upstream transmitter has failed. If an OC-N LOS alarm is not accompanied by additional alarms, a fiber break is usually the cause of the alarm. It clears when two consecutive valid frames are received.

Warning **On the OC-192 card, the laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. The laser is off when the safety key is off (labeled 0).** Statement 293

Warning **Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard.** Statement 1056

Warning **Use of controls, adjustments, or performing procedures other than those specified could result in hazardous radiation exposure.** Statement 1057

Note If a circuit shows a partial status when this alarm is raised, the logical circuit is in place. The circuit is able to carry traffic when the connection issue is resolved. You do not need to delete the circuit when troubleshooting this alarm.

Clear the LOS (OCN) Alarm

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 1 Using site practices, verify fiber continuity to the port.

Step 2 If the cabling is good, verify that the correct port is in service:

a. Confirm that the LED is correctly illuminated on the physical card.

   A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

b. To determine whether the OC-N port is in service, double-click the card in CTC to open the card view.

c. Click the **Provisioning > Line** tabs.

d. Verify that the Admin State column lists the port as IS.

e. If the Admin State column lists the port as OOS,MT or OOS,DSBLD, click the column and choose **IS**.

f. Click **Apply**.

Step 3 If the correct port is in service, clean the fiber according to site practice. If no site practice exists, complete the procedure in the "Maintain the Node" chapter of the *Cisco ONS 15454 Procedure Guide*.

Step 4 Check the incoming optical power through CTC (if available) or with an optical power meter to ensure that it at the correct level as determined by Cisco MetroPlanner.

Step 5 If the alarm does not clear, verify that the power level of the optical signal is within the OC-N card receiver specifications. The "1.14.3 OC-N Card Transmit and Receive Levels" section on page 1-154 lists these specifications for each OC-N card. For DWDM cards, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide* for levels.

Step 6 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 7 If a valid signal exists, replace the connector on the backplane.

Step 8 Repeat Steps 1 to 7 for any other port on the card reporting the LOS (OC-N).

Step 9 If the alarm does not clear, look for and troubleshoot any other alarm that could identify the source of the problem.

Step 10 If no other alarms exist that could be the source of the LOS, or if clearing an alarm did not clear the LOS, complete the "Physically Replace a Traffic Card" procedure on page 2-243 for the reporting card.

Step 11 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

2.8.200 LOS (OTS)

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.201 LOS (TRUNK)

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.202 LOS-O

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.203 LOS-P

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.204 LO-TXPOWER

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Objects: EQPT, OCN

DWDM Logical Objects: 2R, ESCON, FC, GE, ISC, PPM, TRUNK

The Equipment Low Transmit Power alarm is an indicator for the TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, MXP_2.5G_10G and OC192-XFP card transmitted optical signal power. LO-TXPOWER occurs when the measured optical power of the transmitted signal falls under the threshold. The threshold value is user-provisionable.

Note For more information about provisioning MXP or TXP PPMs, refer to the "Provision Transponder and Muxponder Cards" chapter of the *Cisco ONS 15454 DWDM Installation and Operations Guide*. For more information about the cards themselves, refer to the "Card Reference" chapter.

Clear the LO-TXPOWER Alarm

Step 1 Display the TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, MXP_2.5G_10G, or OC192-XFP card view.

Step 2 Click the **Provisioning > Optics Thresholds > Current Values** tabs.

Step 3 Increase the TX Power Low column value by 0.5 dBm.

Step 4 If the card transmit power setting cannot be increased without affecting the signal, complete the "Physically Replace a Traffic Card" procedure on page 2-243.

Step 5 If no ports are shown bad and the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.205 LPBKCRS

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: STSMON, STSTRM

The Loopback Cross-Connect condition indicates that there is a software cross-connect loopback active between an optical card and an OC-192 card. A cross-connect loopback test occurs below line speed and does not affect traffic.

For more information on loopbacks, see the "1.5 Troubleshooting Optical Circuit Paths With Loopbacks" section on page 1-48.

Note Cross-connect loopbacks occur below line speed. They do not affect traffic.

Clear the LPBKCRS Condition

Step 1 To remove the loopback cross-connect condition, double-click the optical card in CTC to open the card view.

Step 2 Complete the "Clear an OC-N Card Cross-Connect (XC) Loopback Circuit" procedure on page 2-245.

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).

2.8.206 LPBKDS1FEAC-CMD

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: DS1, E1

The DS-1 Loopback Command Sent To Far End condition occurs on the near-end node when you send a DS-1 FEAC loopback on DS3XM-6, DS3XM-12, or DS3/EC1-48 cards. For more information about FEAC loopbacks, see the "1.3 Troubleshooting DS3XM-6 or DS3XM-12 Card Electrical Paths With FEAC Loopbacks" section on page 1-46.

Note LPBKDS1FEAC-CMD is an informational condition and does not require troubleshooting.

Caution CTC permits loopbacks on an in-service (IS) circuit. Loopbacks are Service-Affecting (SA).

2.8.207 LPBKDS3FEAC

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: DS3

A Loopback Due to FEAC Command DS-3 condition occurs when a DS3XM-6, DS3XM-12, DS3-12E, or DS3/EC1-48 port loopback signal is received in C-bit framing mode from the far-end node because of an FEAC command. An FEAC command is often used with loopbacks. LPBKDS3FEAC is only reported by these DS cards. DS3XM-6, DS3XM-12, and DS3/EC1-48 cards generate and report FEAC alarms or conditions, but a DS3-12E card only reports FEAC alarms or conditions.

Caution CTC permits loopbacks on an in-service (IS) circuit. Loopbacks are Service-Affecting (SA).

Note LPBKDS3FEAC is an informational condition and does not require troubleshooting.

Clear the LPBKDS3FEAC Condition

Step 1 In node view, double-click the DS-3 card to open the card view.

Step 2 Click the **Maintenance > DS3** tabs.

Step 3 Click the cell for the port in the Send Code column and click **No Code** from the drop-down list.

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).

2.8.208 LPBKDS3FEAC-CMD

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: DS3

The DS-3 Loopback Command Sent To Far End condition occurs on the near-end node when you send a DS-3 FEAC loopback on DS3XM-6, DS3XM-12, or DS3/EC1-48 cards. For more information about FEAC loopbacks, see the "1.3 Troubleshooting DS3XM-6 or DS3XM-12 Card Electrical Paths With FEAC Loopbacks" section on page 1-46.

Note LPBKDS3FEAC-CMD is an informational condition and does not require troubleshooting.

2.8.209 LPBKFACILITY (CE100T)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: CE100T

A Loopback Facility condition on a CE-100T-8 port occurs when a software facility (line) loopback is active for a port on the card.

Note For information about troubleshooting Ethernet circuits with loopbacks, refer to the "1.6 Troubleshooting Ethernet Circuit Paths With Loopbacks" section on page 1-71.

Note For more information about Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.

Clear the LPBKFACILITY (CE100T) Condition

Step 1 Complete the "Clear Other Electrical Card, CE-100T-8, or Ethernet Card Loopbacks" procedure on page 2-246.

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).

2.8.210 LPBKFACILITY (DS1, DS3)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: DS1, DS3

A Loopback Facility condition on a DS-1 or DS-3 port occurs when a software facility (line) loopback is active for the reporting DS3XM-6 card, DS3XM-12 card, a DS1/E1-56 card operating in All DS1 mode, or a DS3/EC1-48 card.

For information about troubleshooting electrical circuits with loopbacks, refer to the "1.2 Troubleshooting Electrical Circuit Paths With Loopbacks" section on page 1-9.

Note CTC permits loopbacks to be performed on an in-service (IS) circuit. Performing a loopback is Service-Affecting (SA). If you did not perform a lockout or Force switch to protect traffic, the LPBKFACILITY condition can be accompanied by a more serious alarms such as LOS.

Note ONS 15454 DS-3 terminal (inward) loopbacks do not transmit an AIS in the direction away from the loopback. Instead of AIS, a continuance of the signal transmitted into the loopback is provided. A DS3/EC1-48 card can be provisioned to transmit AIS for a terminal loopback if desired.

Clear the LPBKFACILITY (DS1, DS3) Condition

Step 1 Complete the "Clear a DS3XM-6, DS3XM-12, or DS3E-12 Card Loopback Circuit" procedure on page 2-246.

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).

2.8.211 LPBKFACILITY (E1)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: E1

A Loopback Facility on an E1 port condition occurs when a software facility (line) loopback is active for a DS1/E1-56 card port operating in All E1 mode.

For information about troubleshooting electrical circuits with loopbacks, refer to the "1.2 Troubleshooting Electrical Circuit Paths With Loopbacks" section on page 1-9.

Note CTC permits loopbacks to be performed on an in-service (IS) circuit. Performing a loopback is Service-Affecting (SA). If you did not perform a lockout or Force switch to protect traffic, the LPBKFACILITY condition can be accompanied by a more serious alarms such as LOS.

Note E1 facility (line) loopbacks transmit an AIS in the direction away from the loopback, but this is provisionable.

Clear the LPBKFACILITY (E1) Condition

Step 1 Complete the "Clear Other Electrical Card, CE-100T-8, or Ethernet Card Loopbacks" procedure on page 2-246.

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).

2.8.212 LPBKFACILITY (EC1)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: EC1

A Loopback Facility condition on an EC-1 port occurs when a software facility (line) loopback is active for a port on the reporting EC1/EC1-12 or DS3/EC1-48 card.

For information about troubleshooting electrical circuits with loopbacks, refer to the "1.2 Troubleshooting Electrical Circuit Paths With Loopbacks" section on page 1-9.

Caution CTC permits loopbacks on an in-service (IS) circuit. Loopbacks are Service-Affecting (SA).

Clear the LPBKFACILITY (EC1) Condition

Step 1 Complete the "Clear Other Electrical Card, CE-100T-8, or Ethernet Card Loopbacks" procedure on page 2-246.

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).

2.8.213 LPBKFACILITY (ESCON)

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.214 LPBKFACILITY (FC)

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.215 LPBKFACILITY (FCMR)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: FCMR

A Loopback Facility for FC_MR condition occurs when a facility loopback is provisioned on an FC_MR-4 card.

For information about troubleshooting these circuits with loopbacks, refer to the "1.7 Troubleshooting MXP, TXP, or FC_MR-4 Circuit Paths With Loopbacks" section on page 1-90.

Clear the LPBKFACILITY (FCMR) Condition

Step 1 Complete the "Clear an MXP, TXP, or FC_MR-4 Card Loopback Circuit" procedure on page 2-246.

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).

2.8.216 LPBKFACILITY (G1000)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: G1000

A Loopback Facility condition for the G1000 object occurs when a software facility (line) loopback is active for a port on the reporting G-Series Ethernet card.

For information about troubleshooting Ethernet circuits with loopbacks, refer to the "1.6 Troubleshooting Ethernet Circuit Paths With Loopbacks" section on page 1-71.

Caution CTC permits loopbacks on an in-service (IS) circuit. Loopbacks are Service-Affecting (SA).

Note For more information about Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.

Clear the LPBKFACILITY (G1000) Condition

Step 1 Complete the "Clear Other Electrical Card, CE-100T-8, or Ethernet Card Loopbacks" procedure on page 2-246.

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).

2.8.217 LPBKFACILITY (GE)

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.218 LPBKFACILITY (ISC)

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.219 LPBKFACILITY (OCN)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: OCN

A Loopback Facility condition for OC-N occurs when a software facility (line) loopback is active for a port on the reporting OC-N card.

For information about troubleshooting optical circuits with loopbacks, refer to the "1.5 Troubleshooting Optical Circuit Paths With Loopbacks" section on page 1-48.

Note OC-3 facility loopbacks do not transmit an AIS in the direction away from the loopback. Instead of AIS, a continuance of the signal transmitted to the loopback is provided.

Caution CTC permits loopbacks on an in-service (IS) circuit. Loopbacks are Service-Affecting (SA).

Caution Before performing a facility (line) loopback on an OC-N card, ensure that the card contains at least two DCC paths to the node where the card is installed. A second 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 DCC is not necessary if you are directly connected to the ONS 15454 containing the loopback OC-N.

Clear the LPBKFACILITY (OCN) Condition

Step 1 Complete the "Clear an OC-N Card Facility or Terminal Loopback Circuit" procedure on page 2-245.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.220 LPBKFACILITY (TRUNK)

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.221 LPBKTERMINAL (CE100T)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: CE100T

A Loopback Terminal condition on a CE-100T-8 port occurs when a software terminal loopback is active for a port on the card.

Note For information about troubleshooting Ethernet circuits with loopbacks, refer to the "1.6 Troubleshooting Ethernet Circuit Paths With Loopbacks" section on page 1-71.

Note For more information about Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.*

Clear the LPBKTERMINAL (CE100T) Condition

Step 1 Complete the "Clear Other Electrical Card, CE-100T-8, or Ethernet Card Loopbacks" procedure on page 2-246.

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).

2.8.222 LPBKTERMINAL (DS1, DS3)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: DS1, DS3

A Loopback Terminal condition for a DS-1 or DS-3 occurs when a software terminal (inward) loopback is active for a DS1 or DS3 port on the reporting DS3XM-6, DS3XM-12, or DS3/EC1-48 card. DS-1 and DS-3 terminal loopbacks do not typically return an AIS signal, but you can provision one for the DS3/EC1-48 card.

For information about troubleshooting electrical circuits with loopbacks, refer to the "1.3 Troubleshooting DS3XM-6 or DS3XM-12 Card Electrical Paths With FEAC Loopbacks" section on page 1-46.

Clear the LPBKTERMINAL (DS1, DS3) Condition

Step 1 Complete the "Clear a DS3XM-6, DS3XM-12, or DS3E-12 Card Loopback Circuit" procedure on page 2-246.

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).

2.8.223 LPBKTERMINAL (E1)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: E1

A Loopback Terminal condition for an E-1 signal on a DS1/E1-56 card occurs when the card is operating in All E1 mode and a software terminal (inward) loopback is active for a port.

For information about troubleshooting electrical circuits with loopbacks, refer to the "1.3 Troubleshooting DS3XM-6 or DS3XM-12 Card Electrical Paths With FEAC Loopbacks" section on page 1-46.

Clear the LPBKTERMINAL (E1) Condition

Step 1 Complete the "Clear Other Electrical Card, CE-100T-8, or Ethernet Card Loopbacks" procedure on page 2-246.

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).

2.8.224 LPBKTERMINAL (EC1)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: EC1

A Loopback Terminal condition on an EC-1 signal occurs when a software terminal (inward) loopback is active for a port on the reporting EC1/EC1-12 or DS3/EC1-48 card.

For information about troubleshooting electrical circuits with loopbacks, refer to the "1.2 Troubleshooting Electrical Circuit Paths With Loopbacks" section on page 1-9.

Caution CTC permits loopbacks on an in-service (IS) circuit. Loopbacks are Service-Affecting (SA).

Clear the LPBKTERMINAL (EC1) Condition

Step 1 Complete the "Clear Other Electrical Card, CE-100T-8, or Ethernet Card Loopbacks" procedure on page 2-246.

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).

2.8.225 LPBKTERMINAL (ESCON)

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.226 LPBKTERMINAL (FC)

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.227 LPBKTERMINAL (FCMR)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: FCMR

A Loopback Terminal for FCMR condition occurs when a terminal loopback is provisioned on an FC_MR-4 card.

For information about troubleshooting these circuits with loopbacks, refer to the "1.7 Troubleshooting MXP, TXP, or FC_MR-4 Circuit Paths With Loopbacks" section on page 1-90.

Clear the LPBKTERMINAL (FCMR) Condition

Step 1 Complete the "Clear an MXP, TXP, or FC_MR-4 Card Loopback Circuit" procedure on page 2-246.

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).

2.8.228 LPBKTERMINAL (G1000)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: G1000

A Loopback Terminal condition for the G1000 occurs when a software terminal (inward) loopback is active for a port on the reporting G-Series Ethernet card.

When a port in terminal (inward) loopback, its outgoing signal is redirected into the receive direction on the same port, and the externally received signal is ignored. On the G1000-4 card, the outgoing signal is not transmitted; it is only redirected in the receive direction.

For more information about troubleshooting Ethernet circuits, refer to the "1.6 Troubleshooting Ethernet Circuit Paths With Loopbacks" section on page 1-71.

Caution CTC permits loopbacks on an in-service (IS) circuit. Loopbacks are Service-Affecting (SA).

Note For more information about Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.

Clear the LPBKTERMINAL (G1000) Condition

Step 1 Complete the "Clear Other Electrical Card, CE-100T-8, or Ethernet Card Loopbacks" procedure on page 2-246.

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).

2.8.229 LPBKTERMINAL (GE)

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.230 LPBKTERMINAL (ISC)

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.231 LPBKTERMINAL (OCN)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: OCN

A Loopback Terminal condition for OC-N occurs when a software terminal (inward) loopback is active for a port on the reporting card.

Note OC-N terminal loopbacks do not typically return an AIS.

Note Performing a loopback on an in-service circuit is Service-Affecting (SA). If you did not perform a lockout or Force switch to protect traffic, the LPBKTERMINAL condition can also be accompanied by a more serious alarm such as LOS.

For information about troubleshooting circuits, refer to the loopback procedures in Chapter 1, "General Troubleshooting."

Clear the LPBKTERMINAL (OCN) Condition

Step 1 Complete the "Clear an OC-N Card Facility or Terminal Loopback Circuit" procedure on page 2-245.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.232 LPBKTERMINAL (TRUNK)

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.233 LWBATVG

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Object: PWR

The Low Voltage Battery alarm occurs in a –48 VDC environment when a battery lead input voltage falls below the low power threshold. This threshold, with a default value of –44 VDC, is user-provisionable. The alarm remains raised until the voltage remains above the threshold for 120 seconds. (For information about changing this threshold, refer to the "Turn Up Node" chapter in the *Cisco ONS 15454 Procedure Guide*.

Clear the LWBATVG Alarm

Step 1 The problem is external to the ONS 15454. 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.

2.8.234 MAN-REQ

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: EQPT, STSMON, VT-MON

The Manual Switch Request condition occurs when a user initiates a Manual switch request on an OC-N port. Clearing the Manual switch clears the MAN-REQ condition. You do not need to clear the switch if you want the Manual switch to remain.

Clear the MAN-REQ Condition

Step 1 Complete the "Initiate a 1+1 Manual Switch Command" procedure on page 2-232.

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).

2.8.235 MANRESET

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: EQPT

A User-Initiated Manual Reset condition occurs when you right-click a card in CTC and choose Reset. Resets performed during a software upgrade also prompt the condition. The MANRESET condition clears automatically when the card finishes resetting.

Note MANRESET is an informational condition and does not require troubleshooting.

2.8.236 MANSWTOINT

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: NE-SREF

The Manual Switch To Internal Clock condition occurs when the NE timing source is manually switched to an internal timing source.

Note MANSWTOINT is an informational condition and does not require troubleshooting.

2.8.237 MANSWTOPRI

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: EXT-SREF, NE-SREF

The Manual Switch To Primary Reference condition occurs when the NE timing source is manually switched to the primary timing source.

Note MANSWTOPRI is an informational condition and does not require troubleshooting.

2.8.238 MANSWTOSEC

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: EXT-SREF, NE-SREF

The Manual Switch To Second Reference condition occurs when the NE timing source is manually switched to a second timing source.

Note MANSWTOSEC is an informational condition and does not require troubleshooting.

2.8.239 MANSWTOTHIRD

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: EXT-SREF, NE-SREF

The Manual Switch To Third Reference condition occurs when the NE timing source is manually switched to a third timing source.

Note MANSWTOTHIRD is an informational condition and does not require troubleshooting.

2.8.240 MANUAL-REQ-RING

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: OCN

The Manual Switch Request on Ring condition occurs when a user initiates a MANUAL RING command on BLSR rings to switch from working to protect or protect to working. This condition is visible on the network view Alarms, Conditions, and History tabs and is accompanied by WKSWPR. The port where the MANUAL RING command originated is marked with an “M” on the network view detailed circuit map.

Clear the MANUAL-REQ-RING Condition

Step 1 Complete the "Clear a BLSR External Switching Command" procedure on page 2-239.

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).

2.8.241 MANUAL-REQ-SPAN

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: OCN

DWDM Logical Objects: 2R, ESCON, FC, GE, ISC, TRUNK

The Manual Switch Request on Ring condition occurs on BLSRs when a user initiates a Manual Span command to move BLSR 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 BLSR External Switching Command" procedure on page 2-239.

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).

2.8.242 MEA (AIP)

Default Severity: Critical (CR), Service-Affecting (SA)

SONET Logical Object: AIP

If the Mismatch of Equipment Attributes (MEA) alarm is reported against the AIP, the fuse in the AIP board blew or is missing. The MEA alarm also occurs when an old AIP board with a 2-A fuse is installed in a newer ANSI 10-Gbps-compatible shelf assembly (15454-SA-ANSI or 15454-SA-HD).

Clear the MEA (AIP) Alarm

Step 1 Complete the "Replace the Alarm Interface Panel" procedure on page 2-251.

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.

2.8.243 MEA (BIC)

Default Severity: Critical (CR), Service-Affecting (SA)

SONET Logical Object: BIC

The Missing Equipment Attributes alarm for the backplane interface connector (BIC) indicates a compatibility issue in using high-density DS-3 cards with universal backplane interface connectors (UBIC) and an older shelf backplane. Backplane versions 15454-SA-HD and later are compatible with the UBIC with horizontal connectors (UBIC-H) and UBIC with vertical connectors (UBIC-V) that the high-density EC-1, DS-1, and DS-3 electrical connections require. The MEA alarm is raised if you attempt to install a high-density card into Slot 4, 5, 6, 12, 13, or 14 with an older noncompatible backplane installed. The card is not usable in this case. It is also raised if you attempt to use an older BIC with the newer backplane.

Clear the MEA (BIC) Alarm

Step 1 Click the **Provisioning > Inventory** tabs to determine your backplane model. If the backplane is not a 15454-SA-HD, replace the backplane or do not attempt to use high-density DS-3 cards. Table 2-14 lists the BICs that are compatible with various backplanes.

Table 2-14 BIC Compatibility Matrix

BIC Type	Part No.
BICs that work with the current and previous backplane	MANUF_EQPT_ID_BIC_A_SMB_HD_BP MANUF_EQPT_ID_BIC_B_SMB_HD_BP MANUF_EQPT_ID_BIC_A_BNC_24_HD_BP MANUF_EQPT_ID_BIC_A_BNC_48_HD_BP MANUF_EQPT_ID_BIC_B_SMB MANUF_EQPT_ID_BIC_B_SMB_ALT MANUF_EQPT_ID_BIC_B_BNC_24 MANUF_EQPT_ID_BIC_B_BNC_48
New HD BICs that work only with the new backplanes	MANUF_EQPT_ID_BIC_A_UNIV_VERT MANUF_EQPT_ID_BIC_B_UNIV_VERT MANUF_EQPT_ID_BIC_A_UNIV_HORIZ MANUF_EQPT_ID_BIC_B_UNIV_HORIZ MANUF_EQPT_ID_BIC_A_MINI_BNC_HD_BP MANUF_EQPT_ID_BIC_B_MINI_BNC_HD_BP
High-density BICs that work only with 15454-SA-HD	MANUF_EQPT_ID_BIC_A_SMB MANUF_EQPT_ID_BIC_A_SMB_ALT MANUF_EQPT_ID_BIC_A_BNC_24 MANUF_EQPT_ID_BIC_A_BNC_48

Step 2 If you determine that your BIC type and backplane are compatible despite the MEA alarm, or if the alarm does not clear after you resolve the incompatibilities, 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.

2.8.244 MEA (EQPT)

Default Severity: Critical (CR), Service-Affecting (SA)

SONET Logical Object: EQPT

The MEA alarm for equipment is reported against a card slot when the physical card inserted into a slot does not match the card type that is provisioned for that slot in CTC. The alarm also occurs when certain cards introduced in Release 3.1 or later are inserted into an older shelf assembly or when older Ethernet cards (E1000-2 and E100T-12) are used in a newer 10-Gbps-compatible shelf assembly.

Removing the incompatible cards clears the alarm.

Note For more information about Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.

Note If an OC3-8 card is installed in Slot 5 to 6 and Slot 12 to 13, it does not appear in CTC and raises an MEA.

Clear the MEA (EQPT) Alarm

Step 1 Physically verify the type of card that is installed in the slot reporting the MEA alarm. In node view, click the **Inventory** tab and compare it to the actual installed card.

Step 2 Determine whether the ONS 15454 shelf assembly is a newer 10-Gbps-compatible shelf assembly (15454-SA-ANSI or 15454-SA-HD) or an earlier shelf assembly. Under the HW Part # column, if the part number is 800-19857-XX or 800-19856-XX, then you have a 15454-SA-ANSI shelf. If the part number is 800-24848-XX, then you have a 15454-SA-HD shelf. If the number is not one of those listed above, then you are using an earlier shelf assembly.

Note On the 15454-SA-HD (P/N: 800-24848), 15454-SA-NEBS3E, 15454-SA-NEBS3, and 15454-SA-R1 (P/N: 800-07149) shelves, the AIP cover is clear plastic. On the 15454-SA-ANSI shelf (P/N: 800-19857), the AIP cover is metal.

Step 3 Verify the type of card that sits in the slot reported in the object column of the MEA row on the Alarms window by reading the name at the top of the card faceplate.

- If you have a newer 10-Gbps-compatible shelf assembly (15454-SA-ANSI or 15454-SA-HD) and the card reporting the alarm is not an E1000-2 or E100T-12, proceed to Step 4.
- If you have a newer 10-Gbps-compatible shelf assembly (15454-SA-ANSI or 15454-SA-HD) and the card reporting the alarm is an E1000-2 or E100T-12, then that version of the Ethernet card is incompatible and must be removed. Proceed to Step 4.

Note The E1000-2-G and E100T-G cards are compatible with the newer ANSI 10-Gbps-compatible shelf assembly and are the functional equivalent of the older, noncompatible E1000-2 and E100T-12 cards. E1000-2-G and E100T-G cards can be used as replacements for E1000-2 and E100T-12 cards in a 10-Gbps-compatible shelf assembly.

- If you have an older shelf assembly and the card reporting the alarm is not a card introduced in Release 3.1 or later, which includes the OC-192, E1000-2-G, E100T-G, or OC-48 any slot (AS), proceed to Step 4.
- If you have an older shelf assembly and the card reporting the alarm is a card introduced in Release 3.1 or later, which includes the OC-192, E1000-2-G, E100T-G, or OC-48 any slot (AS), the reporting card is incompatible with the shelf assembly and must be removed Proceed to Step 4.

Step 4 If you prefer the card type depicted by CTC, complete the "Physically Replace a Traffic Card" procedure on page 2-243 for the reporting card.

Step 5 If you prefer the card that physically occupies the slot but the card is not in service, does not have circuits mapped to it, and is not part of a protection group, place the cursor over the provisioned card in CTC and right-click to choose **Delete Card**.

The card that physically occupies the slot reboots, and CTC automatically provisions the card type into that slot.

Note If the card is in service, does have circuits mapped to it, is paired in a working protection scheme, has DCC communications turned on, or is used as a timing reference, CTC does not allow you to delete the card.

Step 6 If any ports on the card are in service, place them out of service (OOS,MT):

Caution Before placing ports out of service, ensure that live traffic is not present.

a. Double-click the reporting card to open the card view.
b. Click the **Provisioning** tab.
c. Click the admin state of any in-service ports.
d. Choose **OOS,MT** to take the ports out of service.

Step 7 If a circuit has been mapped to the card, complete the "Delete a Circuit" procedure on page 2-244.

Caution Before deleting the circuit, ensure that live traffic is not present.

Step 8 If the card is paired in a protection scheme, delete the protection group:

a. Click the **Provisioning > Protection** tabs.
b. Choose the protection group of the reporting card.
c. Click **Delete**.

Step 9 Right-click the card reporting the alarm.

Step 10 Choose **Delete**.

The card that physically occupies the slot reboots, and CTC automatically provisions the card type into that slot.

Step 11 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

2.8.245 MEA (FAN)

Default Severity: Critical (CR), Service-Affecting (SA)

SONET Logical Object: FAN

The MEA alarm is reported against the fan-tray assembly when a newer fan-tray assembly (15454-FTA3) with a 5-A fuse is used with an older shelf assembly or when an older fan-tray assembly with a 2-A fuse is used with a newer 10-Gbps-compatible shelf assembly (15454-SA-ANSI or 15454-SA-HD) that contains cards introduced in Release 3.1 or later. If a 10-Gbps-compatible shelf assembly contains only cards introduced before Release 3.1, then an older fan-tray assembly (15454-FTA-2) can be used and does not report an MEA alarm.

Clear the MEA (FAN) Alarm

Step 1 Determine whether the shelf assembly is a newer 10-Gbps-compatible shelf assembly (15454-SA-ANSI or 15454-SA-HD) or an earlier shelf assembly. In node view, click the **Inventory** tab.

Under the HW Part # column, if the part number is 800-19857-XX or 800-19856-XX, then you have a 15454-SA-ANSI shelf. If the part number is 800-24848-XX, you have a 15454-SA-HD shelf.

Under the HW Part # column, if the number is not one of those listed above, then you are using an earlier shelf assembly.

Step 2 If you have a 10-Gbps-compatible shelf assembly (15454-SA-ANSI or 15454-SA-HD), the alarm indicates that an older incompatible fan-tray assembly is installed in the shelf assembly. Obtain a newer fan-tray assembly (15454-FTA3) with a 5-A fuse and complete the "Replace the Fan-Tray Assembly" procedure on page 2-249.

Step 3 If you are using an earlier shelf assembly, the alarm indicates that you are using a newer fan-tray assembly (15454-FTA3), which is incompatible with the earlier version of the shelf assembly. Obtain an earlier version of the fan-tray assembly (15454-FTA2) and complete the "Replace the Fan-Tray Assembly" procedure on page 2-249.

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.

2.8.246 MEA (PPM)

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.247 MEM-GONE

Default Severity: Major (MJ), Non-Service-Affecting (NSA)

SONET Logical Object: EQPT

The Memory Gone alarm occurs when data generated by software operations exceeds the memory capacity of the TCC2/TCC2P. The TCC2/TCC2P cards which exceed the memory capacity reboot to avoid failure of card operations.

Note The alarm does not require user intervention. The MEM-LOW alarm always preceeds the MEM-GONE alarm.

2.8.248 MEM-LOW

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: EQPT

The Free Memory of Card Almost Gone alarm occurs when data generated by software operations is close to exceeding the memory capacity of the TCC2/TCC2P. The alarm clears when additional memory becomes available. If additional memory is not made available and the memory capacity of the card is exceeded, CTC ceases to function.

Note The alarm does not require user intervention. If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.249 MFGMEM

Default Severity: Critical (CR), Service-Affecting (SA)

SONET Logical Objects: AICI-AEP, AICI-AIE, AIP, BPLANE, FAN

DWDM Logical Object: PPM

The Manufacturing Data Memory Failure alarm occurs when the EEPROM fails on a card or component, or when the TCC2/TCC2P cannot read this memory. EEPROM stores manufacturing data that a system TCC2/TCC2P uses to determine system compatibility and shelf inventory status. Unavailability of this information can cause less-significant problems. The AIP EEPROM also stores the system MAC address. If the MFGMEM alarm indicates EEPROM failure on these panels, IP connectivity could be disrupted and the system icon is grayed out in CTC network view.

Tip When you lose LAN connectivity with an ONS 15454 due to an MFGMEM alarm on the AIP, you can reestablish node management by disconnecting the Ethernet cable from the panel and connecting it to the active TCC2/TCC2P LAN port.

Clear the MFGMEM Alarm

Step 1 Complete the "Reset an Active TCC2/TCC2P Card and Activate the Standby Card" procedure on page 2-240.

Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card.

Step 2 If the reset card has not rebooted successfully, or the alarm has not cleared, call Cisco TAC (1 800 553-2447). If the Cisco TAC technician tells you to reseat the card, complete the "Remove and Reinsert (Reseat) the Standby TCC2/TCC2P Card" procedure on page 2-241. If the Cisco TAC technician tells you to remove the card and reinstall a new one, complete the "Physically Replace a Traffic Card" procedure on page 2-243.

Step 3 If the MFGMEM alarm continues to report after replacing the TCC2/TCC2Ps, the problem lies with the EEPROM.

Step 4 If the MFGMEM is reported from the fan-tray assembly, obtain a fan-tray assembly and complete the "Replace the Fan-Tray Assembly" procedure on page 2-249.

Step 5 If the MFGMEM is reported from the AIP, the backplane, or the alarm persists after the fan-tray assembly is replaced, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) to report a Service-Affecting (SA) problem.

2.8.250 NO-CONFIG

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: EQPT

The No Startup Configuration condition applies to ML-Series Ethernet cards and occurs when no startup configuration file has been downloaded to the TCC2/TCC2P, whether or not you preprovision the card slot. This alarm can be expected during provisioning. When the startup configuration file is copied to the active TCC2/TCC2P, the alarm clears.

Note For more information about the ML-Series Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.*

Clear the NO-CONFIG Condition

Step 1 Create a startup configuration for the card in Cisco IOS.

Follow the card provisioning instructions in the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.*

Step 2 Upload the configuration file to the TCC2/TCC2P:

a. In node view, right-click the ML-Series card graphic.

b. Choose **IOS Startup Config** from the shortcut menu.

c. Click **Local > TCC** and navigate to the file location.

Step 3 Complete the "Reset a Traffic Card in CTC" procedure on page 2-239.

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).

2.8.251 NOT-AUTHENTICATED

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: SYSTEM

The NOT-AUTHENTICATED alarm is raised by CTC (not by the NE) when CTC fails to log into a node. This alarm only appears in CTC where the login failure occurred. This alarm differs from the "INTRUSION-PSWD" alarm on page 2-120 because INTRUSION-PSWD occurs when a user exceeds the login failures threshold.

Note NOT-AUTHENTICATED is an informational alarm and is resolved when CTC successfully logs into the node.

2.8.252 OCHNC-INC

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.253 ODUK-1-AIS-PM

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.254 ODUK-2-AIS-PM

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.255 ODUK-3-AIS-PM

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.256 ODUK-4-AIS-PM

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.257 ODUK-AIS-PM

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.258 ODUK-BDI-PM

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.259 ODUK-LCK-PM

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.260 ODUK-OCI-PM

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.261 ODUK-SD-PM

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.262 ODUK-SF-PM

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.263 ODUK-TIM-PM

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.264 OOU-TPT

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: STSTRM, VT-TERM

The Out of Use Transport Failure alarm is a VCAT member alarm. (VCAT member circuits are independent circuits that are concatenated from different time slots into a higher-rate signal.) This condition is raised when a member circuit in a VCAT is unused, such as when it is removed by SW-LCAS. It occurs in conjunction with the "VCG-DEG" condition on page 2-226.

Clear the OOT-TPT Condition

Step 1 Complete the "Clear the VCG-DEG Condition" procedure on page 2-226. Clearing that condition clears this condition as well.

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).

2.8.265 OPEN-SLOT

Default Severity: Not Alarmed (NA)

SONET Logical Object: EQPT

The Open Slot condition indicates that there is an open slot in the system shelf. Slot covers assist with airflow and cooling.

Clear the OPEN-SLOT Condition

Step 1 To install a slot cover and clear this condition, refer to the procedures located in the "Install Hardware" chapter of the *Cisco ONS 15454 Procedure Guide*.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.266 OPTNTWMIS

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.267 OPWR-HDEG

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.268 OPWR-HFAIL

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.269 OPWR-LDEG

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.270 OPWR-LFAIL

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.271 OSRION

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.272 OTUK-AIS

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.273 OTUK-BDI

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.274 OTUK-IAE

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.275 OTUK-LOF

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.276 OTUK-SD

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.277 OTUK-SF

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.278 OTUK-TIM

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.279 OUT-OF-SYNC

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.280 PARAM-MISM

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.281 PDI-P

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: STSMON, STSTRM

PDI-P is a set of application-specific codes indicating a signal label mismatch failure (SLMF) in the ONS 15454 STS path overhead. The condition indicates to downstream equipment that there is a defect in one or more of the directly mapped payloads contained in that STS synchronous payload envelope (SPE). For example, the mismatch could occur in the overhead to the path selector in a downstream node configured as part of a path protection. The PDI-P codes appear in the STS Signal Label (C2 byte).

An SLMF often occurs when the payload (for example, ATM) does not match what the signal label is reporting. The "AIS" condition on page 2-32 often accompanies a PDI-P condition. If the PDI-P is the only condition reported with the AIS, clearing PDI-P clears the AIS. PDI-P can also occur during an upgrade, but usually clears itself and is not a valid condition.

A PDI-P condition reported on an OC-N port supporting a G1000-4 card circuit could result from the end-to-end Ethernet link integrity feature of the G1000-4 card. If the link integrity is the cause of the path defect, it is typically accompanied by the "TPTFAIL (G1000)" alarm on page 2-219 or the "CARLOSS (G1000)" alarm on page 2-56 reported against one or both Ethernet ports terminating the circuit. If this is the case, clear the TPTFAIL and CARLOSS alarms to resolve the PDI-P condition.

A PDI-P condition reported on an OC-N port supporting an ML-Series card circuit could result from the end-to-end Ethernet link integrity feature of the ML-Series card. If the link integrity is the cause, it is typically accompanied by the "TPTFAIL (ML100T, ML1000, MLFX)" alarm on page 2-220 reported against one or both packet-over-SONET (POS) ports terminating the circuit. If TPTFAIL is reported against one or both of the POS ports, troubleshooting the accompanying alarm clears the PDI-P condition. Refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327* for more information about ML-Series cards.

Warning **On the OC-192 card, the laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. The laser is off when the safety key is off (labeled 0).** Statement 293

Warning **Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard.** Statement 1056

Warning **Use of controls, adjustments, or performing procedures other than those specified could result in hazardous radiation exposure.** Statement 1057

Note For more information about Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.

Clear the PDI-P Condition

Step 1 Verify that all circuits terminating in the reporting card are DISCOVERED:

a. Click the **Circuits** tab.

b. Verify that the **Status** column lists the circuit as active.

c. If the Status column lists the circuit as PARTIAL, wait 10 minutes for the ONS 15454 to initialize fully. If the PARTIAL status does not change after full initialization, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC to report a Service-Affecting (SA) problem (1 800 553-2447).

Step 2 After determining that the circuit is DISCOVERED, ensure that the signal source to the card reporting the alarm is working.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 3 If traffic is affected, complete the "Delete a Circuit" procedure on page 2-244.

Caution Deleting a circuit can affect existing traffic.

Step 4 Recreate the circuit with the correct circuit size. Refer to the "Create Circuits and VT Tunnels" chapter in the *Cisco ONS 15454 Procedure Guide* for detailed procedures to create circuits.

Step 5 If circuit deletion and re-creation does not clear the condition, verify that there is no problem stemming from the far-end OC-N card providing STS payload to the reporting card.

Step 6 If the condition does not clear, confirm the cross-connect between the OC-N card and the reporting card.

Step 7 If the condition does not clear, clean the far-end optical fiber according to site practice. If no site practice exists, complete the procedure in the "Maintain the Node" chapter of the *Cisco ONS 15454 Procedure Guide*.

Step 8 If the condition does not clear, complete the "Physically Replace a Traffic Card" procedure on page 2-243 for the optical/electrical cards.

Step 9 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.282 PEER-NORESPONSE

Default Severity: Major (MJ), Non-Service-Affecting (NSA)

SONET Logical Object: EQPT

The switch agent raises a Peer Card Not Responding alarm if either traffic card in a protection group does not receive a response to the peer status request message. PEER-NORESPONSE is a software failure and occurs at the task level, as opposed to a communication failure, which is a hardware failure between peer cards.

Clear the PEER-NORESPONSE Alarm

Step 1 Complete the "Reset a Traffic Card in CTC" procedure on page 2-239 for the reporting card. For the LED behavior, see the "2.9.2 Typical Traffic Card LED Activity During Reset" section on page 2-229.

Step 2 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. Verify the LED appearance: A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

Step 3 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.283 PLM-P

Default Severity: Critical (CR), Service-Affecting (SA)

SONET Logical Objects: STSMON, STSTRM

A Payload Label Mismatch Path alarm indicates that signal does not match its label. The condition is indicated by a problematic C2 byte value in the SONET path overhead. The alarm is raised if all of the following conditions are met:

- The received C2 byte is not 0x00 (unequipped).
- The received C2 byte is not a PDI value.
- The received C2 does not match the expected C2.
- The expected C2 byte is not 0x01 (equipped, unspecified).
- The received C2 byte is not 0x01 (equipped, unspecified).

For example, on nodes equipped with CTC Software R4.1 and earlier, this alarm could occur when you have a DS3XM-6 card connected to a DS-3 card instead of a DS-1 card. The DS3XM-6 card expects a C2 label byte value of 01. A DS-1 card transmits this value, but a DS-3 card transmits a value of 04. The mismatch between the sent and expected values causes the PLM-P alarm.

Warning **On the OC-192 card, the laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. The laser is off when the safety key is off (labeled 0).** Statement 293.

Warning **Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard.** Statement 1056

Warning **Use of controls, adjustments, or performing procedures other than those specified could result in hazardous radiation exposure.** Statement 1057

Clear the PLM-P Alarm

Step 1 Complete the "Clear the PDI-P Condition" procedure on page 2-175.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. 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, 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.

2.8.284 PLM-V

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Object: VT-TERM

A Payload Label Mismatch VT Layer alarm indicates that the content of the V5 byte in the SONET overhead is inconsistent or invalid. PLM-V occurs when ONS 15454s interoperate with equipment that performs bit-synchronous mapping for DS-1 signal. The ONS 15454 uses asynchronous mapping.

Clear the PLM-V Alarm

Step 1 Verify that your signal source matches the signal allowed by the traffic card. For example, the traffic card does not allow VT6 or VT9 mapping.

Step 2 If the signal source matches the card, verify that the SONET VT path originator is sending the correct VT label value. You can find the SONET VT path originator using circuit provisioning steps.

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.

2.8.285 PORT-ADD-PWR-DEG-HI

For more information about the PORT-ADD-PWR-DEG-HIGH alarm, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide.*

2.8.286 PORT-ADD-PWR-DEG-LOW

For more information about the PORT-ADD-PWR-DEG-HIGH alarm, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide.*

2.8.287 PORT-ADD-PWR-FAIL-HIGH

For more information about the PORT-ADD-PWR-DEG-HIGH alarm, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide.*

2.8.288 PORT-ADD-PWR-FAIL-LOW

For more information about the PORT-ADD-PWR-DEG-HIGH alarm, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide.*

2.8.289 PORT-FAIL

For more information about the PORT-ADD-PWR-DEG-HIGH alarm, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide.*

2.8.290 PORT-MISMATCH

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Objects: CE-MR-10, ML-MR-10, FC_MR-4

The Pluggable PORT-MISMATCH alarm applies to FC_MR-4, ML-MR-10, and CE-MR-10 Ethernet cards.

For the ML-MR-10 and CE-MR-10 cards the alarm indicates either of the following:

- The provisioned payload, speed, or duplex configured on the port does not match that of the SFP plugged into the port.
- A non-supported SFP is plugged into the port.

For the FC_MR-4 card the alarm indicates that a non-supported GBIC is plugged into the port.

Clear the PORT-MISMATCH Alarm

To clear the alarm on the CE-MR-10 card, either plug-in a supported SFP into the CE-MR-10 port or follow these steps to provision the correct payload, speed, or duplex:

1. In node view (single-shelf mode) or shelf view (multishelf mode), double-click the CE-MR-10 card to open the card view.
2. Click the **Provisioning > Ether Ports** tabs.
3. Specify correct values in the Expected Speed and Expected Duplex fields to match the SFP configuration.
4. Click **Apply**.

To clear the alarm on the FC_MR-4 card, plug-in a supported GBIC into the FC_MR-4 port and follow these steps to provision the media type:

1. In node view (single-shelf mode) or shelf view (multishelf mode), double-click the FC_MR-4 card graphic to open the card.
2. Click the **Provisioning > Port > General** tabs.
3. Specify proper payload value in the Media Type field.
4. Click **Apply**.

For the CE-MR-10 and FC_MR-10 card, the alarm can also be cleared using TL1 commands. For detailed instructions, refer to the *Cisco ONS 15454, Cisco ONS 15600, and Cisco ONS 15310-MA SONET TL1 Command Guide.*

For the ML-MR-10 card, the alarm can be cleared through Cisco IOS commands. For detailed instructions, refer to the *Cisco ONS 15454 and Cisco ONS 15454 SDH Ethernet Card Software Feature and Configuration Guide*.

If the alarm does not clear, log into the Cisco Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) to report a Service-Affecting (SA) problem.

2.8.291 PRC-DUPID

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Object: OCN

The Procedural Error Duplicate Node ID alarm indicates that two identical node IDs exist in the same ring. The ONS 15454 requires each node in the ring to have a unique node ID.

Clear the PRC-DUPID Alarm

Step 1 Log into a node on the ring.

Step 2 Find the node ID by completing the "Identify a BLSR Ring Name or Node ID Number" procedure on page 2-230.

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 a BLSR Node ID Number" procedure on page 2-230 so that each node ID is unique.

Step 5 If the alarm does not clear, log into the 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.

2.8.292 PROTNA

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: EQPT

The Protection Unit Not Available alarm is caused by an OOS protection card when a TCC2/TCC2P or XC10G card that has been provisioned as part of a protection group is not available. Unavailable protection can occur when a card is reset, but the alarm clears as soon as the card is back in service. The alarm clears if the device or facility is brought back in service.

Clear the PROTNA Alarm

Step 1 If the PROTNA alarm occurs and does not clear, and if it is raised against a controller or cross-connect card, ensure that there is a redundant TCC2/TCC2P installed and provisioned in the chassis.

Step 2 If the alarm is raised against a line card, verify that the ports have been taken out of service (OOS,MT):

- **a.** In CTC, double-click the reporting card to open the card view (if the card is not an XC10G card).
- **b.** Click the **Provisioning** tab.
- **c.** Click the admin state of any in-service (IS) ports.
- **d.** Choose **OOS,MT** to take the ports out of service.

Step 3 Complete the "Reset a Traffic Card in CTC" procedure on page 2-239 for the reporting card. For the LED behavior, see the "2.9.2 Typical Traffic Card LED Activity During Reset" section on page 2-229.

Step 4 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. Verify the LED appearance: A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

Step 5 If the alarm does not clear, complete the "Remove and Reinsert (Reseat) Any Card" procedure on page 2-242 for the reporting card.

Step 6 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.293 PROV-MISMATCH

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.294 PTIM

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.295 PWR-FAIL-A

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: EQPT

The Equipment Power Failure at Connector A alarm occurs when there is no power supply from the main power connector to the equipment. This alarm occurs on the electrical interface assemblies (EIA), 15454_MRC-12 Multirate card, MRC-2.5G-4 Multirate card, OC192SR1/STM64IO Short Reach and OC192/STM64 Any Reach cards (also known as OC192-XFP in CTC), OC12 IR/STM4 SH 1310-4 card, OC3 IR/STM1 SH 1310-8 card or TCC2/TCC2P.

Warning **The power supply circuitry for the equipment can constitute an energy hazard. Before you install or replace the equipment, remove all jewelry (including rings, necklaces, and watches). Metal objects can come into contact with exposed power supply wiring or circuitry inside the DSLAM equipment. This could cause the metal objects to heat up and cause serious burns or weld the metal object to the equipment.** Statement 207

Clear the PWR-FAIL-A Alarm

Step 1 If a single card has reported the alarm, take the following actions depending on the reporting card:

- If the reporting card is an active traffic line port in a 1+1 protection group or part of a path protection, ensure that an APS traffic switch has occurred to move traffic to the protect port.

  Note Removing a card that currently carries traffic on one or more ports can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-231 for commonly used traffic-switching procedures.

- If the alarm is reported against a TCC2/TCC2P, complete the "Reset an Active TCC2/TCC2P Card and Activate the Standby Card" procedure on page 2-240.
- If the alarm is reported against an OC-N card, complete the "Reset a Traffic Card in CTC" procedure on page 2-239.
- If the alarm is reported against a cross-connect card, complete the "Reset a Traffic Card in CTC" procedure on page 2-239 for the cross-connect card. (The process is similar.)

Step 2 If the alarm does not clear, complete the "Remove and Reinsert (Reseat) Any Card" procedure on page 2-242.

Step 3 If the alarm does not clear, complete the "Physically Replace a Traffic Card" procedure on page 2-243 for the reporting card.

Step 4 If the single card replacement does not clear the alarm, or if multiple cards report the alarm, verify the office power. Refer to the "Install the Shelf and Backplane Cable" chapter in the *Cisco ONS 15454 Procedure Guide* for procedures. See the "1.15 Power Supply Problems" section on page 1-155 as necessary.

Step 5 If the alarm does not clear, reseat the power cable connection to the connector.

Step 6 If the alarm does not clear, physically replace the power cable connection to the connector.

Step 7 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.296 PWR-FAIL-B

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: EQPT

The Equipment Power Failure at Connector B alarm occurs when there is no power supply from the main power connector to the equipment. This alarm occurs on the electrical interface assemblies (EIA), 15454_MRC-12 Multirate card, MRC-2.5G-4 Multirate card, OC192SR1/STM64IO Short Reach and OC192/STM64 Any Reach cards (also known as OC192-XFP in CTC), OC12 IR/STM4 SH 1310-4 card, OC3 IR/STM1 SH 1310-8 card or TCC2/TCC2P.

Warning **The power supply circuitry for the equipment can constitute an energy hazard. Before you install or replace the equipment, remove all jewelry (including rings, necklaces, and watches). Metal objects can come into contact with exposed power supply wiring or circuitry inside the DSLAM equipment. This could cause the metal objects to heat up and cause serious burns or weld the metal object to the equipment.** Statement 207

Clear the PWR-FAIL-B Alarm

Step 1 Complete the "Clear the PWR-FAIL-A Alarm" procedure on page 2-181.

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).

2.8.297 PWR-FAIL-RET-A

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: EQPT

The Equipment Power Failure at Connector A alarm occurs when there is no power supplied to the backup power connector on the shelf. This alarm occurs on the electrical interface assemblies (EIA), 15454_MRC-12 Multirate card, MRC-2.5G-4 Multirate card, OC192SR1/STM64IO Short Reach and OC192/STM64 Any Reach cards (also known as OC192-XFP in CTC), OC12 IR/STM4 SH 1310-4 card, OC3 IR/STM1 SH 1310-8 card or TCC2/TCC2P.

Clear the PWR-FAIL-RET-A Alarm

Step 1 Complete the "Clear the PWR-FAIL-A Alarm" procedure on page 2-181.

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).

2.8.298 PWR-FAIL-RET-B

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: EQPT

The Equipment Power Failure at Connector B alarm occurs when there is no power supplied to the backup power connector on the shelf. This alarm occurs on the electrical interface assemblies (EIA), 15454_MRC-12 Multirate card, MRC-2.5G-4 Multirate card, OC192SR1/STM64IO Short Reach and OC192/STM64 Any Reach cards (also known as OC192-XFP in CTC), OC12 IR/STM4 SH 1310-4 card, OC3 IR/STM1 SH 1310-8 card or TCC2/TCC2P.

Clear the PWR-FAIL-RET-A Alarm

Step 1 Complete the "Clear the PWR-FAIL-A Alarm" procedure on page 2-181.

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).

2.8.299 RAI

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: DS1, DS3, E1

The Remote Alarm Indication condition signifies an end-to-end failure. The error condition is sent from one end of the SONET path to the other. RAI on a DS3XM-6 card indicates that the far-end node is receiving a DS-3 AIS.

Clear the RAI Condition

Step 1 Complete the "Clear the AIS Condition" procedure on page 2-32.

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).

2.8.300 RCVR-MISS

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Objects: DS1, E1

A Facility Termination Equipment Receiver Missing alarm occurs when the facility termination equipment detects an incorrect amount of impedance on its backplane connector. Incorrect impedance usually occurs when a receive cable is missing from a DS-1 port, or a possible mismatch of backplane equipment occurs. For example, an SMB connector or a BNC connector could be misconnected to a DS-1 card.

Note DS-1s are four-wire circuits and need a positive (tip) and negative (ring) connection for both transmit and receive.

Clear the RCVR-MISS Alarm

Step 1 Ensure that the device attached to the DS-1 port is operational.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 2 If the attachment is good, verify that the cabling is securely connected.

Step 3 If the cabling is good, verify that the pinouts are correct.

Step 4 If the pinouts are correct, replace the receive cable.

Step 5 If the alarm does not clear, log into the 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.

2.8.301 RFI

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.302 RFI-L

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

SONET Logical Objects: EC1, OCN

A RFI Line condition occurs when the ONS 15454 detects an RFI in OC-N card SONET overhead because of a fault in another node. Resolving the fault in the adjoining node clears the RFI-L condition in the reporting node. RFI-L indicates that the condition is occurring at the line level.

Clear the RFI-L Condition

Step 1 Log into the node at the far-end node of the reporting ONS 15454.

Step 2 Identify and clear any alarms, particularly the "LOS (OCN)" alarm on page 2-147.

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).

2.8.303 RFI-P

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

SONET Logical Objects: STSMON, STSTRM

The RFI Path condition occurs when the ONS 15454 detects an RFI in the an STS-1 signal SONET overhead because of a fault in another node. Resolving the fault in the adjoining node clears the RFI-P condition in the reporting node. RFI-P occurs in the terminating node in that path segment.

Clear the RFI-P Condition

Step 1 Verify that the ports are enabled and in service (IS-NR) on the reporting ONS 15454:

- **a.** Confirm that the LED is correctly illuminated on the physical card.

  A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.
- **b.** To determine whether the OC-N port is in service, double-click the card in CTC to open the card view.
- **c.** Click the **Provisioning > Line** tabs.
- **d.** Verify that the Admin State column lists the port as IS.
- **e.** If the Admin State column lists the port as OOS,MT or OOS,DSBLD, click the column and choose **IS**. Click **Apply**.

Step 2 To find the path and node failure, verify the integrity of the SONET STS circuit path at each of the intermediate SONET nodes.

Step 3 Clear alarms in the node with the failure, especially the "UNEQ-P" alarm on page 2-223 or the "UNEQ-V" alarm on page 2-225.

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).

2.8.304 RFI-V

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

SONET Logical Object: VT-TERM

An RFI VT Layer condition occurs when the ONS 15454 detects an RFI in the SONET overhead because of a fault in another node. Resolving the fault in the adjoining node clears the RFI-V condition in the reporting node. RFI-V indicates that an upstream failure has occurred at the VT layer.

Clear the RFI-V Condition

Step 1 Verify that the connectors are securely fastened and connected to the correct slot. For more information, refer to the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15454 Procedure Guide*.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 2 If connectors are correctly connected, verify that the DS-N

Step 3 port is active and in service (IS-NR):

a. Confirm that the LED is correctly illuminated on the physical card:

   A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

b. To determine whether the OC-N port is in service, double-click the card in CTC to open the card view.

c. Click the **Provisioning > Line** tabs.

d. Verify that the Admin State column lists the port as IS.

e. If the Admin State column lists the port as OOS,MT or OOS,DSBLD, click the column and choose **IS**. Click **Apply**.

Step 4 If the ports are active and in service, use an optical test set to verify that the signal source does not have errors. For specific procedures to use the test set equipment, consult the manufacturer.

Step 5 If the signal is valid, log into the node at the far-end of the reporting ONS 15454.

Step 6 Clear alarms in the far-end node, especially the "UNEQ-P" alarm on page 2-223 or the "UNEQ-V" alarm on page 2-225.

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).

2.8.305 RING-ID-MIS

Default Severity: Major (MJ), Non-Service-Affecting (NSA)

SONET Logical Object: OCN

DWDM Logical Objects: OSC-RING

The Ring ID Mismatch condition refers to the ring ID in APC. It occurs when a ring name does not match other detectable node ring names, and can cause problems with applications that require data exchange with APC. This alarm is similar to BLSR RING-MISMATCH, but rather than apply to ring protection, RING-ID-MIS applies to DWDM node discovery within the same network.

Note For more information about APC, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Clear the RING-ID-MIS Alarm

Step 1 Complete the "Clear the RING-MISMATCH Alarm" procedure on page 2-187.

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).

2.8.306 RING-MISMATCH

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Object: OCN

A Procedural Error Mismatch Ring alarm occurs when the ring name of the ONS 15454 node that is reporting the alarm does not match the ring name of another node in the BLSR. Nodes connected in a BLSR must have identical ring names to function. This alarm can occur during BLSR provisioning.

RING-MISMATCH is somewhat similar to RING-ID-MIS, but it applies to BLSR protection discovery instead of DWDM node discovery.

Note For more information about DWDM cards, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Clear the RING-MISMATCH Alarm

Step 1 In node view, click the **Provisioning > BLSR** tabs.

Step 2 Note the name in the Ring Name field.

Step 3 Log into the next ONS 15454 node in the BLSR.

Step 4 Complete the "Identify a BLSR Ring Name or Node ID Number" procedure on page 2-230.

Step 5 If the ring name matches the ring name in the reporting node, repeat Step 4 for the next ONS 15454 in the BLSR.

Step 6 Complete the "Change a BLSR Ring Name" procedure on page 2-230.

Step 7 Verify that the ring map is correct.

Step 8 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

2.8.307 RING-SW-EAST

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: OCN

The Ring Switch Is Active East Side condition occurs when a ring switch occurs at the east side of a BLSR 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.

2.8.308 RING-SW-WEST

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: OCN

The Ring Switch Is Active West Side condition occurs when a ring switch occurs at the west side of a BLSR 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.

2.8.309 ROLL

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: STSMON, STSTRM, VT-MON

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.

2.8.310 ROLL-PEND

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: STSMON, STSTRM, VT-MON

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.

2.8.311 RPRW

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: CE100T, ML100T, ML1000, MLFX

The Resilient Packet Ring (RPR) Wrapped condition applies to ML-Series card and occurs when the RPR protocol initiates a ring wrap due to a fiber cut, node failure, node restoration, new node insertion, or other traffic problem. It can also be raised if the POS port has an Admin down condition. (In this case, you will not see any SONET-level or TPTFAIL alarms.). The POS port can go down for the following reason : Deletion of circuit on the POS port.

When the wrap occurs, traffic is redirected to the original destination by sending it in the opposite direction around the ring after a link state change or after receiving any SONET path-level alarms.

Note ML-Series card POS interfaces normally send the "PDI-P" alarm on page 2-174 to the far end when the POS link goes down or when RPR wraps. ML-Series card POS interfaces do not send a PDI-P alarm to the far end when this alarm is detected, when the alarm is being sent to the far end, or when the only defects being detected are the "GFP-LFD" alarm on page 2-109, the "GFP-CSF" alarm on page 2-107, the VCAT "LOM" alarm on page 2-137, or the VCAT "SQM" alarm on page 2-203.

Note For more information about CE-100T-8 and ML-Series Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.

Clear the RPRW Condition

Step 1 If a circuit on the POS port part of SPR interface had been deleted, recreate the circuit on the POS port for this alarm to clear ring wrapping.

Step 2 Look for and clear any service-affecting SONET path-level alarms on the affected circuit, such as the "LOP-P" alarm on page 2-138, "PLM-P" alarm on page 2-176, or the "TIM-P" alarm on page 2-216. Clearing this alarm can also clear RPRW.

Step 3 If the condition does not clear, look for and clear any service alarms for the ML-Series card itself, such as the "CARLOSS (CE100T)" alarm on page 2-52, "CARLOSS (ML100T, ML1000, MLFX)" alarm on page 2-59, "TPTFAIL (CE100T)" alarm on page 2-218, or the "TPTFAIL (ML100T, ML1000, MLFX)" alarm on page 2-220.

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).

2.8.312 RUNCFG-SAVENEED

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: EQPT

The Run Configuration Save Needed condition occurs when you change the running configuration file for ML-Series cards. It is a reminder that you must save the change to the startup configuration file for it to be permanent.

The condition clears after you save the running configuration to the startup configuration, such as by entering:

```
copy run start
```

at the privileged EXEC mode of the Cisco IOS CLI. If you do not save the change, the change is lost after the card reboots. If the command “copy run start” is executed in configuration mode and not privileged EXEC mode, the running configuration will be saved, but the alarm will not clear.

Note For more information about the ML-Series Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.*

2.8.313 SD (DS1, DS3)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: DS1, DS3

A Signal Degrade (SD) condition for DS-1 or DS-3 occurs when the quality of an electrical signal on a DS3XM-6, DS3XM-12, or DS3/EC1-48 card has exceeded the BER signal degrade threshold. Signal degrade is defined by Telcordia as a soft failure condition. SD and signal fail (SF) both monitor the incoming BER and are similar, but SD is triggered at a lower bit error rate than SF.

The BER threshold is user-provisionable and has a range for SD from 1E–9 dBm to 1E–5 dBm.

SD can be reported on electrical card ports that are In-Service and Normal (IS-NR); Out-of-Service and Autonomous, Automatic In-Service (OOS-AU,AIS); or Out-of-Service and Management, Maintenance (OOS-MA,MT), but not in the Out-of-Service and Management, Disabled (OOS-MA,DSBLD) service state. The BER count increase associated with this alarm does not take an IS-NR port out of service, but if it occurs on an AINS port, the alarm prevents the port from going into service.

The SD condition clears when the BER level falls to one-tenth of the threshold level that triggered the condition. A BER increase is sometimes caused by a physical fiber problem such as a faulty fiber connection, a bend in the fiber that exceeds the permitted bend radius, or a bad fiber splice. SD can also be caused by repeated XC10G card switches that in turn can cause switching on the lines or paths.

Warning **Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard.** Statement 1056

Warning **Use of controls, adjustments, or performing procedures other than those specified could result in hazardous radiation exposure.** Statement 1057

Note Some levels of BER errors (such as 1E–9 dBm) take a long period to raise or clear, about 9,000 seconds, or 150 minutes. If the SD threshold is provisioned at 1E–9 dBm rate, the SD alarm needs at least one and one-half hours to raise and then another period at least as long to clear.

Note The recommended test set for use on all SONET ONS electrical cards is the Omniber 718. For specific procedures to use the test set equipment, consult the manufacturer.

Clear the SD (DS1, DS3) Condition

Step 1 If the condition applies for a DS-3 line on a DS3XM-6, DS3XM-12, DS3E-12, or DS3/EC1-48 card, complete the "Clear a DS3XM-6, DS3XM-12, or DS3E-12 Card Loopback Circuit" procedure on page 2-246. If the condition applies to any other DS-N card (DS3i-N-14, DS3-12, DS3i-N-14, or DS1/E1-56) complete the "Clear Other Electrical Card, CE-100T-8, or Ethernet Card Loopbacks" procedure on page 2-246.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 2 Ensure that the fiber connector for the card is completely plugged in. For more information about fiber connections and card insertion, refer to the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15454 Procedure Guide*.

Step 3 If the BER threshold is correct and at the expected level, use an optical test set to measure the power level of the line to ensure it is within guidelines. For specific procedures to use the test set equipment, consult the manufacturer.

Step 4 If the optical power level is good, verify that optical receive levels are within the acceptable range.

Step 5 If receive levels are good, clean the fibers at both ends according to site practice. If no site practice exists, complete the procedure in the "Maintain the Node" chapter in the *Cisco ONS 15454 Procedure Guide*.

Step 6 If the condition does not clear, verify that single-mode fiber is used.

Step 7 If the fiber is of the correct type, verify that a single-mode laser is used at the far-end node.

Step 8 Clean the fiber connectors at both ends for a signal degrade according to site practice.

Step 9 Verify that a single-mode laser is used at the far end.

Step 10 If the problem does not clear, the transmitter at the other end of the optical line could be failing and require replacement. Refer to the "2.10.4 Physical Card Reseating, Resetting, and Replacement" section on page 2-241.

Step 11 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.314 SD (E1)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: E1

An SD condition for an E1 occurs on a DS1/E1-56 card in E1 only mode when the quality of an electrical signal has exceeded the BER signal degrade threshold.

SD is triggered at a lower bit error rate than SF. The SD BER threshold is user-provisionable and ranges from 1E–9 dBm to 1E–5 dBm.

SD can be reported on electrical card ports that are In-Service and Normal (IS-NR); Out-of-Service and Autonomous, Automatic In-Service (OOS-AU,AIS); or Out-of-Service and Management, Maintenance (OOS-MA,MT) but not in the Out-of-Service and Management, Disabled (OOS-MA,DSBLD) service state. The BER count increase associated with this alarm does not take an IS-NR port out of service, but if it occurs on an AINS port, the alarm prevents the port from going into service.

The SD condition clears when the BER level falls to one-tenth of the threshold level that triggered the condition. A BER increase is sometimes caused by a physical fiber problem such as a faulty fiber connection, a bend in the fiber that exceeds the permitted bend radius, or a bad fiber splice. SD can also be caused by repeated XC10G card switches that in turn can cause switching on the lines or paths.

Warning **Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard.** Statement 1056

Warning **Use of controls, adjustments, or performing procedures other than those specified could result in hazardous radiation exposure.** Statement 1057

Note Some levels of BER errors (such as 1E–9 dBm) take a long period to raise or clear, about 9,000 seconds, or 150 minutes. If the SD threshold is provisioned at 1E–9 dBm rate, the SD alarm needs at least one and a half hours to raise and then another period at least as long to clear.

Note The recommended test set for use on all SONET ONS electrical cards is the Omniber 718. For specific procedures to use the test set equipment, consult the manufacturer.

Clear the SD (E1) Condition

Step 1 Complete the "Clear Other Electrical Card, CE-100T-8, or Ethernet Card Loopbacks" procedure on page 2-246.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 2 Ensure that the fiber connector for the card is completely plugged in. For more information about fiber connections and card insertion, refer to the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15454 Procedure Guide*.

Step 3 If the BER threshold is correct and at the expected level, use an optical test set to measure the power level of the line to ensure it is within guidelines. For specific procedures to use the test set equipment, consult the manufacturer.

Step 4 If the optical power level is good, verify that optical receive levels are within the acceptable range.

Step 5 If receive levels are good, clean the fibers at both ends according to site practice. If no site practice exists, complete the procedure in the "Maintain the Node" chapter of the *Cisco ONS 15454 Procedure Guide*.

Step 6 If the condition does not clear, verify that single-mode fiber is used.

Step 7 If the fiber is of the correct type, verify that a single-mode laser is used at the far-end node.

Step 8 Clean the fiber connectors at both ends for a signal degrade according to site practice.

Step 9 If the problem does not clear, the transmitter at the other end of the optical line could be failing and require replacement. Refer to the "2.10.4 Physical Card Reseating, Resetting, and Replacement" section on page 2-241.

Step 10 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.315 SD (TRUNK)

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.316 SD-L

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: EC1, OCN

An SD Line condition is similar to the "SD (DS1, DS3)" condition on page 2-190. It applies to the line level of the SONET signal and travels on the B2 byte of the SONET overhead.

An SD-L on an Ethernet or OC-N card does not cause a protection switch. If the alarm is reported on a card that has also undergone a protection switch, the SD BER count continues to accumulate. The condition is superseded by higher-priority alarms such as the "LOF (EC1)" alarm on page 2-134, the "LOF (OCN)" alarm on page 2-135, the "LOS (EC1)" alarm on page 2-145, and the "LOS (OCN)" alarm on page 2-147.

Note For more information about Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.

Clear the SD-L Condition

Step 1 Complete the "Clear the SD (DS1, DS3) Condition" procedure on page 2-191.

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).

2.8.317 SD-P

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: STSMON, STSTRM

An SD Path condition is similar to the "SD (DS1, DS3)" condition on page 2-190, but it applies to the path (STS) layer of the SONET overhead. A path or STS-level SD alarm travels on the B3 byte of the SONET overhead.

For path protection protected circuits, the BER threshold is user-provisionable and has a range for SD from 1E–9 dBm to 1E–5 dBm. For BLSR 1+1 and unprotected circuits, the BER threshold value is not user-provisionable and the error rate is hard-coded to 1E–6 dBm.

On path protection configurations, an SD-P condition causes a switch from the working card to the protect card at the path (STS) level. On BLSR, 1+1, and on unprotected circuits, an SD-P condition does not cause switching.

The BER increase that causes the condition is sometimes caused by a physical fiber problem such as a poor fiber connection, a bend in the fiber that exceeds the permitted bend radius, or a bad fiber splice.

The SD clears when the BER level falls to one-tenth of the threshold level that triggered the alarm.

Clear the SD-P Condition

Step 1 Complete the "Clear the SD (DS1, DS3) Condition" procedure on page 2-191.

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).

2.8.318 SD-V

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: VT-MON, VT-TERM

An SD-V condition is similar to the "SD (DS1, DS3)" condition on page 2-190, but it applies to the VT layer of the SONET overhead.

For path protection protected circuits, the BER threshold is user-provisionable and has a range for SD from 1E–9 dBm to 1E–5 dBm. For BLSR 1+1 and unprotected circuits, the BER threshold value is not user-provisionable and the error rate is hard-coded to 1E–6 dBm.

On path protection configurations, an SD-V condition does not cause a switch from the working card to the protect card at the path (STS) level. On BLSR, 1+1, and on unprotected circuits, an SD-V condition does not cause switching.

The BER increase that causes the alarm is sometimes caused by a physical fiber problem such as a poor fiber connection, a bend in the fiber that exceeds the permitted bend radius, or a bad fiber splice.

The SD alarm clears when the BER level falls to one-tenth of the threshold level that triggered the alarm.

Clear the SD-V Condition

Step 1 Complete the "Clear the SD (DS1, DS3) Condition" procedure on page 2-191.

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).

2.8.319 SF (DS1, DS3)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: DS1, DS3

A Signal Fail (SF) condition occurs when the quality of the signal has exceeded the BER signal failure threshold. Signal failure is defined by Telcordia as a "hard failure" condition. The SD and SF conditions both monitor the incoming BER error rate and are similar conditions, but SF is triggered at a higher BER than SD.

The BER threshold is user-provisionable and has a range for SF from 1E–5 dBm to 1E–3 dBm.

Warning **Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard.** Statement 1056

Warning **Use of controls, adjustments, or performing procedures other than those specified could result in hazardous radiation exposure.** Statement 1057

Clear the SF (DS1, DS3) Condition

Step 1 Complete the "Clear the SD (DS1, DS3) Condition" procedure on page 2-191.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.320 SF (E1)

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: E1

An SF condition for an E1 occurs on a DS1/lE1-56 card in E1 only mode when the quality of the signal has exceeded the BER signal failure threshold.

SF monitors the incoming BER error rate just as SD does, but SF is triggered at a higher BER than SD. The SF BER threshold is user-provisionable and has a range for SF from 1E–5 dBm to 1E–3 dBm.

Warning **Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard.** Statement 1056

Warning **Use of controls, adjustments, or performing procedures other than those specified could result in hazardous radiation exposure.** Statement 1057

Clear the SF (E1) Condition

Step 1 Complete the "Clear the SD (E1) Condition" procedure on page 2-192.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.321 SF (TRUNK)

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.322 SF-L

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: EC1, OCN

An SF Line condition is similar to the "SF (DS1, DS3)" condition on page 2-195, but it applies to the line layer B2 overhead byte of the SONET signal. It can trigger a protection switch.

The SF-L condition clears when the BER level falls to one-tenth of the threshold level that triggered the condition. A BER increase is sometimes caused by a physical fiber problem, including a poor fiber connection, a bend in the fiber that exceeds the permitted bend radius, or a bad fiber splice.

The condition is superseded by higher-priority alarms such as the "LOF (EC1)" alarm on page 2-134, the "LOS (EC1)" alarm on page 2-145, and the "LOS (OCN)" alarm on page 2-147.

Clear the SF-L Condition

Step 1 Complete the "Clear the SD (DS1, DS3) Condition" procedure on page 2-191.

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).

2.8.323 SF-P

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: STSMON, STSTRM

An SF Path condition is similar to the "SF (DS1, DS3)" condition on page 2-195, but it applies to the path (STS) layer B3 byte of the SONET overhead. It can trigger a protection switch.

The SF-P condition clears when the BER level falls to one-tenth of the threshold level that triggered the condition. A BER increase is sometimes caused by a physical fiber problem, including a poor fiber connection, a bend in the fiber that exceeds the permitted bend radius, or a bad fiber splice.

Clear the SF-P Condition

Step 1 Complete the "Clear the SD (DS1, DS3) Condition" procedure on page 2-191.

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).

2.8.324 SFTWDOWN

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: EQPT

A Software Download in Progress alarm occurs when the TCC2/TCC2P is downloading or transferring software.

If the active and standby TCC2/TCC2Ps have the same versions of software, it takes approximately three minutes for software to be updated on a standby TCC2/TCC2P.

If the active and standby TCC2/TCC2Ps have different software versions, the transfer can take up to 30 minutes. Software transfers occur when different software versions exist on the two cards. After the transfer completes, the active TCC2/TCC2P reboots and goes into standby mode after approximately three minutes.

No action is necessary. Wait for the transfer or the software download to complete. If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

Note SFTWDOWN is an informational alarm.

2.8.325 SF-V

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: VT-MON, VT-TERM

An SF-V condition is similar to the "SF (DS1, DS3)" condition on page 2-195, but it applies to the VT layer of the SONET overhead.

Clear the SF-V Condition

Step 1 Complete the "Clear the SD (DS1, DS3) Condition" procedure on page 2-191.

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).

2.8.326 SH-INS-LOSS-VAR-DEG-HIGH

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.327 SH-INS-LOSS-VAR-DEG-LOW

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.328 SHUTTER-OPEN

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.329 SIGLOSS

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Object: FCMR

DWDM Logical Objects: FC, GE, ISC, TRUNK

The Signal Loss on Data Interface alarm is raised on FC_MR-4 card receive client ports and MXP card FC and ISC client data ports when there is a loss of signal. (Loss of Gigabit Ethernet client signal results in a CARLOSS [GE], not SIGLOSS.) SIGLOSS can also be raised on the MXP trunk port.

If the SYNCLOSS alarm was previously raised on the port, the SIGLOSS alarm will demote it.

Clear the SIGLOSS Alarm

Step 1 Ensure that the port connection at the near end of the SONET link is operational.

Step 2 Verify fiber continuity to the port. To verify fiber continuity, follow site practices.

Step 3 Check the physical port LED on the card. The port LED looks clear (that is, not lit green) if the link is not connected.

Step 4 If the alarm does not clear, log onto http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

2.8.330 SNTP-HOST

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Object: NE

The Simple Network Timing Protocol (SNTP) Host Failure alarm indicates that an ONS 15454 serving as an IP proxy for the other ONS 15454 nodes in the ring is not forwarding SNTP information to the other nodes in the network. The forwarding failure can result from two causes: either the IP network attached to the ONS 15454 proxy node is experiencing problems, or the ONS 15454 proxy node itself is not functioning properly.

Clear the SNTP-HOST Alarm

Step 1 Ping the SNTP host from a workstation in the same subnet to ensure that communication is possible within the subnet by completing the "Verify PC Connection to the ONS 15454 (ping)" procedure on page 1-124.

Step 2 If the ping fails, contact the network administrator who manages the IP network that supplies the SNTP information to the proxy and determine whether the network is experiencing problems, which could affect the SNTP server/router connecting to the proxy ONS 15454 system.

Step 3 If no network problems exist, ensure that the ONS system proxy is provisioned correctly:

- **a.** In node view for the ONS 15454 serving as the proxy, click the **Provisioning > General** tabs.
- **b.** Ensure that the Use NTP/SNTP Server check box is checked.
- **c.** If the Use NTP/SNTP Server check box is not checked, click it.
- **d.** Ensure that the Use NTP/SNTP Server field contains a valid IP address for the server.

Step 4 If proxy is correctly provisioned, refer to the "Timing" chapter in the *Cisco ONS 15454 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).

2.8.331 SPAN-SW-EAST

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: OCN

The Span Switch Is Active East Side condition occurs when a span switch occurs at the east side of a four-fiber BLSR span using a Force Span command. The condition clears when the switch is cleared. SPAN-SW-EAST is visible on the network view Alarms, Conditions, and History tabs. The port where the Force Span was applied shows an "F" on the network view detailed circuit map.

Note SPAN-SW-EAST is an informational condition and does not require troubleshooting.

2.8.332 SPAN-SW-WEST

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: OCN

The Span Switch Is Active West Side condition occurs when a span switch occurs at the west side of a four-fiber BLSR span using a Force Span command. The condition clears when the switch is cleared. SPAN-SW-WEST is visible on the network view Alarms, Conditions, and History tabs. The port where the Force Span was applied shows an "F" on the network view detailed circuit map.

Note SPAN-SW-WEST is an informational condition and does not require troubleshooting.

2.8.333 SQUELCH

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: OCN

The Ring Squelching Traffic condition occurs in a BLSR when a node that originates or terminates STS circuits fails or is isolated by multiple fiber cuts or maintenance Force Ring commands. The isolation or failure of the node disables circuits that originate or terminate on the failed node. SQUELCH conditions appear on one or both of the nodes on either side of the isolated or failed node. The "AIS-P" condition on page 2-33 also appears on all nodes in the ring except the isolated node.

Warning **On the OC-192 card, the laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. The laser is off when the safety key is off (labeled 0).** Statement 293.

Warning **Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard.** Statement 1056

Warning **Use of controls, adjustments, or performing procedures other than those specified could result in hazardous radiation exposure.** Statement 1057

Clear the SQUELCH Condition

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 1 Determine the isolated node:

a. From the View menu, choose **Go to Network View**.

b. The grayed out node with red spans is the isolated node.

Step 2 Verify fiber continuity to the ports on the isolated node. To verify cable continuity, follow site practices.

Step 3 If fiber continuity is good, verify that the proper ports are in service:

a. Confirm that the LED is correctly illuminated on the physical card.

A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

b. To determine whether the OC-N port is in service, double-click the card in CTC to open the card view.

c. Click the **Provisioning > Line** tabs.

d. Verify that the Admin State column lists the port as IS.

e. If the Admin State column lists the port as OOS,MT or OOS,DSBLD, click the column and choose **IS**. Click **Apply**.

Step 4 If the correct ports are in service, 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 5 If the signal is valid, verify that the power level of the optical signal is within the optical card receiver specifications. Refer to the *Cisco ONS 15454 Reference Manual* for card specifications.

Step 6 If the receiver levels are good, ensure that the optical transmit and receive fibers are connected properly.

Step 7 If the connectors are good, complete the "Physically Replace a Traffic Card" procedure on page 2-243 for the OC-N card.

Step 8 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).

2.8.334 SQUELCHED

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: OCN

DWDM Logical Objects: 2R, ESCON, FC, GE, ISC, TRUNK

The Client Signal Squelched condition is raised by a TXP_MR_10G, TXP_MR_10E, TXP_MR_2.5G, TXPP_MR_2.5G, MXP_2.5G_10G, MXP_2.5G_10E, MXP_MR_2.5G, or MXPP_MR_2.5G card.

The condition can be raised in the following situations:

- An MXP or TXP client facility detects that an upstream receive facility has experienced a loss of signal (such as an Ethernet CARLOSS, DWDM SIGLOSS, or optical LOS). In response, the facility's transmit is turned off (SQUELCHED). The upstream receive facilities are the trunk receive on the same card as the client, as well as the client receive on the card at the other end of the trunk span.
- The client will squelch if the upstream trunk receive (on the same card) experiences a SIGLOSS, Ethernet CARLOSS, LOS, or LOS (TRUNK) alarm. In some transparent modes, the client is squelched if the trunk detects an AIS condition or a TIM alarm.
- The client will squelch if the upstream client receive (on the card at the other end of the DWDM span) experiences CARLOSS, SIGLOSS, or LOS.

In an example situation, an upstream MXP_2.5G_10G client port receive experiences a "loss of light," and this port raises CARLOSS, SIGLOSS, or LOS (determined by the payload type) locally. The port also sends client signal fail (GFP-CSF) to its downstream card. The downstream card raises a GFP-CSF alarm, turns off the client transmit laser, and raises the SQUELCHED condition.

The local client raises SQUELCHED if it also raises one of the following alarms for the client, all of which are signalled by the upstream node:

- 2.8.136 GFP-CSF, page 2-107
- 2.8.139 GFP-LFD, page 2-109
- 2.8.140 GFP-NO-BUFFERS, page 2-109
- 2.8.137 GFP-DE-MISMATCH, page 2-107
- 2.8.138 GFP-EX-MISMATCH, page 2-108
- 2.8.253 ODUK-1-AIS-PM, page 2-170
- 2.8.254 ODUK-2-AIS-PM, page 2-170
- 2.8.255 ODUK-3-AIS-PM, page 2-170
- 2.8.256 ODUK-4-AIS-PM, page 2-170

On the MXP_MR_10G, the local client raises a SQUELCHED condition if the upstream client detects one of the following alarms. Note that no corresponding local alarm is raised to indicate which of these conditions is present upstream.

- LOS for the clients including the "LOS (2R)" alarm on page 2-140, the "LOS (ESCON)" alarm on page 2-146, and the "LOS (ISC)" alarm on page 2-147
- CARLOSS for the clients including the "CARLOSS (FC)" alarm on page 2-56, the "CARLOSS (GE)" alarm on page 2-59, and the "CARLOSS (ISC)" alarm on page 2-59

The local client raises a SQUELCHED condition if the local trunk raises one of the following alarms:

- 2.8.275 OTUK-LOF, page 2-173
- 2.8.272 OTUK-AIS, page 2-173
- 2.8.201 LOS (TRUNK), page 2-149
- 2.8.278 OTUK-TIM, page 2-174 (squelching enabled)
- 2.8.257 ODUK-AIS-PM, page 2-171
- 2.8.259 ODUK-LCK-PM, page 2-171
- 2.8.263 ODUK-TIM-PM, page 2-171 (squelching enabled)
- 2.8.364 TIM, page 2-215 (for the OC-N, squelching enabled)
- 2.8.180 LOF (OCN), page 2-135

- 2.8.199 LOS (OCN), page 2-147
- 2.8.54 CARLOSS (TRUNK), page 2-60
- 2.8.393 WVL-MISMATCH, page 2-229 (client or trunk)

When troubleshooting the SQUELCHED condition locally, look for failures progressing upstream in the following order. (If you are troubleshooting this alarm remotely, reverse the order of progress.)

- Local client alarms, as above
- Local trunk alarms, as above
- Remote (upstream) client receive alarms, as above

Note If you see a SQUELCHED condition on the trunk, this can only be caused by a transponder (TXP) card.

Clear the SQUELCHED Condition

Step 1 If the object is reported against any object besides ESCON, determine whether the remote node and local node reports and LOF or the LOS alarm (for the client trunk, as listed above). If it does, turn to the relevant section in this chapter and complete the troubleshooting procedure.

Step 2 If no LOF or LOS is reported, determine whether any other listed remote node or local node conditions as listed above has occurred. If so, turn to the relevant section of this chapter and complete the troubleshooting procedure.

Step 3 If none of these alarms is reported, determine whether the local port reporting the SQUELCHED condition is in loopback. (You will see LPBKFACILITY OR LPBKTERMINAL in the condition window for this port.) If it is in loopback, complete the following steps:

a. Double-click the client card to open the card view.

b. Click the **Maintenance > Loopback > Port** tabs.

c. If the port Admin State column says OOS,MT or OOS,DSBLD, click the cell to highlight it and choose **IS** from the drop-down list. Changing the state to IS also clears any loopback provisioned on the port.

Step 4 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.335 SQM

Default Severity: Critical (CR), Service-Affecting (SA) for STSTRM; Major (MJ), Service-Affecting (SA) for VT-TERM

SONET Logical Objects: STSTRM, VT-TERM

The Sequence Mismatch alarm is a virtual concatenated (VCAT) member alarm. (VCAT member circuits are independent circuits that are concatenated from different time slots into a higher-rate signal.) The alarm occurs when the expected sequence numbers of VCAT members do not match the received sequence numbers.

Clear the SQM Alarm

Step 1 For the errored circuit, complete the "Delete a Circuit" procedure on page 2-244.

Step 2 Recreate the circuit using the "Create Circuits and VT Tunnels" chapter of the *Cisco ONS 15454 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) in order to report a Service-Affecting (SA) problem.

2.8.336 SSM-DUS

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: BITS, DS1, E1, OCN

DWDM Logical Objects: TRUNK

The Synchronization Status (SSM) Message Quality Changed to Do Not Use (DUS) condition occurs when the synchronization status message (SSM) quality level degrades to DUS or is manually changed to DUS.

The signal is often manually changed to DUS to prevent timing loops from occurring. Sending a DUS prevents the timing from being reused in a loop. The DUS signal can also be sent for line maintenance testing.

Note SSM-DUS is an informational condition and does not require troubleshooting.

2.8.337 SSM-FAIL

Single Failure Default Severity: Minor (MN), Non-Service-Affecting (NSA); Double Failure Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Objects: BITS, DS1, E1, OCN

DWDM Logical Object: TRUNK

The SSM Failed alarm occurs when the synchronization status messaging received by the ONS 15454 fails. The problem is external to the ONS 15454. This alarm indicates that although the ONS 15454 is set up to receive SSM, the timing source is not delivering valid SSM messages.

Clear the SSM-FAIL Alarm

Step 1 Verify that SSM is enabled on the external timing source.

Step 2 If timing is enabled, use an optical test set to determine that the external timing source is delivering SSM. For specific procedures to use the test set equipment, consult the manufacturer.

Step 3 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.338 SSM-LNC

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.339 SSM-OFF

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: BITS, DS1, E1, OCN

DWDM Logical Object: TRUNK

The SSM Off condition applies to references used for timing the node. It occurs when the SSM for the reference has been turned off. The node is set up to receive SSM, but the timing source is not delivering SSM messages.

Clear the SSM-OFF Condition

Step 1 Complete the "Clear the SSM-FAIL Alarm" procedure on page 2-204.

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).

2.8.340 SSM-PRC

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.341 SSM-PRS

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: BITS, DS1, E1, NE-SREF, OCN

DWDM Logical Object: TRUNK

The SSM Primary Reference Source (PRS) Traceable condition occurs when the SSM transmission level is changed to Stratum 1 Traceable.

Note SSM-PRS is an informational condition and does not require troubleshooting.

2.8.342 SSM-RES

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: BITS, DS1, E1, NE-SREF, OCN

DWDM Logical Objects: BITS, DS1, E1, NE-SREF, OCN

The SSM Reserved (RES) For Network Synchronization Use condition occurs when the synchronization message quality level is changed to RES.

Note SSM-RES is an informational condition and does not require troubleshooting.

2.8.343 SSM-SDN-TN

The SSM-SDN-TN condition is not used in this platform in this release. It is reserved for future development.

2.8.344 SSM-SETS

The SSM-SETS condition is not used in this platform in this release. It is reserved for future development.

2.8.345 SSM-SMC

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: BITS, DS1, E1, NE-SREF, OCN

DWDM Logical Objects: TRUNK

The SSM SONET Minimum Clock (SMC) Traceable condition occurs when the synchronization message quality level changes to SMC. The login node does not use the clock because the node cannot use any reference beneath its internal level, which is ST3.

Note SSM-SMC is an informational condition and does not require troubleshooting.

2.8.346 SSM-ST2

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: BITS, DS1, E1, NE-SREF, OCN

DWDM Logical Object: TRUNK

The SSM Stratum 2 (ST2) Traceable condition occurs when the synchronization message quality level is changed to ST2.

Note SSM-ST2 is an informational condition and does not require troubleshooting.

2.8.347 SSM-ST3

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: BITS, DS1, E1, NE-SREF, OCN

DWDM Logical Object: TRUNK

The SSM Stratum 3 (ST3) Traceable condition occurs when the synchronization message quality level is changed to ST3.

Note SSM-ST3 is an informational condition and does not require troubleshooting.

2.8.348 SSM-ST3E

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: BITS, DS1, E1, NE-SREF, OCN

DWDM Logical Object: TRUNK

The SSM Stratum 3E (ST3E) Traceable condition indicates that the synchronization message quality level is changed to ST3E from a lower level of synchronization. SSM-ST3E is a Generation 2 SSM and is used for Generation 1.

Note SSM-ST3E is an informational condition and does not require troubleshooting.

2.8.349 SSM-ST4

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: BITS, DS1, E1, NE-SREF, OCN

DWDM Logical Object: TRUNK

The SSM Stratum 4 (ST4) Traceable condition occurs when the synchronization message quality level is lowered to ST4. The message quality is not used because it is below ST3.

Note SSM-ST4 is an informational condition and does not require troubleshooting.

2.8.350 SSM-STU

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: BITS, DS1, E1, NE-SREF, OCN

DWDM Logical Object: TRUNK

The SSM Synchronization Traceability Unknown (STU) condition occurs when the reporting node is timed to a reference that does not support SSM, but the ONS 15454 has SSM support enabled. SSM-STU can also occur if the timing source is sending out SSM messages but SSM is not enabled on the ONS 15454.

Clear the SSM-STU Condition

Step 1 In node view, click the **Provisioning > Timing > BITS Facilities** tabs.

Step 2 Complete one of the following depending upon the status of the Sync Messaging Enabled check box:

- If the **Sync. Messaging Enabled** check box for the BITS source is checked, uncheck the box.
- If the **Sync. Messaging Enabled** check box for the BITS source is not checked, check the box.

Step 3 Click **Apply**.

Step 4 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.351 SSM-TNC

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: BITS, NE-SREF, OCN

DWDM Logical Object: TRUNK

The SSM Transit Node Clock (TNC) Traceable condition occurs when the synchronization message quality level is changed to TNC.

Note SSM-TNC is an informational condition and does not require troubleshooting.

2.8.352 SWMTXMOD-PROT

Default Severity: Critical (CR), Service-Affecting (SA)

SONET Logical Object: EQPT

The Switching Matrix Module Failure on Protect Slot alarm is raised by the Slot 10 cross connect card if this card is active (ACT). Any kind of cross-connect card can raise this alarm. (Two exceptions are given in the following paragraph.) SWMTXMOD-PROT occurs when a logic component internal to the Slot 10 cross connect is out of frame (OOF) with a traffic card in the system. In this case, the alarm is raised against the traffic card slot.

The XC-VXC-10G card can raise this alarm (in Slot 10) whether it is ACT or standby (SBY). The XCVT card can raise SWMTXMOD-PROT against itself if the cross-connect card is OOF with a second logic component on the same cross connect card.

Clear the SWMTXMOD-PROT Alarm

Step 1 Complete the "Reset a Traffic Card in CTC" procedure on page 2-239 for the Slot 10 card. For the LED behavior, see the "2.9.2 Typical Traffic Card LED Activity During Reset" section on page 2-229.

Step 2 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

Step 3 If the alarm does not clear, complete the "Remove and Reinsert (Reseat) Any Card" procedure on page 2-242 for the Slot 10 cross-connect card.

Step 4 Complete the "Side Switch the Active and Standby Cross-Connect Cards" procedure on page 2-240.

Note After the active cross-connect card goes into standby mode, the original standby slot becomes active. The former standby card ACT/SBY LED becomes green.

Step 5 If the alarm does not clear, log into the 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.

2.8.353 SWMTXMOD-WORK

Default Severity: Critical (CR), Service-Affecting (SA)

SONET Logical Object: EQPT

The Switching Matrix Module Failure on Working Slot alarm is raised by the Slot 8 cross connect card if this card is active (ACT). Any kind of cross-connect card can raise this alarm. (Two exceptions are given in the following paragraph.) SWMTXMOD-WORK occurs when a logic component internal to the Slot 8 cross connect is OOF with a traffic card in the system. In this case, the alarm is raised against the traffic card slot.

The XC-VXC-10G card can raise this alarm (in Slot 8) whether it is ACT or standby (SBY). The XCVT card can raise SWMTXMOD-WORK against itself if the cross-connect card is OOF with a second logic component on the same cross connect card.

Clear the SWMTXMOD-WORK Alarm

Step 1 Complete the "Reset a Traffic Card in CTC" procedure on page 2-239 for the Slot 8 card. For the LED behavior, see the "2.9.2 Typical Traffic Card LED Activity During Reset" section on page 2-229.

Step 2 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. A green ACT/SBY LED indicates an active card. An amber ACT/SBY LED indicates a standby card.

Step 3 If the alarm does not clear, complete the "Remove and Reinsert (Reseat) Any Card" procedure on page 2-242 for the Slot 8 cross-connect card.

Step 4 Complete the "Side Switch the Active and Standby Cross-Connect Cards" procedure on page 2-240.

Note After the active cross-connect card goes into standby mode, the original standby slot becomes active. The former standby card ACT/SBY LED becomes green.

Step 5 If the alarm does not clear, log into the 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.

2.8.354 SWTOPRI

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: EXT-SREF, NE-SREF

The Synchronization Switch to Primary Reference condition occurs when the ONS 15454 switches to the primary timing source (reference 1). The ONS 15454 uses three ranked timing references. The timing references are typically two BITS-level or line-level sources and an internal reference.

Note SWTOPRI is an informational condition and does not require troubleshooting.

2.8.355 SWTOSEC

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: EXT-SREF, NE-SREF

The Synchronization Switch to Secondary Reference condition occurs when the ONS 15454 has switched to a secondary timing source (reference 2).

Clear the SWTOSEC Condition

Step 1 To clear the condition, clear alarms related to failures of the primary source, such as the "SYNCPRI" alarm on page 2-212.

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).

2.8.356 SWTOTHIRD

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: EXT-SREF, NE-SREF

The Synchronization Switch to Third Reference condition occurs when the ONS 15454 has switched to a third timing source (reference 3).

Clear the SWTOTHIRD Condition

Step 1 To clear the condition, clear alarms related to failures of the primary source, such as the "SYNCPRI" alarm on page 2-212 or the "SYNCSEC" alarm on page 2-212.

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).

2.8.357 SYNC-FREQ

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: BITS, DS1, E1, OCN

DWDM Logical Object: TRUNK

The Synchronization Reference Frequency Out of Bounds condition is reported against any reference that is out of the bounds for valid references. The login node fails the reference and chooses another internal or external reference to use.

Clear the SYNC-FREQ Condition

Step 1 Use an optical test set to verify the timing frequency of the line or BITS timing source and ensure that it falls within the proper frequency. For specific procedures to use the test set equipment, consult the manufacturer.

For BITS, the proper timing frequency range is approximately –15 PPM to 15 PPM. For optical line timing, the proper frequency range is approximately –16 PPM to 16 PPM.

Step 2 If the reference source frequency is not outside of bounds, complete the "Physically Replace a Traffic Card" procedure on page 2-243 for the TCC2/TCC2P.

Note It takes up to 30 minutes for the TCC2/TCC2P to transfer the system software to the newly installed TCC2/TCC2P. Software transfer occurs in instances where different software versions exist on the two cards. When the transfer completes, the active TCC2/TCC2P reboots and goes into standby mode after approximately three minutes.

Step 3 If the SYNC-FREQ condition continues to report after replacing the TCC2/TCC2P, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.358 SYNCLOSS

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Object: FCMR

DWDM Logical Objects: FC, GE, ISC, TRUNK

The Loss of Synchronization on Data Interface alarm is raised on FC_MR-4 client ports and MXP cards client or trunk ports when there is a loss of signal synchronization on the port. This alarm is demoted by the SIGLOSS alarm.

Clear the SYNCLOSS Alarm

Step 1 Ensure that the data port connection at the near end of the SONET link is operational.

Step 2 Verify fiber continuity to the port. To do this follow site practices.

Step 3 View the physical port LED to determine whether the alarm has cleared:

- If the LED is green, the alarm has cleared.
- If the port LED is clear (that is, not illuminated green), the link is not connected and the alarm has not cleared.
- If the LED is red, this indicates that the fiber is pulled.

Step 4 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) to report a service-affecting problem.

2.8.359 SYNCPRI

Default Severity: Minor (MN), Non-Service-Affecting (NSA) for EXT-SREF

SONET Logical Objects: EXT-SREF, NE-SREF

A Loss of Timing on Primary Reference alarm occurs when the ONS 15454 loses the primary timing source (reference 1). The ONS 15454 uses three ranked timing references. The timing references are typically two BITS-level or line-level sources and an internal reference. If SYNCPRI occurs, the ONS 15454 should switch to its secondary timing source (reference 2). Switching to the secondary timing source also triggers the "SWTOSEC" alarm on page 2-210.

Note The SYNCPRI alarm will be escalated to Major (MJ), Service-Affecting if no other valid references (SYNCSEC, SYNCTHIRD) are available. If any other reference are available then SYNCPRI gets raised as Minor (MN), non service affecting.

Clear the SYNCPRI Alarm

Step 1 In node view, click the **Provisioning > Timing > General** tabs.

Step 2 Verify the current configuration for REF-1 of the NE Reference.

Step 3 If the primary timing reference is a BITS input, complete the "Clear the LOS (BITS) Alarm" procedure on page 2-141.

Step 4 If the primary reference clock is an incoming port on the ONS 15454, complete the "Clear the LOS (OCN) Alarm" procedure on page 2-148.

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).

2.8.360 SYNCSEC

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Objects: EXT-SREF, NE-SREF

A Loss of Timing on Secondary Reference alarm occurs when the ONS 15454 loses the secondary timing source (reference 2). If SYNCSEC occurs, the ONS 15454 should switch to a third timing source (reference 3) to obtain valid timing for the ONS 15454. Switching to a third timing source also triggers the "SWTOTHIRD" alarm on page 2-210.

Note The SYNCPRI alarm will be escalated to Major (MJ), Service-Affecting if no other valid references (SYNCSEC, SYNCTHIRD) are available. If any other reference are available then SYNCPRI gets raised as Minor (MN), non service affecting.

Clear the SYNCSEC Alarm

Step 1 In node view, click the **Provisioning > Timing > General** tabs.

Step 2 Verify the current configuration of REF-2 for the NE Reference.

Step 3 If the secondary reference is a BITS input, complete the "Clear the LOS (BITS) Alarm" procedure on page 2-141.

Step 4 Verify that the BITS clock is operating properly.

Step 5 If the secondary timing source is an incoming port on the ONS 15454, complete the "Clear the LOS (OCN) Alarm" procedure on page 2-148.

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).

2.8.361 SYNCTHIRD

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Objects: EXT-SREF, NE-SREF

A Loss of Timing on Third Reference alarm occurs when the ONS 15454 loses the third timing source (reference 3). If SYNCTHIRD occurs and the ONS 15454 uses an internal reference for source three, the TCC2/TCC2P could have failed. The ONS 15454 often reports either the "FRNGSYNC" condition on page 2-105 or the "HLDOVRSYNC" condition on page 2-116 after a SYNCTHIRD alarm.

Note The SYNCPRI alarm will be escalated to Major (MJ), Service-Affecting if no other valid references (SYNCSEC, SYNCTHIRD) are available. If any other reference are available then SYNCPRI gets raised as Minor (MN), non service affecting.

Clear the SYNCTHIRD Alarm

Step 1 In node view, click the **Provisioning > Timing > General** tabs.

Step 2 Verify that the current configuration of REF-3 for the NE Reference. For more information about references, refer to the "Timing" chapter in the *Cisco ONS 15454 Reference Manual*.

Step 3 If the third timing source is a BITS input, complete the "Clear the LOS (BITS) Alarm" procedure on page 2-141.

Step 4 If the third timing source is an incoming port on the ONS 15454, complete the "Clear the LOS (OCN) Alarm" procedure on page 2-148.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 5 If the third timing source uses the internal ONS 15454 timing, complete the "Reset an Active TCC2/TCC2P Card and Activate the Standby Card" procedure on page 2-240.

Wait ten minutes to verify that the card you reset completely reboots and becomes the standby card.

Step 6 If the reset card has not rebooted successfully, or the alarm has not cleared, call Cisco TAC (1 800 553-2447). If the Cisco TAC technician tells you to reseat the card, complete the "Remove and Reinsert (Reseat) the Standby TCC2/TCC2P Card" procedure on page 2-241. If the Cisco TAC technician tells you to remove the card and reinstall a new one, follow the "Physically Replace a Traffic Card" procedure on page 2-243.

2.8.362 SYSBOOT

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Object: NE

The System Reboot alarm indicates that new software is booting on the TCC2/TCC2P. No action is required. The alarm clears when all cards finish rebooting the new software. The reboot takes up to 30 minutes.

If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

Note SYSBOOT is an informational alarm. It only requires troubleshooting if it does not clear.

2.8.363 TEMP-MISM

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: NE

Temperature Reading Mismatch Between Control Cards is raised when the temperature readings on the two TCC2/TCC2Ps are out of range of each other by more than some predefined difference (such as 5 degrees C). A message containing power monitoring and temperature information is exchanged between the two TCC2/TCC2Ps, allowing the values to be compared. The temperature of each TCC2/TCC2P is read from a system variable.

This condition can be caused by a clogged fan filter or by fan tray stoppage.

Clear the TEMP-MISM Condition

Step 1 Complete the "Inspect, Clean, and Replace the Reusable Air Filter" procedure on page 2-247.

Step 2 If the condition does not clear, complete the "Remove and Reinsert a Fan-Tray Assembly" procedure on page 2-249.

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).

2.8.364 TIM

Default Severity: Critical (CR), Service-Affecting (SA)

SONET Logical Object: OCN

DWDM Logical Object: TRUNK

The Section TIM alarm occurs when the expected J0 section trace string does not match the received section trace string. This occurs because the data being received is not correct, and the receiving port could not be connected to the correct transmitter port.

If the alarm occurs on a port that has been operating with no alarms, the circuit path has changed due to a fibering misconnection, a TL1 routing change, or to someone entering an incorrect value in the Current Transmit String field.

TIM occurs on a port that has previously been operating without alarms if someone switches optical fibers that connect the ports. TIM is usually accompanied by other alarms, such as the "LOS (OCN)" alarm on page 2-147 or the "UNEQ-P" alarm on page 2-223. If these alarms accompany a TIM alarm, reattach or replace the original cables/fibers to clear the alarms. If a Transmit or Expected String was changed, restore the original string.

Clear the TIM Alarm

Step 1 Ensure that the physical fibers are correctly configured and attached. To do this, consult site documents. For more information about cabling the ONS 15454, refer to the "Install Cards and Fiber-Optic Cable" chapter in the *Cisco ONS 15454 Procedure Guide*.

Step 2 If the alarm does not clear, you can compare the J0 expected and transmitted strings and, if necessary, change them:

- **a.** Log into the circuit source node and click the **Circuits** tab.
- **b.** Select the circuit reporting the condition, then click **Edit**.
- **c.** In the Edit Circuit window, check the **Show Detailed Circuit Map** check box and click **Apply**.
- **d.** On the detailed circuit map, right-click the source circuit port and choose **Edit J0 Path Trace (port)** from the shortcut menu.
- **e.** Compare the Current Transmit String and the Current Expected String entries in the Edit J0 Path Trace dialog box.
- **f.** If the strings differ, correct the Transmit or Expected strings and click **Apply**.
- **g.** Click **Close**.

Step 3 If the alarm does not clear, ensure that the signal has not been incorrectly routed. (Although the ONS 15454 routes circuits automatically, the circuit route could have been changed using TL1.) If necessary, manually correct the routing using TL1. For instructions, refer to the *Cisco ONS SONET TL1 Reference Guide* and the *Cisco SONET TL1 Command Guide* .

Step 4 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem if necessary.

2.8.365 TIM-MON

Default Severity: Minor (MN), Non-Service-Affecting (NSA)

SONET Logical Objects: OCN

DWDM Logical Object: TRUNK

The TIM Section Monitor TIM alarm is similar to the "TIM-P" alarm on page 2-216, but it applies to TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, and MXP_2.5G_10G cards when they are configured in transparent mode. (In transparent termination mode, all SONET overhead bytes are passed through from client ports to the trunk ports or from trunk ports to client ports.)

Note For more information about MXP and TXP cards, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Clear the TIM-MON Alarm

Step 1 Complete the "Clear the TIM-P Alarm" procedure on page 2-217.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.366 TIM-P

Default Severity: Critical (CR), Service-Affecting (SA) for STSTRM; Default Severity: Minor (MN), Non-Service-Affecting (NSA) for STSMON

SONET Logical Objects: STSMON, STSTRM

The TIM Path alarm occurs when the expected path trace string does not match the received path trace string. Path Trace Mode must be set to Manual or Auto for the TIM-P alarm to occur.

In manual mode at the Path Trace window, the user types the expected string into the Current Expected String field for the receiving port. The string must match the string typed into the Transmit String field for the sending port. If these fields do not match, the login node raises the TIM-P alarm. In Auto mode on the receiving port, the card sets the expected string to the value of the received string. If the alarm occurs on a port that has been operating with no alarms, the circuit path has changed or someone entered a new incorrect value into the Current Transmit String field. Complete the following procedure to clear either instance.

Clear the TIM-P Alarm

Step 1 Complete the "Clear the TIM Alarm" procedure on page 2-215. (The option will say "Edit J1 Path Trace" rather than "Edit J0 Path Trace.")

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). If the alarm applies to the STSTRM object, it is Service-Affecting (SA).

2.8.367 TIM-S

Default Severity: Critical (CR), Service-Affecting (SA)

SONET Logical Objects: EC1, OCN

The TIM for Section Overhead alarm occurs when there is a mismatch between the expected and received J0 section overhead strings in either Manual or Auto mode.

In manual mode at the DS3/EC1-48 card Section Trace window, the user enters the expected string into the Current Expected String field for the receiving port. The string must match the string typed into the Transmit String field for the sending port. If these fields do not match, the login node raises the TIM-S alarm.

In Auto mode on the receiving port, the card sets the expected string to the value of the received string. If the alarm occurs on a port that has been operating with no alarms, the circuit path has changed or someone entered a new incorrect value into the Current Transmit String field. Complete the following procedure to clear either problem.

TIM-S also occurs on a port that has previously been operating without alarms if someone switches the cables or optical fibers that connect the ports. If TIM-S is enabled on the port, the "AIS-L" alarm on page 2-32 can be raised downstream and the "RFI-L" alarm on page 2-184 can be raised upstream.

Note AIS-L and RFI-L are disabled or enabled in the **Provisioning > EC1 > Section Trace** tab **Disable AIS/RDI on TIM-S?** check box.

Clear the TIM-S Alarm

Step 1 Double-click the DS3/EC1-48 card to open the card view.

Step 2 Click the **Provisioning > EC1 > Section Trace** tabs.

Step 3 Choose the port from the **Port** pull-down.

Step 4 In the Expected area, enter the correct string into the **Current Expected String** field.

Step 5 Click **Apply**.

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). If the alarm applies to the STSTRM object, it is Service-Affecting (SA).

2.8.368 TIM-V

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Object: VT-TERM

The VT Path TIM alarm is raised on VT terminations when the J2 path trace is enabled and is mismatched with the expected trace string.

Clear the TIM-V Alarm

Step 1 Complete the "Clear the TIM Alarm" procedure on page 2-215.

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 problem.

2.8.369 TPTFAIL (CE100T)

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Object: CE100T

The Transport (TPT) Layer Failure alarm for the CE-100T-8 card indicates a break in the end-to-end Ethernet link integrity feature of the ONS 15454 CE-100T-8 card. TPTFAIL indicates a far-end condition and not a problem with the port reporting TPTFAIL. TPTFAIL may also occurs on local ports with LCAS-enabled CE-100T-8 cards.

Note For more information about Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.*

Clear the TPTFAIL (CE100T) Alarm

Step 1 Complete the "Clear the TPTFAIL (G1000) Alarm" procedure on page 2-219.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) to report a Service-Affecting (SA) problem.

2.8.370 TPTFAIL (FCMR)

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Object: FCMR

The Transport Fail alarm is raised against a local Fibre Channel (FC) port on an FC_MR-4 card when the port receives another SONET error such as AIS-P, LOP-P, UNEQ-P, PLM-P, TIM-P, LOM (for VCAT only), or SQM (for VCAT only).

This TPTFAIL can be raised against Fibre Channel cards if the remote FC card port is down from SIGLOSS or SYNCLOSS. In that case, the remote FC card port sends a PDI-P error code in the SONET C2 byte and signals the local FC port transmitter to turn off (thus causing the local FC port to raise the TPTFAIL alarm). A TPTFAIL can also be raised when a far-end receive fiber is pulled. This alarm can be demoted when a facility loopback is placed on the FC_MR-4 port.

Clear the TPTFAIL (FCMR) Alarm

Step 1 Find and clear any path alarms applying to the port. Refer to the correct section of this chapter for trouble clearing instructions. Clearing the path alarm also clears the TPTFAIL.

Step 2 If the alarm does not clear, log into the 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.

2.8.371 TPTFAIL (G1000)

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Object: G1000

The Transport Layer Failure alarm for the G-Series Ethernet card indicates a break in the end-to-end Ethernet link integrity feature of the ONS 15454 G1000-4 cards. TPTFAIL indicates a far-end condition and not a problem with the port reporting TPTFAIL.

The TPTFAIL alarm indicates a problem on either the SONET path or the remote Ethernet port that prevents the complete end-to-end Ethernet path from working. If any SONET path alarms such as the "AIS-P" alarm on page 2-33, the "LOP-P" alarm on page 2-138, the "PDI-P" alarm on page 2-174, or the "UNEQ-P" alarm on page 2-223 exist on the SONET path used by the Ethernet port, the affected port causes a TPTFAIL alarm. Also, if the far-end G1000-4 port Ethernet port is administratively disabled or it is reporting the "CARLOSS (G1000)" alarm on page 2-56, the C2 byte in the SONET path overhead indicates the "PDI-P" alarm on page 2-174, which in turn causes a TPTFAIL to be reported against the near-end port.

When a TPTFAIL alarm occurs, the near-end port is automatically disabled (transmit laser turned off). In turn, the laser shutoff can also cause the external Ethernet device attached at the near end to detect a link down and turn off its transmitter. This also causes a CARLOSS alarm to occur on the reporting port. In all cases, the source problem is either in the SONET path being used by the G1000-4 port or the far-end G1000-4 port to which it is mapped.

An occurrence of TPTFAIL on an ONS 15454 G1000-4 port indicates either a problem with the SONET path that the port is using or with the far-end G1000-4 port that is mapped to the port.

Note For more information about Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.

Clear the TPTFAIL (G1000) Alarm

Step 1 Clear any alarms being reported by the OC-N card on the G1000-4 circuit.

Step 2 If no alarms are reported by the OC-N card, or if the "PDI-P" condition on page 2-174 is reported, the problem could be on the far-end G1000-4 port. Clear any alarms, such as CARLOSS, reported against the far-end port or card.

Step 3 If the alarm does not clear, log into the 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.

2.8.372 TPTFAIL (ML100T, ML1000, MLFX)

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Objects: ML100T, ML1000, MLFX

The TPT Layer Failure alarm for the ML-Series Ethernet card indicates a break in the end-to-end packet-over-SONET (POS) link integrity feature of the ML-Series POS cards. TPTFAIL indicates a far-end condition or misconfiguration of the POS port.

The TPTFAIL alarm indicates a problem on the SONET path, a problem on the remote POS port, or a misconfiguration of the POS port that prevents the complete end-to-end POS path from working. If any SONET path alarms such as the "AIS-P" condition on page 2-33, the "LOP-P" alarm on page 2-138, the "PDI-P" condition on page 2-174, or the "UNEQ-P" alarm on page 2-223 exist on the circuit used by the POS port, the affected port could report a TPTFAIL alarm. If the far-end ML POS port is administratively disabled, it inserts an "AIS-P" condition on page 2-33 that is detected by the near-end port. The near-end port could report TPTFAIL in this event. If the POS port is misconfigured at the Cisco IOS CLI level, the misconfiguration causes the port to go down and report TPTFAIL.

Note For more information about the ML-Series Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.*

Clear the TPTFAIL (ML100T, ML1000, MLFX) Alarm

Step 1 If there are no SONET alarms reported against the POS port circuit, verify that both POS ports are properly configured. Refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327* for configuration information.

Step 2 If the "PLM-P" alarm on page 2-176 is the only one reported against the POS port circuit, verify that both POS ports are properly configured. Refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327* for configuration information.

Step 3 If the "PDI-P" condition on page 2-174 is the only one reported against the POS port circuit and the circuit is terminated by a G-Series card, determine whether a "CARLOSS (G1000)" alarm on page 2-56 is reported against the G-Series card, and if so, complete the "Clear the CARLOSS (G1000) Alarm" procedure on page 2-57.

Step 4 If the "AIS-P" alarm on page 2-33, the "LOP-P" alarm on page 2-138, or the "UNEQ-P" alarm on page 2-223 is present, clear those alarms using the procedures in those sections.

Step 5 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

2.8.373 TRMT

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Objects: DS1, E1

A Missing Transmitter alarm occurs when there is a transmit failure on the ONS 15454 DS-1 card because of an internal hardware failure. The card must be replaced.

Clear the TRMT Alarm

Step 1 Complete the "Physically Replace a Traffic Card" procedure on page 2-243 for the reporting DS-1 card.

Step 2 If the alarm does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447) in order to report a Service-Affecting (SA) problem.

2.8.374 TRMT-MISS

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Objects: DS1, E1

A Facility Termination Equipment Transmitter Missing alarm occurs when the facility termination equipment detects an incorrect amount of impedance on its backplane connector. Incorrect impedance is detected when a transmit cable is missing on the DS-1 port or the backplane does not match the inserted card. For example, an SMB connector or a BNC connector could be connected to a DS-1 card instead of a DS-3 card.

Note DS-1s are four-wire circuits and need a positive and negative connection for both transmit and receive.

Clear the TRMT-MISS Alarm

Step 1 Verify that the device attached to the DS-1 port is operational.

Step 2 If the device is operational, verify that the cabling is securely connected.

Step 3 If the cabling is secure, verify that the pinouts are correct.

Step 4 If the pinouts are correct, replace the transmit cable.

Step 5 If the alarm does not clear, log into the 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.

2.8.375 TX-AIS

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

SONET Logical Objects: DS1, DS3, E1

The (TX) Transmit Direction AIS condition is raised by the ONS 15454 backplane when it receives a far-end DS-1 LOS.

Clear the TX-AIS Condition

Step 1 Determine whether there are alarms on the downstream nodes and equipment, especially the "LOS (OCN)" alarm on page 2-147, or OOS ports.

Step 2 Clear the downstream alarms using the applicable procedures in this chapter.

Step 3 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.376 TX-LOF

Default Severity: Not Reported (NR), Non-Service-Affecting (NSA)

SONET Logical Objects: DS1, E1

The Transmit Direction LOF condition is transmitted by the backplane when it receives a DS-1 TX-LOF.

This alarm is raised only at the transmit (egress) side.

Clear the TX-LOF Condition

Step 1 Complete the "Clear the LOF (DS1) Alarm" procedure on page 2-132.

Step 2 If the condition does not clear, log into the Technical Support Website at http://www.cisco.com/techsupport for more information or call Cisco TAC (1 800 553-2447).

2.8.377 TX-RAI

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: DS1, DS3, E1

The Transmit Direction RAI condition is transmitted by the backplane when it receives a DS-1 TX-AIS. This alarm is raised only at the transmit side, but RAI is raised at both ends.

Clear the TX-RAI Condition

Step 1 Complete the "Clear the TX-AIS Condition" procedure on page 2-222.

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).

2.8.378 UNC-WORD

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.379 UNEQ-P

Default Severity: Critical (CR), Service-Affecting (SA)

SONET Logical Objects: STSMON, STSTRM

An SLMF UNEQ Path alarm occurs when the path does not have a valid sender. The UNEQ-P indicator is carried in the C2 signal path byte in the SONET overhead. The source of the problem is the node that is transmitting the signal into the node reporting the UNEQ-P.

The alarm could result from a PARTIAL circuit or an empty VT tunnel. UNEQ-P occurs in the node that terminates a path.

Note If a newly created circuit has no signal, a UNEQ-P alarm is reported on the OC-N cards and the "AIS-P" condition on page 2-33 is reported on the terminating cards. These alarms clear when the circuit carries a signal.

Caution Deleting a circuit affects traffic.

Clear the UNEQ-P Alarm

Step 1 In node view, choose **Go to Network View** from the View menu.

Step 2 Right-click the alarm to display the Select Affected Circuits shortcut menu.

Step 3 Click **Select Affected Circuits**.

Step 4 When the affected circuits appear, look in the Type column for VTT, which indicates a VT tunnel circuit. A VT tunnel with no VTs assigned could be the cause of an UNEQ-P alarm.

Step 5 If the Type column does not contain VTT, there are no VT tunnels connected with the alarm. Go to Step 7.

Step 6 If the Type column does contain VTT, attempt to delete these rows:

Note The node does not allow you to delete a valid VT tunnel or one with a valid VT circuit inside.

a. Click the VT tunnel circuit row to highlight it. Complete the "Delete a Circuit" procedure on page 2-244.

b. If an error message dialog box appears, the VT tunnel is valid and not the cause of the alarm.

c. If any other rows contain VTT, repeat Step 6.

Step 7 If all nodes in the ring appear in the CTC network view, determine whether the circuits are complete:

a. Click the **Circuits** tab.

b. Verify that PARTIAL is not listed in the Status column of any circuits.

Step 8 If you find circuits listed as PARTIAL, use an optical test set to verify that these circuits are not working circuits that continue to pass traffic. For specific procedures to use the test set equipment, consult the manufacturer.

Step 9 If the PARTIAL circuits are not needed or are not passing traffic, delete the PARTIAL circuits.

Complete the "Delete a Circuit" procedure on page 2-244.

Step 10 Recreate the circuit with the correct circuit size. Refer to the "Create Circuits and VT Tunnels" chapter in the *Cisco ONS 15454 Procedure Guide*.

Step 11 Log back in and verify that all circuits terminating in the reporting card are active:

a. Click the **Circuits** tab.

b. Verify that the **Status** column lists all circuits as active.

Step 12 If the alarm does not clear, clean the far-end optical fiber according to site practice. If no site practice exists, complete the procedure in the "Maintain the Node" chapter of the *Cisco ONS 15454 Procedure Guide*.

Warning **On the OC-192 card, the laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. The laser is off when the safety key is off (labeled 0).** Statement 293

Warning **Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard.** Statement 1056

Warning **Use of controls, adjustments, or performing procedures other than those specified could result in hazardous radiation exposure.** Statement 1057

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 13 If the alarm does not clear, complete the "Physically Replace a Traffic Card" procedure on page 2-243 for the OC-N and electrical cards.

Step 14 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.

2.8.380 UNEQ-V

Default Severity: Major (MJ), Service-Affecting (SA)

SONET Logical Objects: VT-MON, VT-TERM

An SLMF UNEQ VT alarm indicates that the node is receiving SONET path overhead with Bits 5, 6, and 7 of the V5 overhead byte all set to zeroes. The source of the problem is not the node raising the alarm, but the node transmitting the VT signal to it. The V in UNEQ-V indicates that the failure has occurred at the VT layer.

Warning **On the OC-192 card, the laser is on when the card is booted and the safety key is in the on position (labeled 1). The port does not have to be in service for the laser to be on. The laser is off when the safety key is off (labeled 0).** Statement 293.

Warning **Invisible laser radiation could be emitted from the end of the unterminated fiber cable or connector. Do not stare into the beam directly with optical instruments. Viewing the laser output with certain optical instruments (for example, eye loupes, magnifiers, and microscopes) within a distance of 100 mm could pose an eye hazard.** Statement 1056

Warning **Use of controls, adjustments, or performing procedures other than those specified could result in hazardous radiation exposure.** Statement 1057

Clear the UNEQ-V Alarm

Step 1 Complete the "Clear the UNEQ-P Alarm" procedure on page 2-223.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. 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, 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.

2.8.381 UNREACHABLE-TARGET-POWER

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.382 UT-COMM-FAIL

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.383 UT-FAIL

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.384 VCG-DEG

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: VCG

The VCAT Group Degraded alarm is a VCAT group alarm. (VCATs are groups of independent circuits that are concatenated from different time slots into higher-rate signals.) The alarm occurs when one member circuit carried by the ML-Series Ethernet card is down. This alarm is accompanied by the "OOU-TPT" alarm on page 2-171. It only occurs when a Critical (CR) alarm, such as LOS, causes a signal loss.

Note For more information about Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.

Clear the VCG-DEG Condition

Step 1 Look for and clear any Critical (CR) alarms that apply to the errored card, such as the "LOS (2R)" alarm on page 2-140 or "LOS (OTS)" alarm on page 2-149.

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).

2.8.385 VCG-DOWN

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: VCG

The VCAT Group Down alarm is a VCAT group alarm. (VCATs are groups of independent circuits that are concatenated from different time slots into higher-rate signals.) The alarm occurs when both member circuits carried by the ML-Series Ethernet card are down. This alarm occurs in conjunction with another Critical (CR) alarm, such as the "LOS (2R)" alarm on page 2-140.

Note For more information about Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327*.

Clear the VCG-DOWN Condition

Step 1 Complete the "Clear the VCG-DEG Condition" procedure on page 2-226.

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).

2.8.386 VOA-HDEG

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.387 VOA-HFAIL

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.388 VOA-LDEG

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.389 VOA-LFAIL

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.8.390 VOLT-MISM

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Object: PWR

The Power Monitoring Mismatch Between Control Cards alarm is raised against the shelf when the power voltages of both TCC2/TCC2Ps are out of range of each other by more than 5 VDC.

Clear the VOLT-MISM Condition

Step 1 Check the incoming voltage level to the shelf using a voltmeter. Follow site practices or refer to the "Install the Shelf and Backplane Cable" chapter in the *Cisco ONS 15454 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).

2.8.391 WKSWPR

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: EQPT, OCN, STSMON, VT-MON

DWDM Logical Objects: 2R, ESCON, FC, GE, ISC, TRUNK

The Working Switched To Protection condition occurs when a line experiences the "LOS (OCN)" alarm on page 2-147, the "SD (DS1, DS3)" condition on page 2-190, or the "SD (TRUNK)" condition on page 2-193.

This condition is also raised when you use the FORCE SPAN, FORCE RING 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 LOS (OCN) Alarm" procedure on page 2-148.

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).

2.8.392 WTR

Default Severity: Not Alarmed (NA), Non-Service-Affecting (NSA)

SONET Logical Objects: EQPT, OCN, STSMON, VT-MON

DWDM Logical Objects: 2R, ESCON, FC, GE, ISC, TRUNK

The Wait To Restore condition occurs when the "WKSWPR" condition on page 2-228 is raised, but the wait-to-restore time has not expired, meaning that the active protect path cannot revert to the working path. The condition clears when the timer expires and traffic switches back to the working path.

Caution DS-1 traffic loss can occur on a DS-1 with 1:N protection if a DS-1 card is reset with the protect card in the WTR state.

Note WTR is an informational condition and does not require troubleshooting.

2.8.393 WVL-MISMATCH

For information about this alarm or condition, refer to the "Alarm Troubleshooting" chapter in the *Cisco ONS 15454 DWDM Troubleshooting Guide*. This guide discusses all DWDM alarms.

2.9 Traffic Card LED Activity

ONS 15454 traffic card LED behavior patterns are listed in the following sections. These sections give behavior for card insertion, reset, and side-switch.

2.9.1 Typical Traffic Card LED Activity After Insertion

When a non-DWDM card is inserted, the following LED activities occur:

1. The red FAIL LED turns on and remains illuminated for 20 to 30 seconds.
2. The red FAIL LED blinks for 35 to 45 seconds.
3. All LEDs blink once and turn off for 5 to 10 seconds.
4. The ACT or ACT/SBY LED turns on. The SF LED can persist until all card ports connect to their far-end counterparts and a signal is present.

2.9.2 Typical Traffic Card LED Activity During Reset

While a non-DWDM card resets, the following LED activities occur:

1. The FAIL LED on the physical card blinks and turns off.
2. The white LED with the letters "LDG" appears on the reset card in CTC.
3. The green ACT LED appears in CTC.

2.9.3 Typical Card LED State After Successful Reset

When a non-DWDM card successfully resets, the following LED states are present:

- If you are looking at the physical ONS 15454, the ACT/SBY LED is illuminated.
- If you are looking at node view of the ONS 15454, the current standby card has an amber LED depiction with the initials "SBY," and this has replaced the white "LDG" depiction on the card in CTC.
- If you are looking at node view of the ONS 15454, the current active card has a green LED depiction with the initials "ACT," and this has replaced the white "LDG" depiction on the card in CTC.

2.9.4 Typical Cross-Connect LED Activity During Side Switch

While an XC10G card is switched in CTC from active (ACT) to standby (SBY) or from SBY to ACT, the following LED activities occur:

1. The FAIL LED on the physical card blinks and turns off.

2. The standby card yellow SBY LED becomes a green ACT LED, indicating it is now active.
3. The active card green ACT LED becomes a yellow SBY LED, indicating it is now standby.

2.10 Frequently Used Alarm Troubleshooting Procedures

This section gives common procedures that are frequently used when troubleshooting alarms. Most of these procedures are summarized versions of fuller procedures existing elsewhere in the ONS 15454 documentation. They are included in this chapter for the user's convenience. For further information, please refer to the *Cisco ONS 15454 Procedure Guide*.

2.10.1 Node and Ring Identification, Change, Visibility, and Termination

The following procedures relate how to identify or change BLSR names and node IDs, and how to verify visibility from other nodes.

Identify a BLSR Ring Name or Node ID Number

Step 1 Log into a node on the network.

Step 2 In node view, choose **Go to Network View** from the View menu.

Step 3 Click the **Provisioning > BLSR** tabs.

Step 4 From the Ring Name column, record the ring name, or in the Nodes column, record the Node IDs in the BLSR. The Node IDs are the numbers in parentheses next to the node name.

Change a BLSR Ring Name

Step 1 Log into a node on the network.

Step 2 In node view, choose **Go to Network View** from the View menu.

Step 3 Click the **Provisioning > BLSR** tabs.

Step 4 Highlight the ring and click **Edit**.

Step 5 In the BLSR window, enter the new name in the Ring Name field.

Step 6 Click **Apply**.

Step 7 Click **Yes** in the Changing Ring Name dialog box.

Change a BLSR Node ID Number

Step 1 Log into a node on the network.

Step 2 In node view, choose **Go to Network View** from the View menu.

Step 3 Click the **Provisioning > BLSR** tabs.

Step 4 Highlight the ring and click **Edit**.

Step 5 In the BLSR window, right-click the node on the ring map.

Step 6 Select **Set Node ID** from the shortcut menu.

Step 7 In the Edit Node ID dialog box, enter the new ID. The Node ID is the number in parentheses after the Node Name.

Step 8 Click **OK**.

Verify Node Visibility for Other Nodes

Step 1 Log into a node on the network.

Step 2 In node view, click the **Provisioning > BLSR** tabs.

Step 3 Highlight a BLSR.

Step 4 Click **Ring Map**.

Step 5 In the BLSR Ring Map window, verify that each node in the ring appears on the ring map with a node ID and IP address.

Step 6 Click **Close**.

2.10.2 Protection Switching, Lock Initiation, and Clearing

The following sections give instructions for port, ring, and span switching and switch-clearing commands, as well as lock-ons and lockouts.

Initiate a 1+1 Protection Port Force Switch Command

This procedure switches 1+1 protection group traffic from one port in the group to the other using a Force switch.

Caution The Force command overrides normal protective switching mechanisms. Applying this command incorrectly can cause traffic outages.

Caution Traffic is not protected during a Force protection switch.

Note A Force command switches traffic on a working path even if the path has signal degrade (SD) or signal fail (SF) conditions. A Force switch does not switch traffic on a protect path. A Force switch preempts a Manual switch.

Step 1 In node view, click the **Maintenance > Protection** tabs.

Step 2 In the Protection Groups area, select the protection group with the port you want to switch.

Step 3 In the Selected Groups area, select the port belonging to the card you are replacing. You can carry out this command for the working or protect port. For example, if you need to replace the card with the Protect/Standby port, click this port.

Step 4 In the Switch Commands area, click **Force**.

Step 5 Click **Yes** in the Confirm Force Operation dialog box.

Step 6 If the switch is successful, the group says "Force to working" in the Selected Groups area.

Initiate a 1+1 Manual Switch Command

This procedure switches 1+1 protection group traffic from one port in the group to the other using a Manual switch.

Note A Manual command switches traffic if the path has an error rate less than the signal degrade. A Manual switch is preempted by a Force switch.

Step 1 In node view, click the **Maintenance > Protection** tabs.

Step 2 In the Protection Groups area, select the protection group with the port you want to switch.

Step 3 In the Selected Groups area, select the port belonging to the card you are replacing. You can carry out this command for the working or protect port. For example, if you need to replace the card with the protect/standby port, click this port.

Step 4 In the Switch Commands area, click **Manual**.

Step 5 Click **Yes** in the Confirm Force Operation dialog box.

Step 6 If the switch is successful, the group now says "Manual to working" in the Selected Groups area.

Clear a 1+1 Force or Manual Switch Command

Note If the 1+1 protection group is configured as revertive, clearing a Force switch to protect (or working) moves traffic back to the working port. In revertive operation, the traffic always switches back to working. There is no revert to the protect. If ports are not configured as revertive, clearing a Force switch to protect does not move traffic back.

Note If the Force Switch was user-initiated, the reversion occurs immediately when the clear command is issued. The five-minute WTR period is not needed in this case. If the Force was system-initiated, allow the five-minute waiting period (during WTR) before the reversion occurs.

Step 1 In node view, click the **Maintenance > Protection** tabs.

Step 2 In the Protection Groups area, choose the protection group containing the port you want to clear.

Step 3 In the Selected Group area, choose the port you want to clear.

Step 4 In the Switching Commands area, click **Clear**.

Step 5 Click **Yes** in the Confirmation Dialog box.

The Force switch is cleared. Traffic immediately reverts to the working port if the group was configured for revertive switching.

Initiate a Lock-On Command

Note For 1:1 and 1:N electrical protection groups, working or protect cards can be placed in the Lock On state. For a 1+1 optical protection group, only the working port can be placed in the Lock On state.

Step 1 In node view, click the **Maintenance > Protection** tabs.

Step 2 In the Protection Groups list, click the protection group where you want to apply a lock-on.

Step 3 If you determine that the protect card is in standby mode and you want to apply the lock-on to the protect card, make the protect card active if necessary:

a. In the Selected Group list, click the protect card.

b. In the Switch Commands area, click **Force**.

Step 4 In the Selected Group list, click the active card where you want to lock traffic.

Step 5 In the Inhibit Switching area, click **Lock On**.

Step 6 Click **Yes** in the confirmation dialog box.

Initiate a Card or Port Lockout Command

Note For 1:1 or 1:N electrical protection groups, working or protect cards can be placed in the Lock Out state. For a 1+1 optical protection group, only the protect port can be placed in the Lock Out state.

Step 1 In node view, click the **Maintenance > Protection** tabs.

Step 2 In the Protection Groups list, click the protection group that contains the card you want to lockout.

Step 3 In the Selected Group list, click the card where you want to lock out traffic.

Step 4 In the Inhibit Switching area, click **Lock Out**.

Step 5 Click **Yes** in the confirmation dialog box.

The lockout has been applied and traffic is switched to the opposite card.

Clear a Lock-On or Lockout Command

Step 1 In node view, click the **Maintenance > Protection** tabs.

Step 2 In the Protection Groups list, click the protection group that contains the card you want to clear.

Step 3 In the Selected Group list, click the card you want to clear.

Step 4 In the Inhibit Switching area, click **Unlock**.

Step 5 Click **Yes** in the confirmation dialog box.

The lock-on or lockout is cleared.

Initiate a 1:1 Card Switch Command

Note The Switch command only works on the Active card, whether it is working or protect. It does not work on the Standby card.

Step 1 In node view, click the **Maintenance > Protection** tabs.

Step 2 Click the protection group that contains the card you want to switch.

Step 3 Under Selected Group, click the active card.

Step 4 Next to Switch Commands, click **Switch**.

The working slot should change to Working/Active and the protect slot should change to Protect/Standby.

Initiate a Force Switch for All Circuits on a Path Protection Span

This procedure forces all circuits in a path protection from the working span to the protect. It is used to remove traffic from a card that originates or terminates path protection 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.

Step 2 In node view, choose **Go to Network View** from the View menu.

Step 3 Right-click a network span and choose **Circuits**.

The Circuits on Span dialog box shows the path protection circuits, including circuit names, locations, and a color code showing which circuits are active on the span.

Step 4 Click the **Perform UPSR span switching** field.

Step 5 Choose **Force Switch Away** from the drop-down list.

Step 6 Click **Apply**.

Step 7 In the Confirm UPSR 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 Path Protection Span

This procedure manually switches all circuits in a path protection from the working span to the protect. It is used to remove traffic from a card that originates or terminates path protection circuits.

Caution The Manual command does not override normal protective switching mechanisms.

Step 1 Log into a node on the network.

Step 2 Right-click a network span and choose **Circuits**.

The Circuits on Span dialog box shows the path protection circuits, including circuit names, locations, and a color code showing which circuits are active on the span.

Step 3 Click the **Perform UPSR span switching** field.

Step 4 Choose **Manual** from the drop-down list.

Step 5 Click **Apply**.

Step 6 In the Confirm UPSR 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 Lockout for All Circuits on a Protect Path Protection Span

This procedure prevents all circuits in a path protection working span from switching to the protect span. It is used to keep traffic off cards that originate or terminate path protection circuits.

Caution The Lock Out of Protect command does not override normal protective switching mechanisms.

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 Right-click a network span and choose **Circuits**.

The Circuits on Span dialog box shows the path protection circuits, including circuit names, locations, and a color code showing which circuits are active on the span.

Step 3 Click the **Perform UPSR span switching** field.

Step 4 Choose **Lock Out of Protect** from the drop-down list.

Step 5 Click **Apply**.

Step 6 In the Confirm UPSR 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 an External Switching Command on a Path Protection Span

Note If the ports terminating a span are configured as revertive, clearing a Force switch on a protect port moves traffic back to the working port. If ports are not configured as revertive, clearing a Force switch 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 path protection 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:

a. Click the **Perform UPSR span switching** field.

b. Choose **Clear** from the drop-down list.

c. Click **Apply**.

d. In the Confirm UPSR 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 a BLSR

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 > BLSR** tabs.

Step 4 Click the row of the BLSR you are switching, then click **Edit**.

Step 5 Right-click a BLSR 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 BLSR Operation dialog boxes that appear.

Initiate a Force Span Switch on a Four-Fiber BLSR

Step 1 Log into a node on the network.

Step 2 From the View menu choose **Go to Network View**.

Step 3 In network view, click the **Provisioning > BLSR** tabs.

Step 4 Click the row of the BLSR you are switching, then click **Edit**.

Step 5 Right-click a BLSR node west port and choose **Set West Protection Operation**.

Step 6 In the Set West Protection Operation dialog box, choose **Force Span** from the drop-down list.

Step 7 Click **OK**.

Step 8 Click **Yes** in the two Confirm BLSR Operation dialog boxes that appear.

Initiate a Manual Span Switch on a BLSR

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Click the **Provisioning > BLSR** tabs.

Step 3 Choose the BLSR and click **Edit**.

Step 4 Right-click the BLSR node channel (port) and choose **Set West Protection Operation** (if you chose a west channel) or **Set East Protection Operation** (if you chose an east channel).

Step 5 In the Set West Protection Operation dialog box or the Set East Protection Operation dialog box, choose **Manual Span** from the drop-down list.

Step 6 Click **OK**.

Step 7 Click **Yes** in the two Confirm BLSR Operation dialog boxes.

Initiate a Manual Ring Switch on a BLSR

Step 1 From the View menu, choose **Go to Network View**.

Step 2 Click the **Provisioning > BLSR** tabs.

Step 3 Choose the BLSR and click **Edit**.

Step 4 Right-click the BLSR node channel (port) and choose **Set West Protection Operation** (if you chose a west channel) or **Set East Protection Operation** (if you chose an east channel).

Step 5 In the Set West Protection Operation dialog box or the Set East Protection Operation dialog box, choose **Manual Ring** from the drop-down list.

Step 6 Click **OK**.

Step 7 Click **Yes** in the two Confirm BLSR Operation dialog boxes.

Initiate a Lockout on a BLSR Protect Span

Step 1 From the View menu choose **Go to Network View**.

Step 2 Click the **Provisioning > BLSR** tabs.

Step 3 Choose the BLSR and click **Edit**.

Step 4 Right-click the BLSR node channel (port) and choose **Set West Protection Operation** (if you chose a west channel) or **Set East Protection Operation** (if you chose an east channel).

Step 5 In the Set West Protection Operation dialog box or the Set East Protection Operation dialog box, choose **Lockout Protect Span** from the drop-down list.

Step 6 Click **OK**.

Step 7 Click **Yes** in the two Confirm BLSR Operation dialog boxes.

Initiate an Exercise Ring Switch on a BLSR

Step 1 Log into a node on the network.

Step 2 Click **View > Go to Network View**.

Step 3 Click the **Provisioning > BLSR** tabs.

Step 4 Click the row of the BLSR 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 BLSR Operation dialog box.

Initiate an Exercise Ring Switch on a Four Fiber BLSR

Step 1 Log into a node on the network.

Step 2 From the View menu, choose **Go to Network View**.

Step 3 Click the **Provisioning > BLSR** tabs.

Step 4 Click the row of the BLSR 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 BLSR Operation dialog box.

Clear a BLSR External Switching Command

Step 1 Log into a node on the network.

Step 2 From the View menu, choose **Go to Network View**.

Step 3 Click the **Provisioning > BLSR** tabs.

Step 4 Click the BLSR you want to clear.

Step 5 Right-click the west port of the BLSR node where you invoked the switch and choose **Set West Protection Operation**.

Step 6 In the Set West Protection Operation dialog box, choose **Clear** from the drop-down list.

Step 7 Click **OK**.

Step 8 Click **Yes** in the Confirm BLSR Operation dialog box.

2.10.3 CTC Card Resetting and Switching

This section gives instructions for resetting traffic cards, TCC2/TCC2Ps, and cross-connect cards.

Caution For TXP and MXP cards placed in a Y-cable protection group, do not perform a software reset on both cards simultaneously. Doing so will cause a traffic hit of more than one minute. For more information about Y-cable protection groups, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Caution Resetting the active card in a Y-cable group will cause a traffic outage if the standby card is down for any reason.

Note When an AIC-I card is rest in CTC, any subsequent user client operations (such as CTC or TL1 activity) is paused for approximately 5-10 seconds. The reset does not cause any conditions to be raised.

Note For more information about MXP and TXP cards, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

Reset a Traffic Card in CTC

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 In node view, position the cursor over the optical or electrical traffic card slot reporting the alarm.

Step 3 Right-click the card. Choose **Reset Card** from the shortcut menu.

Step 4 Click **Yes** in the Resetting Card dialog box.

Reset an Active TCC2/TCC2P Card and Activate the Standby Card

Caution Resetting an active TCC2/TCC2P can be service-affecting.

Note Before you reset the TCC2/TCC2P, you should wait at least 60 seconds after the last provisioning change you made to avoid losing any changes to the database.

Step 1 Log into a node on the network. If you are already logged in, continue with Step 2.

Step 2 Identify the active TCC2/TCC2P:

If you are looking at the physical ONS 15454 shelf, the ACT/SBY LED of the active card is green. The ACT/STBLY LED of the standby card is amber.

Step 3 Right-click the active TCC2/TCC2P in CTC.

Step 4 Choose **Reset Card** from the shortcut menu.

Step 5 Click **Yes** in the Confirmation Dialog box.

The card resets, the FAIL LED blinks on the physical card, and connection to the node is lost. CTC switches to network view.

Step 6 Verify that the reset is complete and error-free and that no new related alarms appear in CTC. For LED appearance, see the "2.9.3 Typical Card LED State After Successful Reset" section on page 2-229.

Step 7 Double-click the node and ensure that the reset TCC2/TCC2P is in standby mode and that the other TCC2/TCC2P is active. Verify the following:

- If you are looking at the physical ONS 15454 shelf, the ACT/SBY LED of the active card is green. The ACT/STBLY LED of the standby card is amber.
- No new alarms appear in the Alarms window in CTC.

Side Switch the Active and Standby Cross-Connect Cards

Caution The cross-connect card side switch is usually service-affecting.

Step 1 Log into a node on the network. For instructions regarding how to log into a node, refer *Cisco ONS 15454 Procedure Guide, Release 8.0*. If you are already logged in, continue with Step 2.

Step 2 Display node view.

Step 3 Determine the active or standby XC10G card.

The ACT/SBY LED of the active card is green. The ACT/SBY LED of the standby card is amber.

Note You can also position the cursor over the card graphic to display a popup identifying the card as active or standby.

Step 4 In node view, click the **Maintenance > Cross-Connect > Cards** tabs.

Step 5 Click **Switch**.

Step 6 Click **Yes** in the Confirm Switch dialog box. See the "2.9.4 Typical Cross-Connect LED Activity During Side Switch" section on page 2-229 for LED information.

Note During a maintenance side switch or soft reset of an active XC10G card, the 1+1 protection group might display a protection switch. To disallow the protection switch from being displayed, the protection group should be locked at the node where XC switch or soft reset of an active XC switch is in progress.

Caution Active cross connect (XC10G/XCVT) cards should not be physically removed.

The following rules must be followed for removing an Active Cross Connect Card (XC10G/XCVT):

If the active cross connect has to be removed, perform an XCVT/XC10G side switch to change the status of the card from active to standby and then remove the cross connect card once it goes back to standby.

OR

Perform a lockout on all circuits that originate from the node whose active cross connect card has to be removed (performing a lockout on all spans will also accomplish the same goal).

2.10.4 Physical Card Reseating, Resetting, and Replacement

This section gives instructions for physically reseating and replacing TCC2/TCC2P, cross-connect, and traffic cards.

Caution Do not physically replace a card without first making provisions to switch or move traffic to a different card or circuit. General procedures for this are located in the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-231. In-depth traffic switching procedures and information can be found in the "Maintain the Node" chapter of the *Cisco ONS 15454 Procedure Guide*.

Remove and Reinsert (Reseat) the Standby TCC2/TCC2P Card

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Caution Do not perform this action without the supervision and direction of Cisco TAC (1 800 553-2447).

Caution The TCC2/TCC2P reseat could be service-affecting. Refer to the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-231 for traffic-switching procedures.

Note Before you reset the TCC2/TCC2P, you should wait at least 60 seconds after the last provisioning change you made to avoid losing any changes to the database.

Note When a standby TCC2/TCC2P card is removed and reinserted (reseated), all three fan lights could momentarily turn on, indicating that the fans have also reset.

Step 1 Log into a node on the network.

Ensure that the TCC2/TCC2P you want to reseat is in standby mode. A standby card has an amber ACT/SBY (Active/Standby) LED illuminated.

Step 2 When the TCC2/TCC2P is in standby mode, unlatch both the top and bottom ejectors on the TCC2/TCC2P.

Step 3 Physically pull the card at least partly out of the slot until the lighted LEDs turn off.

Step 4 Wait 30 seconds. Reinsert the card and close the ejectors.

Note The TCC2/TCC2P requires several minutes to reboot and display the amber standby LED after rebooting. Refer to the *Cisco ONS 15454 Reference Manual* for more information about LED behavior during a card reboot.

Remove and Reinsert (Reseat) Any Card

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 1 Open the card ejectors.

Step 2 Slide the card halfway out of the slot along the guide rails.

Step 3 Slide the card all the way back into the slot along the guide rails.

Step 4 Close the ejectors.

Physically Replace a Traffic Card

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Caution Removing an active card can cause a traffic hit. To avoid this, perform an external switch if a switch has not already occurred. See the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-231 for commonly used traffic-switching procedures.

When you replace a card with the identical type of card, you do not need to make any changes to the database.

Step 1 Open the card ejectors.

Step 2 Slide the card out of the slot.

Step 3 Open the ejectors on the replacement card.

Step 4 Slide the replacement card into the slot along the guide rails.

Step 5 Close the ejectors.

Physically Replace an In-Service Cross-Connect Card

Caution The cross-connect reseat could be service-affecting. Refer to the "2.10.2 Protection Switching, Lock Initiation, and Clearing" section on page 2-231 for traffic-switching procedures prior to completing this procedure.

Note This procedure is placed in the chapter as a quick guide for the user's convenience. A more detailed procedure is located in the "Maintain the Node" chapter of the *Cisco ONS 15454 Procedure Guide*.

When you replace a card with the identical type of card, you do not need to make any changes to the database.

Step 1 Determine the active cross-connect card (XCVT/XC10G/XC-VXC-10G). The ACT/SBY LED of the active card is green. The ACT/SBY LED of the standby card is amber.

Note You can also place the cursor over the card graphic to display a popup identifying the card as active or standby.

Step 2 Switch the active cross-connect card to standby:

a. In the node view, click the **Maintenance > Cross-Connect** tabs.

b. Under Cross Connect Cards, choose **Switch**.

c. Click **Yes** in the Confirm Switch dialog box.

Note After the active cross-connect card becomes standby, the original standby slot becomes active. This causes the ACT/SBY LED to become green on the former standby card.

Step 3 Physically remove the new standby cross-connect card from the ONS 15454.

Note An improper removal (IMPROPRMVL) alarm is raised when a card reseat is performed, unless the card is first deleted in Cisco Transport Controller (CTC). The alarm clears after the card is replaced.

Step 4 Insert the replacement cross-connect card into the empty slot.

The replacement card boots up and becomes ready for service after approximately one minute.

2.10.5 Generic Signal and Circuit Procedures

This section gives instructions for verify BER thresholds, deleting circuits, provisioning SDCC terminations, and clearing loopbacks.

Verify the Signal BER Threshold Level

Step 1 Log into a node on the network.

Step 2 In node view, double-click the card reporting the alarm to open the card view.

Step 3 Click the **Provisioning > Line** tabs.

Step 4 Under the **SD BER** (or **SF BER**) column in the Provisioning window, verify that the cell entry is consistent with the originally provisioned threshold. The default setting is 1E-7.

Step 5 If the entry is consistent with the original provisioning, go back to your original procedure.

Step 6 If the entry is not consistent with what the system was originally provisioned for, click the cell to reveal the range of choices and click the original entry.

Step 7 Click **Apply**.

Delete a Circuit

Step 1 Log into a node on the network.

Step 2 In node view, click the **Circuits** tab.

Step 3 Click the circuit row to highlight it and click **Delete**.

Step 4 Click **Yes** in the Delete Circuits dialog box.

Verify or Create Node Section DCC Terminations

Note Portions of this procedure are different for ONS 15454 DWDM nodes.

Step 1 Log into a node on the network.

Step 2 In node view, click the **Provisioning > Comm Channels > SDCC** tab.

Step 3 View the Port column entries to see where terminations are present for a node. If terminations are missing, proceed to Step 4.

Step 4 If necessary, create a DCC termination:

- **a.** Click **Create**.
- **b.** In the Create SDCC Terminations dialog box, click the ports where you want to create the DCC termination. To select more than one port, press the Shift key.
- **c.** In the port state area, click the **Set to IS** radio button.
- **d.** Verify that the Disable OSPF on Link check box is unchecked.
- **e.** Click **OK**.

Clear an OC-N Card Facility or Terminal Loopback Circuit

Step 1 Log into a node on the network.

Step 2 Double-click the reporting card in CTC to open the card view.

Step 3 Click the **Maintenance > Loopback > Port** tabs.

Step 4 In the Loopback Type column, determine whether any port row shows a state other than None.

Step 5 If a row contains another state besides None, click in the column cell to display the drop-down list and select None.

Step 6 In the Admin State column, determine whether any port row shows a state other than IS.

Step 7 If a row shows a state other than IS, click in the column cell to display the drop-down list and select **IS**.

Step 8 Click **Apply**.

Clear an OC-N Card Cross-Connect (XC) Loopback Circuit

Step 1 Log into a node on the network.

Step 2 Double-click the reporting card in CTC to open the card view.

Step 3 Click the **Maintenance > Loopback > SONET STS** tabs.

Step 4 Uncheck the XC Loopback check box.

Step 5 Click **Apply**.

Clear a DS3XM-6, DS3XM-12, or DS3E-12 Card Loopback Circuit

Step 1 Log into a node on the network.

Step 2 Double-click the reporting card in CTC to open the card view.

Step 3 Click the **Maintenance > DS3** tabs or the **Maintenance > DS1** tabs.

Step 4 In the Loopback Type column, determine whether any port row shows a state other than None.

Step 5 If a row contains another state besides None, click in the column cell to display the drop-down list and select None.

Step 6 In the Admin State column, determine whether any port row shows a state other than IS.

Step 7 If a row shows a state other than IS, click in the column cell to display the drop-down list and select **IS**.

Step 8 Click **Apply**.

Clear Other Electrical Card, CE-100T-8, or Ethernet Card Loopbacks

Note This procedure does not apply to DS3XM-6 or DS3XM-12 cards.

Note For more information about Ethernet cards, refer to the *Ethernet Card Software Feature and Configuration Guide for the Cisco ONS 15454, Cisco ONS 15454 SDH, and Cisco ONS 15327.*

Step 1 Log into a node on the network.

Step 2 Double-click the reporting card in CTC to open the card view.

Step 3 Click the **Maintenance > Loopback** tabs.

Step 4 In the Loopback Type column, determine whether any port row shows a state other than None.

Step 5 If a row contains another state besides None, click in the column cell to display the drop-down list and select **None**.

Step 6 In the Admin State column, determine whether any port row shows a state other than IS.

Step 7 If a row shows a state other than IS, click in the column cell to display the drop-down list and select **IS**.

Step 8 Click **Apply**.

Clear an MXP, TXP, or FC_MR-4 Card Loopback Circuit

Step 1 Log into a node on the network.

Step 2 Double-click the reporting card in CTC to open the card view.

Step 3 Click the **Maintenance > Loopback** tabs.

Step 4 In the Loopback Type column, determine whether any port row shows a state other than None.

Step 5 If a row contains another state besides None, click in the column cell to display the drop-down list and select None.

Step 6 In the Admin State column, determine whether any port row shows an admin state other than IS, for example, OOS,MT.

Step 7 If a row shows an admin state other than IS, click in the column cell to display the drop-down list and select **IS**.

Step 8 Click **Apply**.

2.10.6 Air Filter and Fan Procedures

This section gives instructions for cleaning or replacing the air filter and reseating or replacing the fan tray assembly.

Inspect, Clean, and Replace the Reusable Air Filter

To complete this task, you need a vacuum cleaner or detergent and water faucet, a spare filter, and a pinned hex key.

Warning **Do not reach into a vacant slot or chassis while you install or remove a module or a fan. Exposed circuitry could constitute an energy hazard.** Statement 206

Although the filter works if it is installed with either side facing up, Cisco recommends that you install it with the metal bracing facing up to preserve the surface of the filter.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

Step 1 Verify that you are replacing a reusable air filter. The reusable filter is made of a gray, open-cell, polyurethane foam that is specially coated to provide fire and fungi resistance. NEBS 3E and later versions of the ONS 15454 use a reusable air filter.

Step 2 If the air filter is installed in the external filter brackets, slide the filter out of the brackets while being careful not to dislodge any dust that could have collected on the filter. If the filter is installed beneath the fan tray and not in the external filter brackets, open and remove the front door assembly by completing the following steps:

a. Open the front door of the shelf assembly by completing the following substeps.(If it is already open or if the shelf assembly does not have a front door, continue with Step 3.)

- Open the front door lock.
- Press the door button to release the latch.
- Swing the door open.

b. Remove the front door by completing the following substeps (optional):

- Detach the ground strap from either the door or the chassis by removing one of the Kepnuts.
- Place the Kepnut back on the stud after the ground strap is removed to avoid misplacement.

- Secure the dangling end of the ground strap to the door or chassis with tape.

Step 3 Push the outer side of the handles on the fan-tray assembly to expose the handles.

Step 4 Pull the handles and slide the fan-tray assembly one inch (25.4 mm) out of the shelf assembly and wait until the fans stop.

Step 5 When the fans have stopped, pull the fan-tray assembly completely out of the shelf assembly.

Step 6 Gently remove the air filter from the shelf assembly. Be careful not to dislodge any dust that could have collected on the filter.

Step 7 Visually inspect the air filter material for dirt and dust.

Step 8 If the reusable air filter has a concentration of dirt and dust, either vacuum or wash the air filter. Prior to washing the air filter, replace the dirty air filter with a clean air filter and also reinsert the fan-tray assembly. Wash the dirty air filter under a faucet with a light detergent.

Spare ONS 15454 filters should be kept in stock for this purpose.

Note Cleaning should take place outside the operating environment to avoid releasing dirt and dust near the equipment.

Step 9 If you washed the filter, allow it to completely air dry for at least eight hours.

Caution Do not put a damp filter back in the ONS 15454.

Step 10 If the air filter should be installed in the external filter brackets, slide the air filter all the way to the back of the brackets to complete the procedure.

Step 11 If the filter should be installed beneath the fan-tray assembly, remove the fan-tray assembly and slide the air filter into the recessed compartment at the bottom of the shelf assembly. Put the front edge of the air filter flush against the front edge of the recessed compartment. Push the fan tray back into the shelf assembly.

Caution If the fan tray does not slide all the way to the back of the shelf assembly, pull the fan tray out and readjust the position of the reusable filter until the fan tray fits correctly.

Note On a powered-up ONS 15454, the fans start immediately after the fan-tray assembly is correctly inserted.

Step 12 To verify that the tray is plugged into the backplane, ensure that the LCD on the front of the fan-tray assembly is activated and displays node information.

Step 13 Rotate the retractable handles back into their compartments.

Step 14 Replace the door and reattach the ground strap.

Remove and Reinsert a Fan-Tray Assembly

Step 1 Use the retractable handles embedded in the front of the fan-tray assembly to pull it forward several inches.

Step 2 Push the fan-tray assembly firmly back into the ONS 15454.

Step 3 Close the retractable handles.

Replace the Fan-Tray Assembly

Caution The 15454-FTA3 fan-tray assembly can only be installed in ONS 15454 R3.1 and later shelf assemblies (15454-SA-ANSI, P/N: 800-19857; 15454-SA-HD, P/N: 800-24848). It includes a pin that does not allow it to be installed in ONS 15454 shelf assemblies released before ONS 15454 R3.1 (15454-SA-NEBS3E, 15454-SA-NEBS3, and 15454-SA-R1, P/N: 800-07149). Equipment damage can result from attempting to install the 15454-FTA3 in a incompatible shelf assembly.

Caution Do not force a fan-tray assembly into place. Doing so can damage the connectors on the fan tray and/or the connectors on the backplane.

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

To replace the fan-tray assembly, it is not necessary to move any of the cable management facilities.

Step 1 Open the front door of the shelf assembly by completing the following steps. If the shelf assembly does not have a front door, continue with Step 3.

- **a.** Open the front door lock.
- **b.** Press the door button to release the latch.
- **c.** Swing the door open.

Step 2 Remove the front door (optional):

- **a.** Detach the ground strap from either the door or the chassis by removing one of the Kepnuts.
- **b.** Place the Kepnut back on the stud after the ground strap is removed to avoid misplacement.
- **c.** Secure the dangling end of the ground strap to the door or chassis with tape.

Step 3 Push the outer side of the handles on the fan-tray assembly to expose the handles.

Step 4 Fold out the retractable handles at the outside edges of the fan tray.

Step 5 Pull the handles and slide the fan-tray assembly one inch (25.4 mm) out of the shelf assembly and wait until the fans stop.

Step 6 When the fans have stopped, pull the fan-tray assembly completely out of the shelf assembly.

Step 7 If you are replacing the fan-tray air filter and it is installed beneath the fan-tray assembly, slide the existing air filter out of the shelf assembly and replace it before replacing the fan-tray assembly.

If you are replacing the fan-tray air filter and it is installed in the external bottom bracket, you can slide the existing air filter out of the bracket and replace it at anytime. For more information on the fan-tray air filter, see the "Inspect, Clean, and Replace the Reusable Air Filter" section on page 2-247.

Step 8 Slide the new fan tray into the shelf assembly until the electrical plug at the rear of the tray plugs into the corresponding receptacle on the backplane.

Step 9 To verify that the tray has plugged into the backplane, check that the LCD on the front of the fan tray is activated.

Step 10 If you replace the door, be sure to reattach the ground strap.

2.10.7 Interface Procedures

This section includes instructions for replacing an EIA and an AIP.

Replace the Electrical Interface Assembly

Note You need a #2 Phillips screwdriver. If you use high-density BNC EIAs, you also need a BNC insertion and removal tool.

Step 1 To remove the lower backplane cover, loosen the five screws that secure it to the ONS 15454 and pull it away from the shelf assembly.

Step 2 Loosen the nine perimeter screws that hold the backplane sheet metal cover or EIA in place. Do not remove the interior screws.

If you are removing an AMP Champ EIA, remove the fastening plate before proceeding. To remove the fastening plate, loosen the two thumbscrews.

Step 3 If a backplane cover is attached to the ONS 15454, lift the panel by the bottom to remove it from the shelf assembly and store the panel for later use.

Step 4 If an EIA is attached to the ONS 15454, lift the EIA handles and gently pull it away from the backplane.

Note Attach backplane sheet metal covers whenever EIAs are not installed.

Step 5 Line up the connectors on the new EIA with the mating connectors on the backplane.

Step 6 Gently push the EIA until both sets of connectors fit together snugly.

Step 7 Replace the nine perimeter screws that you removed while removing the backplane cover.

Step 8 If you are installing an AMP Champ EIA, attach the fastening plate with the two thumbscrews.

Step 9 Reattach the lower backplane cover.

Replace the Alarm Interface Panel

Caution Do not use a 2A AIP with a 5A fan-tray assembly; doing so causes a blown fuse on the AIP.

Caution If any nodes in an Ethernet circuit are not using Software R4.0 or later, there is a risk of Ethernet traffic disruptions. Contact Cisco TAC at 1 800 553-2447 when prompted to do so in the procedure.

Note Perform this procedure during a maintenance window. Resetting the active TCC2/TCC2P can cause a service disruption of less then 50 ms to OC-N or DS-N traffic. Resetting the active TCC2/TCC2P can cause a service disruption of 3 to 5 minutes on all Ethernet traffic due to spanning tree reconvergence if any nodes in the Ethernet circuit are not using Software R4.0 or later.

Caution Do not perform this procedure on a node with live traffic. Hot-swapping the AIP can affect traffic and result in a loss of data. For assistance with AIP replacement contact Cisco TAC (1 800 553-2447).

Caution Always use the supplied electrostatic discharge wristband when working with a powered ONS 15454. Plug the wristband cable into the ESD jack located on the lower-right edge of the shelf assembly.

This procedure replaces an existing AIP with a new AIP on an in-service node without affecting traffic. Ethernet circuits that traverse nodes with a software release prior to R4.0 is affected.

You need a #2 Phillips screwdriver.

Step 1 Ensure that all nodes in the affected network are running the same software version before replacing the AIP and repairing circuits:

a. In network view, click the **Maintenance > Software** tabs. The working software version for each node is listed in the Working Version column.

b. If you need to upgrade the software on a node, refer to the release-specific software upgrade document for procedures. No hardware should be changed or circuit repair performed until after the software upgrade is complete. If you do not need to upgrade software or have completed the software upgrade, proceed to Step 2.

Step 2 Record the MAC address of the old AIP:

a. Log into the node where you are replacing the AIP. For login procedures, refer to the “Connect the PC and Log into the GUI” chapter in the *Cisco ONS 15454 Procedure Guide*.

b. In node view, click the **Provisioning > Network > General** tabs.

c. Record the MAC address.

Step 3 Call Cisco TAC (1 800 553-2447) for assistance in replacing the AIP and maintaining the original MAC address.

Step 4 Unscrew the five screws that hold the lower backplane cover in place.

Step 5 Grip the lower backplane cover and gently pull it away from the backplane.

Step 6 Unscrew the two screws that hold the AIP cover in place.

Step 7 Grip the cover and gently pull away from the backplane.

Note On the 15454-SA-HD (P/N: 800-24848), 15454-SA-NEBS3E, 15454-SA-NEBS3, and 15454-SA-R1 (P/N: 800-07149) shelves the AIP cover is clear plastic. On the 15454-SA-ANSI shelf (P/N: 800-19857), the AIP cover is metal.

Step 8 Grip the AIP and gently pull it away from the backplane.

Step 9 Disconnect the fan-tray assembly power cable from the AIP.

Step 10 Set the old AIP aside for return to Cisco.

Caution The type of shelf the AIP resides in determines the version of AIP that should replace the failed AIP. The 15454-SA-ANSI shelf (P/N: 800-19857) and 15454-SA-HD (P/N: 800-24848) currently use the 5A AIP, (P/N: 73-7665-01). The 15454-SA-NEBS3E, 15454-SA-NEBS3, and 15454-SA-R1 (P/N: 800-07149) shelves and earlier use the 2A AIP (P/N: 73-5262-01).

Caution Do not put a 2A AIP (P/N: 73-5262-01) into a 15454-SA-ANSI (P/N: 800-19857) or 15454-SA-HD (P/N: 800-24848) shelf; doing so causes a blown fuse on the AIP.

Step 11 Attach the fan-tray assembly power cable to the new AIP.

Step 12 Place the new AIP on the backplane by plugging the panel into the backplane using the DIN connector.

Step 13 Replace the AIP cover over the AIP and secure the cover with the two screws.

Step 14 Replace the lower backplane cover and secure the cover with the five screws.

Step 15 In node view, click the **Provisioning > Network** tabs.

Caution Cisco recommends TCC2/TCC2P resets be performed in a maintenance window to avoid any potential service disruptions.

Step 16 Reset the standby TCC2/TCC2P:

- **a.** Right-click the standby TCC2/TCC2P and choose **Reset Card**.
- **b.** Click **Yes** in the Resetting Card dialog box. As the card resets, a loading (Ldg) indication appears on the card in CTC.The reset takes approximately five minutes. Do not perform any other steps until the reset is complete.

Step 17 Reset the active TCC2/TCC2P:

- **a.** Right click the active TCC2/TCC2P and choose **Reset Card**.
- **b.** Click **Yes** in the Resetting Card dialog box. As the card resets, a Ldg indication appears on the card in CTC. The reset takes approximately five minutes and CTC loses its connection with the node.

Step 18 From the **File** drop-down list, choose **Exit** to exit the CTC session.

Step 19 Log back into the node. At the Login dialog box, choose **(None)** from the Additional Nodes drop-down list.

Step 20 Record the new MAC address:

a. In node view, click the **Provisioning > Network > General** tabs.

b. Record the MAC address.

Step 21 In node view, click the **Circuits** tab. Note that all circuits listed are PARTIAL.

Step 22 In node view, choose **Repair Circuits** from the **Tools** drop-down list. The Circuit Repair dialog box appears.

Step 23 Read the instructions in the Circuit Repair dialog box. If all the steps in the dialog box have been completed, click **Next**. Ensure that you have the old and new MAC addresses.

Step 24 The Node MAC Addresses dialog box appears. Complete the following steps:

a. From the Node drop-down list, choose the name of the node where you replaced the AIP.

b. In the Old MAC Address field, enter the old MAC address that was recorded in Step 2.

c. Click **Next**.

Step 25 The Repair Circuits dialog box appears. Read the information in the dialog box and click **Finish**.

The CTC session freezes until all circuits are repaired. Circuit repair can take up to five minutes or more depending on the number of circuits provisioned on it.

When the circuit repair is complete, the Circuits Repaired dialog box appears.

Step 26 Click **OK**.

Step 27 In the node view of the new node, click the **Circuits** tab. Note that all circuits listed are DISCOVERED. If all circuits listed do not have a DISCOVERED status, call the Cisco TAC (1 800 553-2447) to open a Return Material Authorization (RMA).

CHAPTER 3

Transients Conditions

This chapter gives a description, entity, SNMP number, and trap for each commonly encountered Cisco ONS 15454 transient condition.

3.1 Transients Indexed By Alphabetical Entry

Table 3-1 alphabetically lists all ONS 15454 transient conditions and their entity, SNMP number, and SNMP trap.

Note The CTC default alarm profile might contain conditions that are not currently implemented but are reserved for future use.

Table 3-1 ONS 15454 Transient Condition Alphabetical Index

Transient Condition	Entity	SNMP Number	SNMP Trap
3.3.1 ADMIN-DISABLE, page 3-4	NE	5270	disableInactiveUser
3.3.2 ADMIN-DISABLE-CLR, page 3-4	NE	5280	disableInactiveClear
3.3.3 ADMIN-LOCKOUT, page 3-4	NE	5040	adminLockoutOfUser
3.3.4 ADMIN-LOCKOUT-CLR, page 3-4	NE	5050	adminLockoutClear
3.3.5 ADMIN-LOGOUT, page 3-4	NE	5020	adminLogoutOfUser
3.3.6 ADMIN-SUSPEND, page 3-4	NE	5340	suspendUser
3.3.7 ADMIN-SUSPEND-CLR, page 3-5	NE	5350	suspendUserClear
3.3.8 AUTOWDMANS, page 3-5	NE	5690	automaticWdmAnsFinished
3.3.9 BLSR-RESYNC, page 3-5	OCN	2100	blsrMultiNodeTableUpdateCompleted
3.3.10 DBBACKUP-FAIL, page 3-5	EQPT	3724	databaseBackupFailed
3.3.11 DBRESTORE-FAIL, page 3-5	EQPT	3726	databaseRestoreFailed
3.3.12 EXERCISING-RING, page 3-6	OCN	3400	exercisingRingSuccessfully
3.3.13 FIREWALL-DIS, page 3-6	NE	5230	firewallHasBeenDisabled

Table 3-1 ONS 15454 Transient Condition Alphabetical Index (continued)

Transient Condition	Entity	SNMP Number	SNMP Trap
3.3.14 FRCDWKSWBK-NO-TRFSW, page 3-6	OCN	5560	forcedSwitchBackToWorkingResultedInNoTrafficSwitch
3.3.15 FRCDWKSWPR-NO-TRFSW, page 3-6	OCn	5550	forcedSwitchToProtectResultedInNoTrafficSwitch
3.3.16 INTRUSION, page 3-6	NE	5250	securityIntrusionDetUser
3.3.17 INTRUSION-PSWD, page 3-6	NE	5240	securityIntrusionDetPwd
3.3.18 IOSCFG-COPY-FAIL, page 3-7	—	3660	iosConfigCopyFailed
3.3.19 LOGIN-FAILURE-LOCKOUT, page 3-7	NE	5080	securityInvalidLoginLockedOutSeeAuditLog
3.3.20 LOGIN-FAILURE-ONALRDY, page 3-7	NE	5090	securityInvalidLoginAlreadyLoggedOnSeeAuditLog
3.3.21 LOGIN-FAILURE-PSWD, page 3-7	NE	5070	securityInvalidLoginPasswordSeeAuditLog
3.3.22 LOGIN-FAILURE-USERID, page 3-7	NE	3722	securityInvalidLoginUsernameSeeAuditLog
3.3.23 LOGOUT-IDLE-USER, page 3-7	—	5110	automaticLogoutOfIdleUser
3.3.24 MANWKSWBK-NO-TRFSW, page 3-8	OCN	5540	manualSwitchBackToWorkingResultedInNoTrafficSwitch
3.3.25 MANWKSWPR-NO-TRFSW, page 3-8	OCN	5530	manualSwitchToProtectResultedInNoTrafficSwitch
3.3.26 PARAM-MISM, page 3-8	OTS, OMS, OCH, AOTS	5840	pluginModuleRangeSettingsMismatch
3.3.27 PM-TCA, page 3-8	—	2120	performanceMonitorThresholdCrossingAlert
3.3.28 PS, page 3-8	EQPT	2130	protectionSwitch
3.3.29 PSWD-CHG-REQUIRED, page 3-8	NE	6280	userPasswordChangeRequired
3.3.30 RMON-ALARM, page 3-8	—	2720	rmonThresholdCrossingAlarm
3.3.31 RMON-RESET, page 3-9	—	2710	rmonHistoriesAndAlarmsResetReboot
3.3.32 SESSION-TIME-LIMIT, page 3-9	NE	6270	sessionTimeLimitExpired
3.3.33 SFTWDOWN-FAIL, page 3-9	EQPT	3480	softwareDownloadFailed
3.3.34 SPANLENGTH-OUT-OF-RANGE, page 3-9	OTS	6150	spanLengthOutOfRange
3.3.35 SWFTDOWNFAIL, page 3-9	EQPT	3480	softwareDownloadFailed

Table 3-1 ONS 15454 Transient Condition Alphabetical Index (continued)

Transient Condition	Entity	SNMP Number	SNMP Trap
3.3.36 USER-LOCKOUT, page 3-9	NE	5030	userLockedOut
3.3.37 USER-LOGIN, page 3-10	NE	5100	loginOfUser
3.3.38 USER-LOGOUT, page 3-10	NE	5120	logoutOfUser
3.3.39 WKSWBK, page 3-10	EQPT, OCN	2640	switchedBackToWorking
3.3.40 WKSWPR, page 3-10	2R, TRUNK, EQPT, ESCON, FC, GE, ISC, OCN, STSMON, VT-MON	2650	switchedToProtection
3.3.41 WRMRESTART, page 3-10	NE	2660	warmRestart
3.3.42 WTR-SPAN, page 3-10	—	3420	spanIsInWaitToRestoreState

3.2 Trouble Notifications

The ONS 15454 system reports trouble by using standard condition characteristics that follow the rules in Telcordia GR-253 and graphical user interface (GUI) state indicators.

The ONS 15454 uses standard Telcordia categories to characterize levels of trouble. The system reports trouble notifications as alarms and reports status or descriptive notifications (if configured to do so) as conditions in the CTC Alarms window. Alarms typically signify a problem that you need to remedy, such as a loss of signal. Conditions do not necessarily require troubleshooting.

3.2.1 Condition Characteristics

Conditions include any problem detected on an ONS 15454 shelf. They can include standing or transient notifications. You can retrieve a snapshot of all currently raised conditions on the network, node, or card in the CTC Conditions window or by using the RTRV-COND commands in TL1.

Note Some cleared conditions are found on the History tab.

For a comprehensive list of conditions, refer to the *Cisco ONS SONET TL1 Command Guide*.

3.2.2 Condition States

The History tab state (ST) column indicates the disposition of the condition, as follows:

- A raised (R) event is active.
- A cleared (C) event is no longer active.

- A transient (T) event is automatically raised and cleared in CTC during system changes such as user login, log out, and loss of connection to node view. Transient events do not require user action.

3.3 Transient Conditions

This section lists in alphabetical order all the transient conditions encountered in Software Release 6.0. The description, entity, SNMP number, and SNMP trap accompany each condition.

3.3.1 ADMIN-DISABLE

The ADMIN-DISABLE (Disable Inactive User) condition occurs when the administrator disables the user or the account is inactive for a specified period.

This transient condition does not result in a standing condition.

3.3.2 ADMIN-DISABLE-CLR

The ADMIN-DISABLE-CLR (Disable Inactive Clear) condition occurs when the administrator clears the disable flag on the user account.

This transient condition does not result in a standing condition.

3.3.3 ADMIN-LOCKOUT

The ADMIN-LOCKOUT (Admin Lockout of User) condition occurs when the administrator locks a user account.

This transient condition does not result in a standing condition.

3.3.4 ADMIN-LOCKOUT-CLR

The ADMIN-LOCKOUT-CLR (Admin Lockout Clear) condition occurs when the administrator unlocks a user account or the lockout time expires.

This transient condition does not result in a standing condition.

3.3.5 ADMIN-LOGOUT

The ADMIN-LOGOUT (Admin Logout of User) condition occurs when the administrator logs off a user session.

This transient condition does not result in a standing condition.

3.3.6 ADMIN-SUSPEND

The ADMIN-SUSPEND (Suspend User) condition occurs when the password for a user account expires.

This transient condition does not result in a standing condition.

3.3.7 ADMIN-SUSPEND-CLR

The ADMIN-SUSPEND-CLR (Suspend User Clear) condition occurs when the user or administrator changes the password.

This transient condition does not result in a standing condition.

3.3.8 AUTOWDMANS

The AUTOWDMANS (Automatic WDM ANS Finish) condition indicates that an automatic node setup command has been initiated. It normally occurs when you replace DWDM cards; the condition is an indication that the system has regulated the card.

This transient condition does not result in a standing condition.

3.3.9 BLSR-RESYNC

The BLSR-RESYNC (BLSR Multinode Table Update Completed) condition might occur when you create or delete circuits on a bidirectional line switched ring (BLSR), change a ring topology (for example, add or delete a BLSR node), or change the BLSR circuit state and ring ID.

This transient condition does not result in a standing condition.

3.3.10 DBBACKUP-FAIL

The DBBACKUP-FAIL (Database Backup Failed) condition occurs when the system fails to back up the database when the backup command is initiated.

This condition can occur when the server is not able to handle the backup operation due to network or server issues. Repeat the same operation again and check to see if it is successful. If the backup fails, it could be due to a network issue or software program failure. Contact TAC for assistance; see the "Obtaining Documentation and Submitting a Service Request" section on page l as needed.

3.3.11 DBRESTORE-FAIL

The DBRESTORE-FAIL (Database Restore Failed) condition occurs when the system fails to restore the backed up database when the restore command is initiated.

This condition can be due to server issues, network issues, or human error (pointing to a file that does not exist, wrong file name, etc.). Retrying the database restore with the correct file will usually succeed. If the network issue persists, you must contact network lab support. If the condition is caused by a network element (NE) failure, contact TAC for assistance. See the "Obtaining Documentation and Submitting a Service Request" section on page l as needed.

3.3.12 EXERCISING-RING

The EXERCISING-RING (Exercising Ring Successfully) condition occurs whenever you issue an Exercise-Ring command from CTC or TL1. This condition indicates that a command is being executed. You must issue another command to clear the exercise and the condition.

3.3.13 FIREWALL-DIS

The FIREWALL-DIS (Firewall Has Been Disabled) condition occurs when you provision the firewall to Disabled.

This transient condition does not result in a standing condition.

3.3.14 FRCDWKSWBK-NO-TRFSW

The FRCDWKSWBK-NO-TRFSW (Forced Switch Back to Working Resulted in No Traffic Switch) condition occurs when you perform a Force Switch to the working port/card and the working port/card is already active.

This transient condition might result in a Force Switch (Ring or Span) standing condition for a BLSR.

3.3.15 FRCDWKSWPR-NO-TRFSW

The FRCDWKSWPR-NO-TRFSW (Forced Switch to Protection Resulted in No Traffic Switch) condition occurs when you perform a Force Switch to the protect port/card, and the protect port/card is already active.

This transient condition does not result in a standing condition.

3.3.16 INTRUSION

The INTRUSION (Invalid Login Username) condition occurs when you attempt to log in with an invalid user ID.

This transient condition does not result in a standing condition.

3.3.17 INTRUSION-PSWD

The INTRUSION -PSWD (Security Intrusion Attempt Detected) condition occurs when you attempt to login with an invalid password.

This transient condition does not result in a standing condition.

3.3.18 IOSCFG-COPY-FAIL

The IOSCFG-COPY-FAIL (IOS Config Copy Failed) condition occurs on ML-Series Ethernet cards when the software fails to upload or download the Cisco IOS startup configuration file to or from an ML-Series card. This condition is similar to the "SFTWDOWN-FAIL" condition on page 3-9, but the IOSCFG-COPY-FAIL condition applies to ML-Series Ethernet cards rather than the TCC2/TCC2P card.

3.3.19 LOGIN-FAILURE-LOCKOUT

The LOGIN-FAILURE-LOCKOUT (Invalid Login–Locked Out) condition occurs when you attempt to log into a locked account.

This transient condition does not result in a standing condition.

3.3.20 LOGIN-FAILURE-ONALRDY

The LOGIN-FAILURE-ONALRDY (Security: Invalid Login–Already Logged On) condition occurs when you attempt to log in with an existing session and SUPN policy.

This transient condition does not result in a standing condition.

3.3.21 LOGIN-FAILURE-PSWD

The LOGIN-FAILURE-PSWD (Invalid Login–Password) condition occurs when you attempt to log in with an invalid password.

This transient condition does not result in a standing condition.

3.3.22 LOGIN-FAILURE-USERID

The LOGIN-FAILURE-USERID (Invalid Login–Username) condition occurs when a user login (CTC, CTM, or TL1) fails because the login username is not present on the node database. You must log in again with an existing user ID.

This transient condition is equivalent to a security warning. You must check the security log (audit log) for other security-related actions that have occurred.

3.3.23 LOGOUT-IDLE-USER

The LOGOUT-IDLE-USER (Automatic Logout of Idle User) condition occurs when a user session is idle for too long (the idle timeout expires) and the session terminates as a result. You must log in again to restart your session.

3.3.24 MANWKSWBK-NO-TRFSW

The MANWKSWBK-NO-TRFSW (Manual Switch Back To Working Resulted in No Traffic Switch) condition occurs when you perform a Manual switch to the working port/card and the working port/ card is already active.

This transient condition does not result in a standing condition.

3.3.25 MANWKSWPR-NO-TRFSW

The MANWKSWPR-NO-TRFSW (Manual Switch to Protect Resulted in No Traffic Switch) condition occurs when you perform a Manual switch to the protect port/card and the protect port/card is already active.

This transient condition results in a BLSR Manual Switch (Span or Ring) standing condition.

3.3.26 PARAM-MISM

The PARAM-MISM (Plug-in Module Range Settings Mismatch) condition occurs when the parameter range values stored on a small-form factor pluggable (SFP) device are different from the parameters stored in the TCC2/TCC2P database.

The transient condition is not user-serviceable. Refer to the "Obtaining Documentation and Submitting a Service Request" section on page l.

3.3.27 PM-TCA

The PM-TCA (Performance Monitor Threshold Crossing Alert) condition occurs when network collisions cross the rising threshold for the first time.

3.3.28 PS

The PS (Protection Switch) condition occurs when the traffic switches from a working/active card to a protect/standby card.

3.3.29 PSWD-CHG-REQUIRED

The PSWD-CHG-REQUIRED (User Password Change Required) condition occurs when you are denied login for a shell function such as telnet or FTP because you did not change the login password. You can change the password through CTC or TL1.

3.3.30 RMON-ALARM

The RMON-ALARM (RMON Threshold Crossing Alarm) condition occurs when the remote monitoring variable crosses the threshold.

3.3.31 RMON-RESET

The RMON-RESET (RMON Histories and Alarms Reset Reboot) condition occurs when the time-of-day settings on the TCC2/TCC2P card are increased or decreased by more than five seconds. This invalidates all the history data and remote monitoring (RMON) must restart. It can also occur when you reset a card.

3.3.32 SESSION-TIME-LIMIT

The SESSION-TIME-LIMIT (Session Time Limit Expired) condition occurs when a login session exceeds the time limit and you are logged out of the session. You must login again.

3.3.33 SFTWDOWN-FAIL

The SFTDOWN-FAIL (Software Download Failed) condition occurs when the system fails to download the required software.

An incorrect input that points to the wrong place or file, network issues, or a bad (corrupt) package can cause this failure. Retrying the operation with the correct name/location will usually succeed. If network issues persist, you must contact the network lab support. If the package is corrupt, contact Cisco TAC. See the "Obtaining Documentation and Submitting a Service Request" section on page l for details.

3.3.34 SPANLENGTH-OUT-OF-RANGE

The SPANLENGTH-OUT-OF-RANGE (Span Length Out of Range) condition occurs when the measured span loss does not fall within the limits of minimum and maximum expected span loss. It can also occur when the difference between MaxExpSpanLoss and MinExpSpanLoss is greater than 1dB.

When you perform a Calculate Span Loss operation on a DWDM node, the software measures the real span loss in the field by comparing the far-end POSC power and the near-end OSC power.

3.3.35 SWFTDOWNFAIL

The SFTDOWN-FAIL (Software Download Failed) condition occurs when the system fails to download the required software.

An incorrect input that points to the wrong place or file, network issues, or a bad (corrupt) package can cause this failure. Retrying the operation with the correct name/location will usually succeed. If network issues persist, you must contact the network lab support. If the package is corrupt, contact Cisco TAC. See the "Obtaining Documentation and Submitting a Service Request" section on page l for details.

3.3.36 USER-LOCKOUT

The USER-LOCKOUT (User Locked Out) condition occurs when the system locks an account because of a failed login attempt. To proceed, the administrator must unlock the account or the lockout time must expire.

3.3.37 USER-LOGIN

The USER-LOGIN (Login of User) occurs when you begin a new session by verifying your User ID and password.

This transient condition does not result in a standing condition.

3.3.38 USER-LOGOUT

The USER-LOGOUT (Logout of User) condition occurs when you stop a login session by logging out of your account.

This transient condition does not result in a standing condition.

3.3.39 WKSWBK

The WKSWBK (Switched Back to Working) condition occurs when traffic switches back to the working port/card in a non-revertive protection group.

This transient condition does not result in a standing condition.

3.3.40 WKSWPR

The Switched to Protection (WKSWPR) condition occurs when traffic switches to the protect port/card in a non-revertive protection group. This transient condition does not result in a standing condition. The (WKSWPR) is raised as a standing condition in a revertive protection group.

The Switched to Protection (WKSWPR) condition also occurs after the protection switch in a 1+1 non-revertive protection group as a transient condition. When the protection group is changed to revertive, the (WKSWPR) is not raised as a standing condition or as a new transient condition. However, after a protection switch in a 1:1 protection group, the user will not be allowed to configure the protection group from non-revertive to revertive.

3.3.41 WRMRESTART

The WRMRESTART (Warm Restart) condition occurs when the node restarts while powered up. A restart can be caused by provisioning, such as database-restore and IP changes, or software defects. A WRMRESTART is normally accompanied by MANRESET or AUTORESET to indicate whether the reset was initiated manually (MAN) or automatically (AUTO).

This is the first condition that appears after a TCC2/TCC2P card is powered up. The condition changes to COLD-START if the TCC2/TCC2P card is restarted from a physical reseat or a power loss.

3.3.42 WTR-SPAN

The WTR-SPAN (Span is in Wait To Restore State) condition occurs when a BLSR switches to another span due to a Signal Failure-Span command or a fiber is pulled from a four-fiber BLSR configuration. The condition is raised until the WaitToRestore (WTR) period expires.

This transient condition clears when the BLSR returns to a normal condition or the IDLE state.

Error Messages

Note The terms "Unidirectional Path Switched Ring" and "UPSR" may appear in Cisco literature. These terms do not refer to using Cisco ONS 15xxx products in a unidirectional path switched ring configuration. Rather, these terms, as well as "Path Protected Mesh Network" and "PPMN," refer generally to Cisco's path protection feature, which may be used in any topological network configuration. Cisco does not recommend using its path protection feature in any particular topological network configuration.

This chapter lists the Cisco ONS 15454, 15454 SDH, 15600, 15327 and 15310-CL error messages. The error dialog box in Figure 4-1 consists of three parts: the error title, error ID, and error message. The table lists two types of messages: error messages (EID-*nnnn*) and warning messages (WID-*nnnn*). Error messages are alerts that an unexpected or undesirable operation has occurred which either indicates the risk of loss of traffic or an inability to properly manage devices in the network. Warnings are alerts that the requested operation could lead to an error. Warnings are sometimes used to convey important information.

Figure 4-1 Error Dialog Box

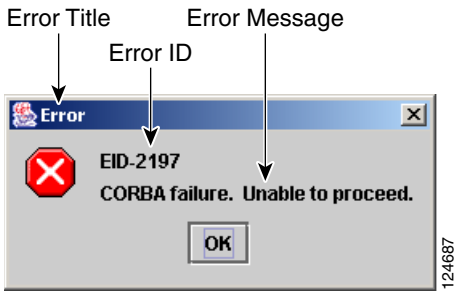


Table 4-1 gives a list of all error or warning message numbers, the messages, and a brief description of each message.

Table 4-1 Error Messages

Error or Warning ID	Error or Warning Message	Description
EID-0	Invalid error ID.	The error ID is invalid.
EID-1	Null pointer encountered in {0}.	Cisco Transport Controller (CTC) encountered a null pointer in the area described by the specified item.
EID-1000	The host name of the network element cannot be resolved to an address.	Refer to error or warning message text.
EID-1001	Unable to launch CTC due to applet security restrictions. Please review the installation instructions to make sure that the CTC launcher is given the permissions it needs. Note that you must exit and restart your browser in order for the new permissions to take effect.	Refer to error or warning message text.
EID-1002	The host name (e.g., for the network element) was successfully resolved to its address, but no route can be found through the network to reach the address.	The node is not reachable from CTC client station.
EID-1003	An error was encountered while attempting to launch CTC. {0}	Unexpected exception or error while launching CTC from the applet.
EID-1004	Problem Deleting CTC Cache: {0} {1}	Unable to delete the CTC cached JARs, because another application may have the JAR files running; for example, another instance of CTC.
EID-1005	An error occurred while writing to the {0} file.	CTC encountered an error while writing to log files, preference files, etc.
EID-1006	The URL used to download {0} is malformed.	The URL used to download the Launcher.jar file is malformed.
EID-1007	An I/O error occurred while trying to download {0}.	An input or output exception was encountered when CTC tried to download the GUI launcher.
EID-1018	Password must contain at least 1 alphabetic, 1 numeric, and 1 special character (+, # or %). Password shall not contain the associated user-ID.	The password is invalid.
EID-1019	Could not create {0}. Please enter another filename.	CTC could not create the file due to an invalid filename.
EID-1020	Fatal exception occurred, exiting CTC. Unable to switch to the Network view.	CTC was unable to switch from the node or card view to the network view, and is now shutting down.
EID-1021	Unable to navigate to {0}.	Failed to display the indicated view—node or network.
EID-1022	A session cannot be opened right now with this slot. Most likely someone else (using a different CTC) already has a session opened with this slot. Please try again later.	Refer to the error message text. Ensure that the shell access in CTC (Provisioning>Security>Access) is set to non-secure mode.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
EID-1023	This session has been terminated. This can happen if the card resets, the session has timed out, or if someone else (possibly using a different CTC) already has a session open with this slot.	Refer to error message text.
EID-1025	Unable to create Help Broker.	CTC was unable to create the help broker for the online help.
EID-1026	Unable to locate HelpSet.	CTC was unable to locate the help set for the online help.
EID-1027	Unable to locate Help ID: {0}	CTC was unable to locate the help ID for the online help.
EID-1028	Error saving table. {0}	There was an error while saving the specified table.
EID-1031	CTC cannot locate the online user manual files. The files may have been moved, deleted, or not installed. To install online user manuals, run the CTC installation wizard on the software or documentation CD.	Refer to error message text.
EID-1032	CTC cannot locate Acrobat Reader. If Acrobat Reader is not installed, you can install the Reader using the CTC installation wizard provided on the software or documentation CD.	Refer to error message text.
EID-1034	Unable to locate HelpSet when searching for Help ID "{0}".	CTC is unable to locate the specified help ID of the context sensitive help files.
EID-1035	CTC experienced an I/O error while working with the log files. Usually this means that the computer has run out of disk space. This problem may or may not cause CTC to stop responding. Ending this CTC session is recommended, but not required.	Refer to error message text.
WID-1036	WARNING: Deleting the CTC cache may cause any CTC running on this system to behave in an unexpected manner.	Refer to warning message text.
EID-1037	Could not open {0}. Please enter another filename.	Invalid file name. CTC is unable to open the file.
EID-1038	The file {0} does not exist.	The specified file does not exist.
EID-1039	The version of the browser applet does not match the version required by the network element. Please close and restart your browser in order to launch the Cisco Transport Controller.	Refer to error message.
WID-1040	WARNING: Running the CTC with a JRE version other than the recommended JRE version might cause the CTC to behave in an unexpected manner.	Refer to warning message.
EID-2001	No rolls selected. {0}	No rolls were selected for the bridge and roll.
EID-2002	The Roll must be completed or cancelled before it can be deleted.	You cannot delete the roll unless it has been completed or cancelled.
EID-2003	Error deleting roll.	There was an error when CTC tried to delete the roll.
EID-2004	No IOS slot selected.	You did not select a Cisco IOS slot.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
EID-2005	CTC cannot find the online help files for {0}. The files may have been moved, deleted, or not installed. To install online help, run the setup program on the software or documentation CDs.	CTC cannot find the online help files for the specified window. The files might have been moved, deleted, or not installed. To install online help, run the setup program on the software or documentation CDs.
EID-2006	Error editing circuit(s). {0} {1}.	An error occurred when CTC tried to open the circuit for editing.
EID-2007	Unable to save preferences.	CTC cannot save the preferences.
EID-2008	Unable to store circuit preferences: {0}	CTC cannot find the file needed to save the circuit preferences.
EID-2009	Unable to download package: {0}	Refer to error message text.
EID-2010	Delete destination failed.	CTC could not delete the destination.
EID-2011	Circuit destroy failed.	CTC could not destroy the circuit.
EID-2012	Reverse circuit destroy failed.	CTC could not reverse the circuit destroy.
EID-2013	Circuit creation error. Circuit creation cannot proceed due to changes in the network which affected the circuit(s) being created. The dialog will close. Please try again.	Refer to error message text.
EID-2014	No circuit(s) selected. {0}	You must select a circuit to complete this function.
EID-2015	Unable to delete circuit {0}as it has one or more rolls.	You must delete the rolls in the circuit before deleting the circuit itself.
EID-2016	Unable to delete circuit.	CTC could not delete the tunnel as there are circuits that use the tunnel.
EID-2017	Error mapping circuit. {0}	There was an error mapping the circuit.
EID-2018	Circuit roll failure. The circuit has to be in the DISCOVERED state in order to perform a roll.	There was a failure in circuit roll. Change the circuit state to DISCOVERED and proceed.
EID-2019	Circuit roll failure. Bridge and roll is not supported on a DWDM circuit.	Refer to error message text.
EID-2020	Circuit roll failure. The two circuits must have the same direction.	Refer to error message text.
EID-2021	Circuit roll failure. The two circuits must have the same size.	Refer to error message text.
EID-2022	Circuit roll failure. A maximum of two circuits can be selected for a bridge and roll operation.	Refer to error message text.
EID-2023	Unable to create new user account.	Refer to error message text.
EID-2024	Node selection error.	There was an error during node selection.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
EID-2025	This feature cannot be used. Verify that each of the endpoints of this circuit are running software that supports this feature.	Refer to error or warning message text. This error is generated from the AnsOpticsParamsPane to indicate that the selected ring type is not supported by the endpoints of the circuit. In the VLAN tab it indicates that the back-end spanning tree protocol (STP) disabling is not supported.
EID-2026	Unable to apply {0} request. {1}	Error occurred while attempting to switch a path protection circuit away from a span.
EID-2027	Error deleting circuit drop.	CTC could not delete the circuit drop.
EID-2028	Error removing circuit node.	CTC could not remove the circuit node.
EID-2029	The requested operation is not supported.	The task you are trying to complete is not supported by CTC.
EID-2030	Provisioning error.	There was an error during provisioning.
EID-2031	Error adding node.	There was an error while adding a node.
EID-2032	Unable to rename circuit. {0}	CTC could not rename the circuit.
EID-2033	An error occurred during validation. {0}	There was an internal error while validating the user changes after the Apply button was pressed. This error can occur in the Edit Circuit dialog box or in the BLSR table in the shelf view (rare condition).
EID-2034	Unable to add network circuits: {0}	Refer to error message text.
EID-2035	The source and destination nodes are not connected.	Refer to error message text.
EID-2036	Cannot delete this {0}. LAN Access has been disabled on this node and this {0} is needed to access the node.	You cannot delete the DCC/GCC link as it is needed to access the node.
EID-2037	Application error. Cannot find attribute for {0}.	CTC cannot find an attribute for the specified item.
EID-2038	Invalid protection operation.	The protection operation you tried to execute is invalid.
EID-2040	Please select a node first.	You must select a node before performing the task.
EID-2041	No paths are available on this link. Please make another selection.	You must select a link that has paths available.
EID-2042	This span is not selectable. Only the green spans with an arrow may be selected.	Refer to error message text.
EID-2043	This node is not selectable. Only the source node and nodes attached to included spans (blue) are selectable. Selecting a selectable node will enable its available outgoing spans.	Refer to error message text.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
EID-2044	This link may not be included in the required list. Constraints only apply to the primary path. Each node may have a maximum of one incoming signal and one outgoing link.	You must select only one link going in and out of a node. Selecting more than one link is contradictory to the path selection algorithm.
EID-2045	This link may not be included in the required list. Only one outgoing link may be included for each node.	Refer to error message text.
EID-2047	Error validating slot number. Please enter a valid value for the slot number.	There was an error due to an invalid slot number.
EID-2048	Error validating port number. Please enter a valid value for the port number.	There was an error due to an invalid port number.
EID-2050	New circuit destroy failed.	CTC could not destroy the new circuit.
EID-2051	Circuit cannot be downgraded. {0}	The specified circuit cannot be downgraded.
EID-2052	Error during circuit processing.	There was an error during the circuit processing.
EID-2054	Endpoint selection error.	There was an error during the endpoint selection.
EID-2055	No endpoints are available for this selection. Please make another selection.	This error occurs in the circuit creation dialog only during a race condition that has incorrectly allowed entities without endpoints to be displayed in the combo boxes.
EID-2056	Communication error. {0}	An internal error occurred in Network Alarm tab while synchronizing alarms with the nodes.
EID-2059	Node deletion Error. {0}	There was an error during the node deletion.
EID-2060	No PCA circuits found.	CTC could not find any protection channel access (PCA) circuits for this task.
EID-2061	Error provisioning VLAN.	There was an error defining the VLAN.
EID-2062	Cannot delete VLAN. No VLAN(s) are selected. Please select a VLAN.	Cannot delete VLAN. No VLAN(s) are selected. Please select a VLAN.
EID-2063	Cannot delete default VLAN.	The selected VLAN is the default VLAN, and cannot be deleted.
EID-2064	Error deleting VLANs. {0}	There was an error deleting the specified VLAN.
EID-2065	Cannot import profile. Profile "{0}" exists in the editor and the maximum number of copies (ten) exists in the editor. Aborting the import. The profile has already been loaded eleven times.	Cannot import the profile as the profile has reached the maximum number of copies in the editor.
EID-2066	Unable to store profile. Error writing to {0}.	CTC encountered an error while trying to store the profile.
EID-2067	File write error. {0}	CTC encountered an error while writing the specified file.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
EID-2068	Unable to load alarm profile from node.	CTC encountered an error trying to load the alarm profile from the node.
EID-2069	File not found or I/O exception. (No such file or directory)	Either the specified file was not found, or there was an input/output exception.
EID-2070	Failure deleting profile. {0}	There was a failure in deleting the specified profile.
EID-2071	Only one column may be highlighted.	You cannot select more than one column during clone action.
EID-2072	Only one profile may be highlighted.	You cannot select more than one profile.
EID-2073	This column is permanent and may not be removed.	You cannot delete a permanent column.
EID-2074	Select one or more profiles.	You have not selected any profile or column. Reset operation is done by right-clicking the selected column.
EID-2075	This column is permanent and may not be reset.	A permanent column is non resettable.
EID-2077	This column is permanent and may not be renamed.	You cannot rename a permanent column.
EID-2078	At least two columns must be highlighted.	You connot compare two profiles unless you select two columns.
EID-2079	Cannot load alarmables into table. There are no reachable nodes from which the list of alarmables may be loaded. Please wait until such a node is reachable and try again.	Refer to error message text.
EID-2080	Node {0} has no profiles.	The specified node does not have any profiles.
EID-2081	Error removing profile {0} from node {1}.	There was an error while removing the specified profile from the specified node.
EID-2082	Cannot find profile {0} on node {1}.	CTC cannot find the specified profile from the specified node.
EID-2083	Error adding profile {0} to node {1}.	There was an error adding the specified profile to the specified node.
EID-2085	Invalid profile selection. No profiles were selected.	You tried to select an invalid profile. Select another profile.
EID-2086	Invalid node selection. No nodes were selected.	You tried to select an invalid node. Select another node.
EID-2087	No profiles were selected. Please select at least one profile.	Refer to error message text.
EID-2088	Invalid profile name.	The profile name cannot be empty.
EID-2089	Too many copies of {0} exist. Please choose another name.	Select a unique name.
EID-2090	No nodes selected. Please select the node(s) on which to store the profile(s).	You must select one or more nodes on which you can store the profile.
EID-2091	Unable to switch to node {0}.	CTC is unable to switch to the specified node.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
EID-2092	General exception error.	CTC encountered a general exception error while trying to complete the task.
EID-2093	Not enough characters in name. {0}	The name must have a minimum of six characters.
EID-2094	Password and confirmed password fields do not match.	You must make sure the two fields have the same password.
EID-2095	Illegal password. {0}	The password you entered is not allowed.
EID-2096	The user must have a security level.	You must have an assigned security level to perform this task.
EID-2097	No user name specified.	You did not specify a user name.
EID-2099	Ring switching error.	There was an error during the ring switch.
EID-2100	Please select at least one profile to delete.	You have not selected the profile to delete.
EID-2101	Protection switching error.	There was an error during the protection switching.
EID-2102	The forced switch could not be removed for some circuits. You must switch these circuits manually.	The forced switch could not be removed for some circuits. You must switch these circuits manually.
EID-2103	Error upgrading span.	There was an error during the span upgrade.
EID-2104	Unable to switch circuits back as one or both nodes are not reachable.	This error occurs during the path protection span upgrade procedure.
EID-2106	The node name cannot be empty.	You must supply a name for the node.
EID-2107	Error adding {0}, unknown host.	There was an error adding the specified item.
EID-2108	{0} is already in the network.	The specified item exists in the network.
EID-2109	The node is already in the current login group.	The node you are trying to add is already present in the current login group.
EID-2110	Please enter a number between 0 and {0}.	You must enter a number in the range between 0 and the specified value.
EID-2111	This node ID is already in use. Please choose another.	Select a node ID that is not in use.
EID-2113	Cannot set extension byte for ring. {0}	CTC cannot set the extension byte.
EID-2114	Card communication failure. Error applying operation.	This error can occur during an attempt to apply a BLSR protection operation to a line.
EID-2115	Error applying operation. {0}	There was an error in applying the specified operation.
EID-2116	Invalid extension byte setting for ring. {0}	The extension byte set for the specified ring is invalid.
EID-2118	Cannot delete ring. There is a protection operation set. All protection operations must be clear for ring to be deleted.	Delete all the protection operations for the ring before it can be deleted.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
EID-2119	Cannot delete {0} because a protection switch is in effect. Please clear any protection operations, make sure that the reversion time is not "never" and allow any protection switches to clear before trying again.	Clear all protection operations or switches before deleting the ring.
EID-2120	The following nodes could not be unprovisioned {0} Therefore you will need to delete this {1} again later.	The specified nodes could not be unprovisioned. Try deleting this BLSR or MS-SPRing later.
EID-2121	Cannot upgrade ring. {0}	CTC cannot upgrade the specified ring.
EID-2122	Inadequate ring speed for upgrade. Only {0} (or higher) {1} can be upgraded to 4-fiber.	You have selected an incorrect ring speed for upgrade. Only rings within the specified parameters can be upgraded to 4-fiber BLSR.
EID-2123	Verify that the following nodes have at least two in-service ports with the same speed as the 2-fiber {0}. The ports cannot serve as a timing reference, and they cannot have DCC terminations or overhead circuits. {1}	Nonupgradable nodes. Verify that the specified nodes have at least two IS-NR ports with the same speed as the 2-fiber BLSR. The specified ports cannot serve as a timing reference, and they cannot have data communications channel (DCC) terminations or overhead circuits.
EID-2124	You cannot add this span because it is connected to a node that already has the east and west ports defined.	Refer to error message text.
EID-2125	You cannot add this span as it would cause a single card to host both the east span and the west span. A card cannot protect itself.	Refer to error message text.
EID-2126	OSPF area error. {0}	There is an Open Shortest Path First (OSPF) area error.
EID-2127	You cannot add this span. It would cause the following circuit(s) to occupy different STS regions on different spans. {0} Either select a different span or delete the above circuit(s).	A circuit cannot occupy different STS regions on different spans. You may add a different span or delete the specified circuit.
EID-2128	Illegal state error.	An internal error occurred while trying to remove a span from a BLSR. This alarm occurs in the network-level BLSR creation dialog box.
EID-2129	This port is already assigned. The east and west ports must be different.	Refer to error message text.
EID-2130	The ring ID value, {0}, is not valid. Please enter a valid number between 0 and 9999.	Enter a ring ID value between 0 and 9999.
EID-2131	Cannot set reversion to INCONSISTENT.	You must select another reversion type.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
EID-2135	Unable to store overhead circuit preferences: {0}	Input/Output error. Unable to store overhead circuit preferences.
EID-2137	Circuit merge error. {0}	There was an error while merging the circuits.
EID-2138	Cannot delete all destinations. Please try again.	Refer to error message text.
EID-2139	Error updating destinations.	There was an error in updating the circuit destinations.
EID-2143	No online help version selected. Cannot delete the online help book.	Select the version of online help, and proceed.
EID-2144	Error deleting online help book(s). {0}	You cannot delete the specified online help.
EID-2145	Unable to locate a node with an IOS card.	Refer to error message.
EID-2146	Security violation. You may only logout your own account.	You cannot logout of an account other than your own.
EID-2147	Security violation. You may only change your own account.	You cannot change an account other than your own.
EID-2148	Security violation. You may not delete the account under which you are currently logged in.	You cannot delete the account you are currently loggd in.
WID-2149	There is nothing exportable on this view.	Refer to error message text.
WID-2150	Node {0} is not initialized. Please wait and try again.	Wait till the specified node is initialized and try again.
WID-2152	Spanning tree protection is being disabled for this circuit.	Refer to warning message text.
WID-2153	Adding this drop makes the circuit a PCA circuit.	Refer to warning message text.
WID-2154	Disallow creating monitor circuits on a port grouping circuit.	Refer to warning message text.
WID-2155	Only partial switch count support on some nodes. {0}	The specified nodes do not support switch counts completely.
WID-2156	Manual roll mode is recommended for dual rolls. For auto dual rolls, please verify that roll to facilities are in service and error free.	Refer to warning message text.
WID-2157	Cannot complete roll(s). {0}	CTC could not complete the roll because roll is destroyed, roll is in incomplete state, roll is in TL1_roll state, roll is cancelled, or roll is not ready to complete.
EID-2158	Invalid roll mode. {0}	There are two roll modes such as auto and manual. For one way circuit source roll, the roll mode must be auto and for one way circuit destination roll, the roll mode must be manual.
EID-2159	Roll not ready for completion. {0}	The roll is not ready for completion.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
EID-2160	Roll not connected. {0}	Refer to error messge text.
EID-2161	Sibling roll not complete. {0}	One of the rolls is not completed for the dual roll. If it is auto roll, it will be completed when a valid signal is detected. If it is manual roll, you must complete the roll from CTC if Bridge and Roll is operated from CTC, or from TL1 if Bridge and Roll is operated from TL1.
EID-2162	Error during roll acknowledgement. {0}	Refer to error message text.
EID-2163	Cannot cancel roll. {0}	CTC cannot cancel the roll.
EID-2164	Roll error. {0}	CTC encountered a roll error.
WID-2165	The MAC address of node {0} has been changed. All circuits originating from or dropping at this node will need to be repaired.	Repair the circuits that originate from or drop at the specified node, with the new MAC address.
WID-2166	Unable to insert node into the domain as the node is not initialized.	Initialize the node and proceed.
WID-2167	Insufficient security privilege to perform this action.	You do not have the previlege to perform this action.
WID-2168	Warnings loading{0}. {1}	CTC encountered warnings while loading the alarm profile import file.
WID-2169	One or more of the profiles selected do not exist on one or more of the nodes selected.	The profile selected does not exist on the node. Select another profile.
WID-2170	The profile list on node {0} is full. Please delete one or more profiles if you wish to add profile. {1}	The number of profile that can exist on a node has reached the limit. To add a profile, delete any of the existing profiles.
WID-2171	You have been logged out. Click OK to exit CTC.	Refer to warning message text.
WID-2172	The CTC CORBA (IIOP) listener port setting of {0} will be applied on the next CTC restart.	The Internet Inter-ORB Protocol (IIOP) listener port setting for the CTC Common Object Request Broker Architecture (CORBA) will be applied on the next CTC restart.
EID-2173	Port unavailable. The desired CTC CORBA (IIOP) listener port, {0}, is already in use or you do not have permission to listen on it. Please select an alternate port.	Select an alternate port, as the current port is either in use or you do not have enough permission on it.
EID-2174	Invalid number entered. Please check it and try again.	You entered an invalid firewall port number. Try again.
WID-2175	Extension byte mismatch. {0}	There is a mismatch with the extension byte.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
WID-2176	Not all spans have the same OSPF Area ID. This will cause problems with protection switching. To determine the OSPF Area for a given span, click on the span and the OSPF Area will be displayed in the pane to the left of the network map.	Refer to warning message text.
WID-2178	Only one edit pane can be opened at a time. The existing pane will be displayed.	Refer to warning message text.
WID-2179	There is no update as the circuit has been deleted.	Refer to warning message text.
EID-2180	CTC initialization failed in step {0}.	CTC initialization has failed in the specified step.
EID-2181	This link may not be included as it originates from the destination.	You must not include this link as it originates from destination of a circuit. It is against the path selection algorithm.
EID-2182	The value of {0} is invalid.	The value of the specified item is invalid.
EID-2183	Circuit roll failure. Current version of CTC does not support bridge and roll on a VCAT circuit.	Refer to error message text.
EID-2184	Cannot enable the STP on some ports because they have been assigned an incompatible list of VLANs. You can view the VLAN/Spanning Tree table or reassign ethernet ports VLANs.	Refer to error message text.
EID-2185	Cannot assign the VLANs on some ports because they are incompatible with the Spanning Tree Protocol. You can view the VLAN/Spanning Tree table or reassign VLANs.	Refer to error message text.
EID-2186	Software download failed on node {0}.	The software could not be downloaded onto the specified node.
EID-2187	The maximum length for the ring name that can be used is {0}. Please try again.	You must shorten the length of the ring name.
EID-2188	The nodes in this ring do not support alphanumeric IDs. Please use a ring ID between {0} and {1}.	The ring ID should not contain alphanumeric characters, and must be in the specified range.
EID-2189	TL1 keyword "all" can not be used as the ring name. Please provide another name.	Refer to error message text.
EID-2190	Adding this span will cause the ring to contain more nodes than allowed.	You have reached the maximum number of nodes allowed.
EID-2191	Ring name must not be empty.	You must supply a ring name.
EID-2192	Cannot find a valid route for the circuit creation request.	CTC could not complete the circuit creation request either beacuse there are no physical links, or the bandwidth of the available links are already reserved.
EID-2193	Cannot find a valid route for the circuit drop creation request.	Refer to error message text.
EID-2194	Cannot find a valid route for the roll creation request.	Refer to error message text.
EID-2195	The circuit VLAN list cannot be mapped to one spanning tree. You can view the VLAN/Spanning Tree table or reassign VLANs.	Refer to error message text.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
EID-2196	Unable to relaunch the CTC. {0}	There is an error relaunching CTC.
EID-2197	CORBA failure. Unable to proceed.	There was a CORBA failure, and the task cannot proceed. Verify the Java version.
EID-2198	Unable to switch to the {0} view.	CTC is unable to switch to the specified view.
EID-2199	Login failed on {0} {1}	The login failed on the specified tasks.
EID-2200	CTC has detected a jar file deletion. The jar file was used to manage one or more nodes. This CTC session will not be able to manage those nodes and they will appear gray on the network map. It is recommended that you exit this CTC session and start a new one.	Refer to error message text.
EID-2202	Intra-node circuit must have two sources to be Dual Ring Interconnect.	Intranode circuit must have two sources to be a dual ring interconnect (DRI).
EID-2203	No member selected.	You must select a member.
EID-2204	Number of circuits must be a positive integer	The number of circuits cannot be zero or negative.
EID-2205	Circuit Type must be selected.	You must select a circuit type.
EID-2206	Unable to autoselect profile! Please select profile(s) to store and try again.	Refer to error message text.
EID-2207	You cannot add this span. Either the ring name is too big (i.e., ring name length is greater than {0}) or the endpoints do not support alphanumeric IDs.	Reduce the length of the ring name, or remove the alphanumberic characters from the end points.
EID-2208	This is an invalid or unsupported JRE.	The version of Java Runtime Environment (JRE) is either invalid or unsupported.
EID-2209	The user name must be at least {0} characters long.	The user name must be at least of the specified character length.
EID-2210	No package name selected.	You must select a package name.
EID-2211	No node selected for upgrade.	You must select a node for the upgrade.
EID-2212	Protected Line is not provisionable.	The protected line cannot be provisioned. Choose another line.
WID-2213	The current type or state of some drops does not allow the new circuit state of {0} to be applied to them indirectly.	The circuit state, specified by {0} cannot be applied to the selected drops.
EID-2214	The node is disconnected. Please wait till the node reconnects.	Refer to error message text.
EID-2215	Error while leaving {0} page.	There was an error while leaving the specified page.
EID-2216	Error while entering {0} page.	There was an error while entering the specified page.
EID-2217	Some conditions could not be retrieved from the network view	Refer to error message text.
EID-2218	Bandwidth must be between {0} and {1} percent.	The bandwidth must be within the specified parameters.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
EID-2219	Protection operation failed, XC loopback is applied on cross-connection.	As the protection operation failed, a cross-connect (XC) loopback will be applied on cross-connection.
EID-2220	The tunnel status is PARTIAL. CTC will not be able to change it. Please try again later	Refer to error message text.
EID-2221	Cannot find a valid route for the unprotected to {0} upgrade request.	Refer to error message text.
EID-2222	One or more of the following nodes are currently part of a 4-fiber {0}. Only a single 4-fiber {0} is supported per node. {1}	The nodes, specified by {1}, are already part of a 4-fiber ring type, specified by {0}.
EID-2223	Only one circuit can be upgraded at a time.	Refer to error message text.
EID-2224	This link may not be included as it terminates on the source.	Refer to error message text.
EID-2225	No valid signal while trying to complete the roll. (0)	Roll can be completed only when a valid signal is detected. If not, the roll completion may result in an error.
EID-2226	Circuit roll failure. {0}	Refer to error message text.
EID-2320	This VCAT circuit does not support deletion of its member circuits.	You can not delete a circuit that is a member of VCAT circuit.
EID-2321	Error deleting member circuits. {0}	Refer to error message text.
WID-2322	Not all cross-connects from selected circuits could be merged into the current circuit. They may appear as partial circuits.	Refer to warning message text.
EID-2323	Circuit roll failure. Bridge and roll is not supported on a monitor circuit.	A monitor circuit does not support Bridge and Roll.
EID-2324	Circuit upgrade error. {0}	Refer to error message text.
EID-2325	You have failed {0} times to unlock this session. CTC will exit after you click OK or close this dialog box.	The maximum amount of attempts to unlock this session has been reached.
WID-2326	Currently, CTC does not support bridge and roll on circuits that are entirely created by TL1. To continue with bridge and roll in CTC, selected circuits must be upgraded. OK to upgrade selected circuits and continue bridge and roll operation?	Refer to warning message text.
WID-2327	Currently, CTC does not support bridge and roll on circuits that are partially created by TL1. To continue with bridge and roll in CTC, selected circuits must be upgraded. OK to upgrade selected circuits and continue bridge and roll operation?	Refer to warning message text.
EID-2328	Circuit reconfigure error. {0}	The attempt to reconfigure the specified circuit has failed.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
EID-2329	{0} of {1} circuits could not be successfully created.	A few circuits could not be created.
EID-2330	Circuit verification: selected {0} invalid! {1}	The selected item, specified by {0}, is invalid as per the details, specified in {1}.
EID-2331	Deleting {0} may be service affecting.	Deleting the item can affect the service of CTC.
EID-2332	Hold-off timer validation error in row [0]. {1} hold-off timer for {2} must be between {3}-10,000 ms, in steps of 100 ms.	Refer to error message text.
EID-3001	An Ethernet RMON threshold with the same parameters already exists. Please change one or more of the parameters and try again.	Change a few parameters in an Ethernet remote monitoring (RMON) threshold and try again.
EID-3002	Error retrieving defaults from the node: {0}	There was an error while retrieving the defaults from the specified node.
EID-3003	Cannot load file {0}.	CTC cannot load the specified file.
EID-3004	Cannot load properties from the node	Refer to error message text.
EID-3005	Cannot save NE Update values to file {0}	CTC cannot save the network element (NE) update values to the specified file.
EID-3006	Cannot load NE Update properties from the node	Refer to error message text.
EID-3007	Provisioning Error for {0}	There was a provisioning error for the specified item.
EID-3008	Not a valid Card	You cannot perform DWDM automatic node setup (ANS) from the Card view. Please navigate to the Node view and try again.
EID-3009	No {0} selected	Select the specified item, for example, VLAN, port, slot, etc.
EID-3010	Unable to create bidirectional optical link	Refer to error message text.
EID-3011	The file {0} doesn't exist or cannot be read.	The specified file does not exist or cannot be read.
EID-3012	The size of {0} is zero.	The size of the specified item is zero.
EID-3013	{0} encountered while restoring database.	The specified item was encountered while restoring the database.
EID-3014	The operation was terminated due to the following error: {0}	Refer to error message text.
EID-3015	{0} encountered while performing DB backup.	The specified item or condition was encountered while performing the DB backup.
EID-3016	Invalid subnet address.	Refer to error message text.
EID-3017	Subnet address already exists.	Refer to error message text.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
EID-3018	Standby TSC not ready.	The standby Timing and Shelf Control card (TSC) not ready.
EID-3019	Incomplete internal subnet address.	Enter the complete internal subnet address.
EID-3020	TSC One and TSC Two subnet addresses cannot be the same.	A node's internal subnet must be different from one another as each TSC is on separate ethernet buses, isolated by broadcast domains.
EID-3021	An error was encountered while retrieving the diagnostics: {0}	Refer to error message text.
EID-3022	Requested action not allowed.	The requested action is not allowed.
EID-3023	Unable to retrieve low order cross connect mode.	Refer to error message text.
EID-3024	Unable to switch {0} cross connect mode. Please verify that the type and/or number of circuits provisioned does not exceed the criterion for switching modes.	CTC cannot switch the cross-connect mode for the specified item, as the type or the number of circuits does not match with the criterion for switching modes.
EID-3025	Error while retrieving thresholds.	There was an error retrieving the thresholds.
EID-3026	Cannot modify send DoNotUse.	You cannot modify the Send DoNotUse field.
EID-3027	Cannot modify SyncMsg.	You cannot modify the SyncMsg field.
EID-3028	Cannot change port type.	You cannot change the port type.
EID-3029	Unable to switch to the byte because an overhead change is present on this byte of the port.	Refer to error message text.
EID-3031	Error hard-resetting card.	There was an error while resetting card hardware.
EID-3032	Error resetting card.	There was an error while resetting the card.
EID-3033	The lamp test is not supported on this shelf.	Refer to error message text.
EID-3035	The cross connect diagnostics cannot be performed	Refer to error message text.
EID-3036	The cross connect diagnostics test is not supported on this shelf.	The cross-connect diagnostics test is not supported on this shelf.
EID-3037	A software downgrade cannot be performed to the selected version while a SSXC card is inserted in this shelf. Please follow the steps to replace the SSXC with a CXC card before continuing the software downgrade.	Refer to error message text.
EID-3038	A software downgrade cannot be performed at the present time.	Refer to error message text.
EID-3039	Card change error.	There was an error while changing the card.
EID-3040	Invalid card type.	The selected card type is invalid.
EID-3041	Error applying changes.	CTC is unable to create a protection group. Check if the protect port supports circuits, a timing reference, SONET SDCC, orderwire, or a test access point.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
EID-3042	The flow control low value must be less than the flow control high value for all ports in the card.	Refer to error message text.
EID-3043	Error while retrieving line info settings.	Refer to error message text.
EID-3044	Error while retrieving line admin info settings.	Refer to error message text.
EID-3045	Error while retrieving transponder line admin info settings.	Refer to error message text.
EID-3046	The flow control water mark value must be between {0} and {1}, inclusive.	The flow control watermark value must be between the two specified values.
EID-3047	The file named {0} could not be read. Please check the name and try again.	Refer to error message text.
EID-3048	There is no IOS startup config file available to download.	CTC could not find the configuration file for IOS startup.
EID-3049	There is an update in progress so the download cannot be done at this time.	Refer to error message text.
EID-3050	An exception was caught trying to save the file to your local file system.	Check whether the file already exists and cannot be over written, or there isa space constraint in the file system.
EID-3051	The maximum size for a config file in bytes is: {0}	The size of the configuration file should not exceed the specified number of bytes.
EID-3052	There was an error saving the config file to the TCC.	Refer to error message text.
EID-3053	The value of {0} must be between {1} and {2}	The value of the item must be between the specified values.
EID-3054	Cannot remove provisioned input/output ports or another user is updating the card, please try later.	Another user may be updating the card. You can try again later.
EID-3055	Cannot create soak maintance pane.	Refer to error message text.
EID-3056	Cannot save defaults to file {0}	CTC cannot save the defaults to the specified file.
EID-3057	Cannot load default properties from the node.	Refer to error message text.
EID-3058	File {0} does not exist.	Refer to error message text.
EID-3059	Error encountered while refreshing.	There was an error while refreshing.
EID-3060	The ALS Recovery Pulse Interval must be between {0} seconds and {1} seconds.	The automatic laser shutdown (ALS) Recovery Interval must be between the specified range of seconds.
EID-3061	The ALS Recovery Pulse Duration must be between {0} seconds and {1} seconds.	The automatic laser shutdown (ALS) Recovery Duration must be between the specified range of seconds.
EID-3062	Error encountered while setting values.	Refer to error message text.
EID-3063	Unable to retriever bridge port settings.	Refer to error message text.
EID-3064	Not a G1000 Card.	This card is not a G1000-4 card.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
EID-3065	An error was encountered while attempting to create RMON threshold: {0}	You must wait some time before you try again.
EID-3066	Minimum sample period must be greater than or equal to 10.	Refer to error message text.
EID-3067	Rising Threshold: Invalid Entry, valid range is from 1 to {0}	This is an invalid rising threshold entry. The valid range is from 1 to the specified value.
EID-3068	Falling Threshold: Invalid Entry, valid range is from 1 to {0}	This is an invalid falling threshold entry. The valid range is from 1 to the specified value.
EID-3069	Rising threshold must be greater than or equal to falling threshold.	Refer to error message text.
EID-3070	Error in data for ports {0} Exactly one VLAN must be marked untagged for each port. These changes will not be applied.	CTC encountered data error for the specified ports. Only one VLAN should be marked untagged for each port.
EID-3071	Get Learned Address	Unable to retrieve the learned MAC address from the NE.
EID-3072	Clear Learned Address	Failure attempting to clear the learned MAC address from a specific card or Ether group.
EID-3073	Clear Selected Rows	Failure attempting to clear the learned MAC address from a specific card or Ether group.
EID-3074	Clear By {0}	Error encountered trying to clear the learned MAC address from either a VLAN or a port.
EID-3075	At least one row in param column needs to be selected.	Refer to error message text.
EID-3076	CTC lost its connection with this node. The NE Setup Wizard will exit.	Refer to error message text.
EID-3077	No optical link selected.	Refer to error message text.
EID-3078	Unable to create optical link.	Refer to error message text.
EID-3079	Cannot apply defaults to node: {0}	CTC cannot apply the defaults to the specified node.
EID-3080	Cannot go to the target tab {0}	CTC cannot go to the specified target tab.
EID-3081	Port type cannot be changed.	Refer to error message text.
EID-3082	Cannot modify the {0} extension byte.	You cannot modify the specified extension byte.
EID-3083	Error while retrieving stats.	Error in getting statistics.
EID-3084	Error encountered while trying to retrieve laser parameters for {0}	There is no card, or there was an internal communications error when attempting to get the laser parameters for the card.
EID-3085	No OSC Terminations selected	Select an OSC termination and proceed.
EID-3086	One or more Osc terminations could not be created.	Refer to error message text.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
EID-3087	OSC termination could not be edited.	Refer to error message text.
EID-3088	No {0} card to switch.	No card of the specified type to switch.
EID-3089	Cannot use/change {0} state when {1} is failed or missing.	Cannot use or change the specified state when the card is failed or missing.
EID-3090	Cannot perform operation as {0} is {1}LOCKED_ON/LOCKED_OUT.	Cannot perform operation.
EID-3091	Cannot perform the operation as protect is active.	Refer to error message text.
EID-3092	Invalid service state. The requested action cannot be applied.	Select another service state and proceed.
EID-3093	Cannot perform the operation as duplex pair is {0}locked.	Refer to error message text.
EID-3094	Cannot perform the operation as no XC redundancy is available.	You cannot perform the requested operation on the cross connect card without having a backup cross connect card.
EID-3095	Deletion failed since the circuit is in use	Refer to error message text.
WID-3096	Internal communication error encountered while trying to retrieve laser parameters. This can happen when equipment is not present or when equipment is resetting. Check the equipment state and try to refresh the values again.	Refer to warning message text.
EID-3097	The ring termination is in use.	The ring termination you are trying to access is in use. Try after sometime.
EID-3098	No ring terminations selected.	Select one of the ring terminations.
EID-3099	Sorry, entered key does not match existing authentication key.	Check the authentication key and reenter.
EID-3100	Error encountered during authentication.	There was an error in authentication. Verify that the key does not exceed the character limit .
EID-3101	DCC Metric is not in the range 1 - 65535.	The DCC metric should be in the range of 1 to 65535.
EID-3102	Invalid DCC Metric	There was an invalid DCC metric.
EID-3103	Invalid IP Address: {0}	The IP address is invalid.
EID-3104	Router priority is not in the range of 0 - 255	The router priority should be in the range of 0 to 255.
EID-3105	Invalid Router Priority	The router priority is invalid.
EID-3106	Hello Interval is not in the range of 1 - 65535	The hello interval should be in the range of 1 to 65535.
EID-3107	Invalid Hello Interval	The hello interval is invalid.
EID-3109	Invalid Dead Interval value. Valid range is 1 - 2147483647	The dead interval value must be between 1 and 2147483647.
EID-3110	Dead Interval must be larger than Hello Interval	Refer to error message text.
EID-3111	LAN transit delay is not in the range of 1 - 3600 seconds	The LAN transit delay should be in the range of 1 to 3600 seconds.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
EID-3112	Invalid Transmit Delay	The transmit delay is invalid.
EID-3113	Retransmit Interval is not in the range 1 - 3600 seconds	The retransmit interval should be in the range of 1 to 3600 seconds.
EID-3114	Invalid Retransit Interval	The retransmit interval is invalid.
EID-3115	LAN Metric is not in the range 1 - 65535.	The LAN metric should be in the range of 1 to 65535.
EID-3116	Invalid LAN Metric	The LAN metric is invalid.
EID-3117	If OSPF is active on LAN, no DCC Area Ids may be 0.0.0.0. Please change all DCC Area Ids to non-0.0.0.0 values before enabling OSPF on the LAN.	Refer to error message text.
EID-3118	If OSPF is active on LAN, LAN Area ID may not be the same as DCC Area Id.	LAN must be part of a different OSPF area other than the DCC network.
EID-3119	Validation Error	CTC was unable to validate the values entered by the user. This error message is common to several different provisioning tabs within CTC (examples include the SNMP provisioning tab, the General> Network provisioning tab, the Security > Configuration provisioning tab, etc.).
EID-3120	No object of type {0} selected to delete.	Choose an object of the specified type to delete.
EID-3121	Error Deleting {0}	There is an error deleting the item.
EID-3122	No object of type {0} selected to edit.	Choose an object of the specified type to edit.
EID-3123	Error Editing {0}	There was an error editing the item.
EID-3124	{0} termination is in use. Delete the associated OSPF Range Table Entry and try again	Refer to error message text.
EID-3125	No {0} Terminations selected.	No specified terminations are selected.
EID-3126	{0} termination could not be edited.	CTC could not edit the specified termination.
EID-3127	Unable to provision orderwire because E2 byte is in use by {0}.	Refer to error message text.
EID-3128	The authentication key may only be {0} characters maximum	The authentication key cannot exceed the specified number of characters.
EID-3129	The authentication keys do not match!	Refer to error message text.
EID-3130	Error creating OSPF area virtual link.	CTC encountered an error while creating the area virtual link.
EID-3131	Error creating OSPF virtual link.	CTC encountered an error creating the virtual link.
EID-3132	Error setting OSPF area range: {0}, {1}, false.	CTC encountered an error while setting the area range for the specified values.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
EID-3133	Max number of OSPF area ranges exceeded.	OSPF area ranges exceeded the maximum number.
EID-3134	Invalid Area ID. Use DCC OSPF Area ID, LAN Port Area ID, or 0.0.0.0.	Refer to error message text.
EID-3135	Invalid Mask	Refer to error message text.
EID-3136	Invalid Range Address	The range address is invalid. Try again.
EID-3137	Your request has been rejected because the timing source information was updated while your changes were still pending. Please retry.	Refer to error message text.
EID-3138	Invalid clock source for switching.	You have selected an invalid clock source. Choose another clock.
EID-3139	Cannot switch to a reference of inferior quality.	Refer to error message text.
EID-3140	Higher priority switch already active.	You cannot switch the timing source manually when a higher priority switch is already active.
EID-3141	Attempt to access a bad reference.	Refer to error message text.
EID-3142	No Switch Active.	None of the switches are active.
EID-3143	Error creating static route entry.	CTC encountered an error while a creating static route entry.
EID-3144	Max number of static routes exceeded.	The number of static routes has exceeded its limit.
EID-3145	RIP Metric is not in the range 1-15.	The Routing Information Protocol (RIP) metric should be in the range of 1 to 15.
EID-3146	Invalid RIP Metric	Refer to error message text.
EID-3147	Error creating summary address.	There was an error while creating the summary address.
EID-3148	No Layer 2 domain has been provisioned.	You must provision any one of the layer 2 domain.
EID-3149	Unable to retrieve MAC addresses.	Refer to error message text.
EID-3150	The target file {0} is not a normal file.	The specified target file is not a normal file.
EID-3151	The target file {0} is not writeable.	The target file is not writeable. Specify another file.
EID-3152	Error creating Protection Group	CTC encountered an error creating Protection Group.
EID-3153	Cannot delete card, it is in use.	Cannot delete card. It is in use.
EID-3154	Cannot {0} card, provisioning error.	CTC cannot perform the task on the card.
EID-3155	Error Building Menu	CTC encountered an error building the menu.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
EID-3156	Error on building menu (cards not found for {0} group)	CTC encountered an error while building the menu, as cards could not be found for the specified group).
EID-3157	Unable to set selected model: unexpected model class {0}	CTC encountered an unexpected model class while trying to complete the task.
EID-3158	Unable to switch, a similar or higher priority condition exists on peer or far-end card.	Refer to error message text.
EID-3159[1]	Error applying operation.	CTC encountered an error while applying this operation.
EID-3160	{0} error encountered.	CTC encountered the specified error.
EID-3161	Ring Upgrade Error	An error was encountered while attempting to upgrade the BLSR. Refer to the details portion of the error dialog box for more information.
EID-3162	This protection operation cannot be set because the protection operation on the other side has been changed but not yet applied.	Refer to error message text.
EID-3163	Cannot validate data for row {0}	CTC cannot validate the data for the specified row.
EID-3164	New Node ID ({0}) for Ring ID {1} duplicates ID of node {2}	The new specified node ID for the specified ring ID is the same as another node ID.
EID-3165	The Ring ID provided is already in use. Ring IDs must be unique	Refer to error message text.
EID-3166	Error refreshing {0} table	CTC encountered an error while refreshing the specified table.
EID-3167	Slot already in use	Refer to error message text.
EID-3168	Provisioning Error	An error was encountered while attempting the specified provisioning operation. Refer to the details portion of the error dialog box for more information.
EID-3169	Error Adding Card	CTC encountered an error while adding the card.
EID-3170	Cannot delete card, {0}	Refer to error message text.
EID-3171	Error creating Trap Destination	CTC encountered an error creating the trap destination.
EID-3172	No RMON Thresholds selected	Select an RMON threshold.
EID-3173	The contact “{0}” exceeds the limit of {1} characters.	The specified contact exceeds the specified character limit.
EID-3174	The location “{0}” exceeds the limit of {1} characters.	The specified location exceeds the specified character limit.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
EID-3175	The operator identifier "{0}" exceeds the limit of {1} characters.	The specified operator identifier exceeds the specified character limit.
EID-3176	The operator specific information "{0}" exceeds the limit of {1} characters.	The specified operator specific information exceeds the specified character limit.
EID-3177	The node name cannot be empty.	The specified name is empty.
EID-3178	The name "{0}" exceeds the limit of {1} characters.	The specified name exceeds the specified character limit.
EID-3179	Protect card is in use.	Refer to error message text.
EID-3180	1+1 Protection Group does not exist.	Create a 1+1 protection group.
EID-3181	Y Cable Protection Group does not exist.	Refer to error message text.
EID-3182	The Topology Element is in use and cannot be deleted as requested	You cannot delete the topology element which is in use.
EID-3183	Error Deleting Protection Group	CTC encountered an error while deleting the protection group.
EID-3184	No {0} selected.	You must select an item before completing this task.
EID-3185	There is a protection switch operation on this ring. Therefore, it cannot be deleted at this time.	Refer to error message text.
EID-3186	Busy: {0} is {1} and cannot be deleted as requested.	The request cannot be completed.
EID-3187	Error deleting trap destination.	CTC encountered an error deleting the trap destination.
EID-3214	Could not get number of HOs for line.	The number of High Orders for line is not available.
EID-3215	Error in refreshing.	Used frequently in pane classes to indicate a general error condition when trying to refresh from the model.
EID-3216	Invalid proxy port.	Refer to error message text.
EID-3217	Could not refresh stats.	CTC could not refresh statistics values.
EID-3218	Unable to launch automatic node setup.	Refer to error message text.
EID-3219	Unable to refresh automatic node setup information.	Failure trying to retrieve automatic node setup information.
EID-3220	Error refreshing row {0}	Error refreshing the specified row.
EID-3222	Could not clear stats.	Refer to error message text.
EID-3223	Error cancelling software upgrade.	CTC encountered an error while cancelling the upgrade. Software is not upgraded.
EID-3224	Error accepting load.	Refer to error message text.
EID-3225	Error while refreshing pane.	Used frequently in pane classes to indicate a general error condition when trying to refresh from the model.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
EID-3226	{0} termination(s) could not be deleted. {1}	Refer to error message text.
EID-3227	Unable to record a baseline, performance metrics will remain unchanged.	CTC failed to set the baseline values while provisioning NE. Previous values remain unchanged.
EID-3228	{0} termination(s) could not be created. {1}	Refer to error message text.
EID-3229	RIP is active on the LAN. Please disable RIP before enabling OSPF.	Turn off the Routing Information Protocol (RIP) on the LAN, before enabling OSPF.
EID-3230	OSPF is active on the LAN. Please disable OSPF before enabling RIP.	Turn off the OSPF on the LAN before enabling RIP.
EID-3231	Error in Set OPR	An error was encountered while attempting to provision the optical power received (OPR).
WID-3232	Cannot transition port state indirectly because the port is still providing services: if the port state should be changed, edit it directly via port provisioning.	Edit the port state while provisioning the port.
EID-3233	Current loopback provisioning does not allow this state transition.	Refer to error message text.
EID-3234	Current synchronization provisioning does not allow this state transition	You cannot transition the port state to the target date while in the current synchonization state.
EID-3235	Cannot perform requested state transition on this software version.	Refer to error message text.
EID-3236	Database Restore failed. {0}	CTC failed to restore the specified database.
EID-3237	Database Backup failed. {0}	CTC failed to backup the specified database.
EID-3238	Send PDIP setting on {0} is inconsistent with that of control node {1}	The send payload defect indicator path (PDI-P) setting on the specified item should be consistent with that of the specified control node.
EID-3239	The overhead termination is invalid	Refer to error message text.
EID-3240	The maximum number of overhead terminations has been exceeded.	Overhead terminations have exceeded the limit.
EID-3241	The {0} termination port is in use.	The specified termination port is in use. Select another port.
EID-3242	{1} exists on the selected ports. Please create {0} one by one.	The specified DCC already exists on the selected port. You may create a DCC of another type.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
WID-3243	The port you have chosen as an {0} endpoint already supports an {1}. The port cannot support both DCCs. After the {0} is created, verify that no EOC alarms are present and then delete the {1} to complete the downgrade.	The same port can not be used by multiple DCCs.
EID-3244	{0} exists on the selected ports. Please create {1} one by one.	The specified DCC already exists on the selected port. You may create a DCC of another type.
WID-3245	The port you have chosen as an {1} endpoint already supports an {0}. The port cannot support both DCCs. After the {1} is created, verify that no EOC alarms are present and then delete the {0} to complete the upgrade.	The port selected as a DCC endpoint already supports another DCC. Refer to warning message text.
EID-3246	Wizard unable to validate data: {0}	CTC encountered an error.
EID-3247	Ordering error. The absolute value should be {0}	The absolute value entered was wrong.
EID-3248	Wrong parameter is changed: {0}	CTC changed the incorrect parameter.
EID-3249	Invalid voltage increment value.	Refer to error message text.
EID-3250	Invalid power monitor range.	Refer to error message text.
EID-3251	Unable to complete requested action. {0}	CTC could not complete the specified action.
EID-3252	No download has been initiated from this CTC session.	Refer to error message text.
EID-3253	Reboot operation failed. {0}	Refer to error message text.
EID-3254	Validation Error. {0}	The Cisco Transport Controller (CTC) was unable to validate the values entered by the user, specified by {0}. This error message is common to several different provisioning tabs within the CTC.
EID-3255	Cannot change timing configuration, manual/force operation is performed.	Refer to error message text.
WID-3256	Could not assign timing reference(s) because - at least one timing reference has already been used and/or - a timing reference has been attempted to be used twice. Please use the “Reset” button and verify the settings.	Refer to warning message text.
EID-3257	Duplicate DCC number detected: {0}.	CTC detected more than one occurene of the a DCC number. Remove one of them.
EID-3258	There was a software error attempting to download the file. Please try again later.	Refer to error message text.
EID-3259	Create FC-MR Threshold	You must create a Fibre Channel Multirate (FC_MR) card threshold.
EID-3260	An error was encountered while provisioning the internal subnet: {0}	The specified internal subnet could not be provisoned.
EID-3261	The port rate provisioning cannot be changed while circuits exist on this port.	Refer to error message text.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
EID-3262	The port provisioning cannot be changed when the port status is not OOS.	You must provision the ports only when the port is Out of Service.
WID-3263	You are using Java version {0}. CTC should run with Java version {1}. It can be obtained from the installation CD or http://java.sun.com/j2se/	CTC is being launched with the wrong version of the JRE {0}. This version of CTC requires a particular version of the JRE {1}. The CTC and browser must be closed and restarted to allow the correct Java version to be loaded.
EID-3264	The port provisioning cannot be changed while the port is {0}.	You must modify the port provisioning only when the port is out of service.
EID-3265	Error modifying Protection Group	Protection Group could not be modified.
EID-3266	Conditions could not be retrieved from the shelf or card view.	Refer to error message text.
WID-3267	Cannot edit XTC protection group.	Refer to warning message text.
WID-3268	Invalid entry. {0}	The specified entry is invalid.
WID-3269	{0} was successfully initiated for {1} but its completion status was not able to be obtained from the node. {0} may or may not have succeeded. When the node is accessible, check its software version.	Refer to error message text.
WID-3270	The file {0} does not exist.	The specified file does not exist.
WID-3271	The value entered must be greater than {0}.	The value entered must be greater than the specified value.
WID-3272	Entry required	An entry is required to complete this task.
WID-3273	{0} already exists in the list.	The specified item already exists in the list.
WID-3274	A software upgrade is in progress. Network configuration changes that results a node reboot can not take place during software upgrade. Please try again after software upgrade is done.	Refer to warning message text.
WID-3275	Make sure the Remote Interface ID and the Local Interface ID on the two sides are matched. (Local Interface ID on this node should equal Remote Interface ID on the neighbor node and vice-versa.)	Refer to warning message text.
WID-3276	Both {0} and {1} exist on the same selected port. {2}	The specified port has both SDCC and LDCC.
WID-3277	The description cannot contain more than {0} characters. Your input will be truncated.	The input exceeds the character limit. The value will be truncated to the maximum chacter limit.
WID-3279	Card deleted, returning to shelf view.	CTC returns to node view.
WID-3280	ALS will not engage until both the protected trunk ports detect LOS.	Refer to warning message text.
WID-3281	A software upgrade is in progress. {0} can not proceed during a software upgrade. Please try again after the software upgrade has completed.	Refer to warning message text.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
WID-3282	Performing a software upgrade while TSC 5 is active could result in a service disruption. It is recommended that you make TSC 10 the active TSC by performing a soft reset of TSC 5. The following 15600s are currently unsafe to upgrade...	Refer to warning message text.
WID-3283	Before activating a new version, make sure you have a database backup from the current version.	Refer to warning message text.
WID-3284	Reverting to an older version.	CTC is being reverted to an older version of application.
WID-3285	Applying FORCE or LOCKOUT operations may result in traffic loss.	Refer to warning message text.
WID-3286	The ring status is INCOMPLETE. CTC cannot determine if there are existing protection operations or switches in other parts of the ring. Applying a protection operation at this time could cause a traffic outage. Please confirm that no other protection operations or switches exist before continuing.	Refer to warning message text.
WID-3287	There is a protection operation or protection switch present on the ring. Applying this protection operation now will probably cause a traffic outage.	Refer to warning message text.
WID-3288	This ring status is INCOMPLETE. CTC will not be able to apply this change to all of the nodes in the {0}.	Change the ring status to apply the change to all nodes in the ring type.
EID-3290	Unable to delete specified provisionable patchcord(s).	Refer to error message text.
EID-3291	Cannot change revertive behavior due to an active protection switch.	Protection switch should not be active to change the revertive behaviour.
EID-3292	Error resetting shelf.	CTC encountered an error while resetting the node.
EID-3293	No such provisionable patchcord.	You are attempting to delete a provisionable patchcord that does not exist. This happens when multiple instances of CTC are running and attempting to delete the same provisionable patchcord concurrently.
EID-3294	No RMON thresholds available for selected port.	Refer to error message text.
EID-3295	This card does not support RMON thresholds.	Refer to error message text.
EID-3296	Buffer-to-buffer credit is only supported for Fibre Channel (FC) and FICON.	Refer to error message text.
EID-3298	ALS Auto Restart is not supported by this interface.	Refer to error message text.
EID-3300	Can not have duplicate OSPF area IDs.	OSPF area IDs should be unique.
EID-3301	LAN metric may not be zero.	Refer to error message text.
EID-3302	Standby {0} not ready.	Standby controller card is not ready.
EID-3303	DCC Area ID and {0} conflict. {1}	DCC Area ID and ring type, specified by {0}, conflict each other due to the details specified by {1}.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
EID-3304	DCC number is out of range.	Enter a DCC number that is within the range
EID-3305	Can not have OSPF turned on on the LAN interface and the back bone area set on a DCC interface.	You cannot have the default OSPF area on a DCC while OSPF is enabled on the LAN.
EID-3306	Ethernet circuits must be bidirectional.	Refer to error message text.
EID-3307	Error while creating connection object at {0}.	CTC encountered an error at the specified connection while creating the connection.
EID-3308	DWDM Link can be used only for optical channel circuits.	Refer to error message text.
EID-3309	OCH-NC circuit: link excluded - wrong direction.	The optical channel (circuit) does not allow the specified link to be included because it is in the wrong optical direction.
EID-3310	DWDM Link does not have wavelength available.	Refer to error message text.
EID-3311	Laser already on.	Refer to error message text.
EID-3312	Unable to change the power setpoint {0} {1}	CTC cannot change change the power setpoint. The new setpoint would either make the thresholds inconsistent or set the fail threshold outside the range.
EID-3313	Unable to modify offset. Amplifier port is in service state.	Refer to error message text.
EID-3314	Requested action not allowed. Invalid state value.	Refer to error message text.
EID-3315	Unable to perform operation.	CTC is unable to perform operation.
EID-3316	Wrong node side.	This task was applied to the wrong node side.
EID-3317	Name too long.	Reduce the number of charcters in the name.
EID-3318	Illegal name.	The name you entered is illegal.
EID-3319	Wrong line selection.	Select another line
EID-3320	Unable to delete optical link.	CTC cannot delete the optical link.
EID-3321	This feature is unsupported by this version of software.	Refer to error message text.
EID-3322	Equipment is not plugged-in.	Plug-in the equipment and proceed.
EID-3323	APC system is busy.	Automatic Power Control (APC) system is busy.
EID-3324	No path to regulate.	There is no circuit path to regulate.
EID-3325	Requested action not allowed.	Generic DWDM provisioning failure message.
EID-3326	Wrong input value.	The input value is incorrect.
EID-3327	Error in getting thresholds.	There was an error retrieving the thresholds. This message is displayed only for the OSCM/OSC-CSM line thresholds.
EID-3328	Error applying changes to row {0}.Value out of range.	There was an error applying the changes to the specified row. The value is out of range.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
EID-3330	Unable to switch to the byte because an overhead channel is present on this byte of the port.	Refer to error message text.
EID-3331	Error applying changes to row.	Refer to error message text.
EID-3334	Cannot change timing parameters on protect port.	You cannot change timing parameters on protect port.
EID-3335	The type of this port cannot be changed: SDH validation check failed. Check if this port is part of a circuit, protection group, SONET DCC, orderwire, or UNI-C interface.	Refer to error message text.
EID-3336	Error on reading a control mode value.	The Control Mode must be retrieved.
EID-3337	Error on setting a set point gain value.	The Gain Set Point must be set.
EID-3338	Error on reading a set-point gain value.	The Gain Set Point must be retrieved.
EID-3339	Error on setting a tilt calibration value.	The tilt calibration must be set.
EID-3340	Error on setting expected wavelength.	The expected wavelength must be set.
EID-3341	Error on reading expected wavelength.	The expected wavelength must be retrieved.
EID-3342	Error on reading actual wavelength.	The actual wavelength must be retrieved.
EID-3343	Error on reading actual band.	The actual band must be retrieved.
EID-3344	Error on reading expected band.	The expected band must be retrieved.
EID-3345	Error on setting expected band.	The expected band must be set.
EID-3346	Error retrieving defaults from the node: {0}.	There was an error retrieving defaults from the specified node.
EID-3347	Cannot load file {0}.	CTC cannot load the specified file.
EID-3348	Cannot load properties from the node.	Refer to error message text.
EID-3349	Cannot save NE Update values to file.	Check your file system for space constraint or any other problem.
EID-3350	Cannot load NE Update properties from the node:	Refer to error message text.
EID-3351	File {0} does not exist.	The specified file does not exist.
EID-3352	Error on setting value at {0}.	There was an error while setting the value at the specified location.
EID-3353	There is no such interface available.	The interface specified is not present in CTC.
EID-3354	Specified endpoint is in use.	Select another endpoint that is not in use.
EID-3355	Specified endpoint is incompatible.	Refer to error message text.
EID-3357	Unable to calculate connections.	Refer to error message text.
EID-3358	Optical link model does not exist for specified interface.	Create an optical linkmodel for the interface, and proceed.
EID-3359	Unable to set optical parameters for the node.	Refer to error message text.
EID-3361	Ring termination is in use. Error deleting ring termination	You cannot delete a ring in use.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
EID-3362	Error deleting ring termination.	There was an error while deleting ring termination.
EID-3363	No ring terminations selected.	You must select a ring termination.
EID-3364	Error creating ring ID.	There was an error while creating the ring ID.
EID-3365	OSC termination is in use.	Select another optical service channel (OSC) which is not in use.
EID-3366	Unable to delete OSC termination.	There was an error deleting the OSC termination.
EID-3370	No optical link has been selected	You must select an optical link.
EID-3371	Error while calculating automatic optical link list.	Refer to error message text.
EID-3372	Attempt to access an OCH-NC connection that has been destroyed.	CTC destroyed an external attempt to access an optical channel network connection.
EID-3375	Expected span loss must be set.	Refer to error message text.
EID-3376	Unable to retrieve measured span loss.	Refer to error message text.
EID-3377	Wrong interface used.	The interface used for the card is wrong.
EID-3378	Duplicate origination patchcord identifier.	The provisionable patchcord identifier to the patchcord you are attempting to provision is already in use by another patchcord on the origination node.
EID-3379	Duplicate termination patchcord identifier.	The provisionable patchcord identifier to the patchcord you are attempting to provision is already in use by another patchcord on the remote node.
EID-3380	Unable to locate host.	Refer to error message text.
EID-3381	Maximum Frame size must be between {0} and {1} and may be increased in increments of {2}.	The frame size must be in the specified range. This can incremented by the specified value.
EID-3382	Number of credits must be between {0} and {1}.	The number of credits must be between the specified values.
EID-3383	GFP Buffers Available must be between {0} and {1} and may be increased in increments of {2}.	The GFP buffers must be in the specified range. This can incremented by the specified value.
WID-3384	You are about to force the use of Secure Mode for this chassis. You will not be able to undo this operation. OK to continue?	Refer to warning message text.
EID-3385	{0}. Delete circuits, then try again.	Refer to error message text.
EID-3386	Unable to provision transponder mode: {0}	The specified transponder mode canot be provisioned.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
EID-3387	You must change port{0} to an out-of-service state before changing card parameters. Click Reset to revert the changes.	All the card ports should be changed to out-of-service before changing the parameters.
EID-3388	Unable to change the card mode because the card has circuits.	Refer to error message text.
EID-3389	Error encountered while changing the card mode.	Refer to error message text.
EID-3390	Port is in use.	Refer to error message text.
EID-3391	Unable to change the port rate because the port has been deleted.	You cannot change the port rate of a card that has been deleted.
WID-3392	Could not assign timing reference(s) because - with external timing, only a single protected, or two unprotected timing references per BITS Out may be selected. Please use the "Reset" button and verify the settings.	Refer to warning message text.
WID-3393	Could not assign timing reference(s) because - with line or mixed timing, only a single unprotected timing reference per BITS Out may be selected. Please use the "Reset" button and verify the settings.	Refer to warning message text.
EID-3394	Error refreshing Power Monitoring values.	Refer to error message text.
EID-3395	Invalid Configuration: {0}	CTC encountered an error in IP address, net mask length, or default router, or a restricted IIOP port was selected.
EID-3396	Invalid Configuration: The standby controller card is not a TCC2P card.	The standby controller card should be a TCC2P card.
EID-3397	Wrong version for file {0}.	The specified file is of wrong version.
EID-3398	Cannot delete PPM.	Refer to error message text.
EID-3399	Cannot delete PPM. It has port(s) in use.	Remove the ports coonected to the Pluggable Port Module before it can be deleted.
EID-3400	Unable to switch, force to Primary Facility not allowed.	Refer to error message text.
EID-3401	{0} cannot be provisioned for the port while {1} is enabled.	The relationship between parameters {0} and {1} are such that enabling either one, prevents the provisioning of the other.
EID-3402	Unable to complete the switch request. The protect card is either not present or is not responding. Try again after ensuring that the protect card is present and is not resetting.	Refer to error message text.
EID-3403	Admin state transition has not been attempted on the monitored port.	Refer to error message text.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
EID-3404	The far end IP address could not be set on the {0} termination. The IP address cannot be: loopback (127.0.0.0/8) class D (224.0.0.0/4) class E (240.0.0.0/4) broadcast (255.255.255.255/32) internal {1}	Refer to error message text.
EID-4000	The {0} ring name cannot be changed now. A {0} switch is active.	You cannot change the ring name because a switch of the same ring type is active.
EID-4001	The {0} ring ID cannot be changed now. A {0} switch is active.	You cannot change the ring ID because a switch of the same ring type is active.
WID-4002	CAUTION: Reverting to an earlier software release may result in TRAFFIC LOSS and loss of connectivity to the node. It may require onsite provisioning to recover. If the node was running 7.0.0 before, reverting will restore the 7.0.0 provisioning, losing any later provisioning. If the node was running some other version, reverting will LOSE ALL PROVISIONING. Also, any FPGA downgrades that occur while reverting might affect traffic. OK to continue?	Refer to warning message text.
EID-5000	Cannot find a valid route for tunnel change request.	Refer to error message text.
EID-5001	Tunnel could not be changed.	Refer to error message text.
EID-5002	Tunnel could not be restored and must be recreated manually.	Refer to error message text.
EID-5003	Circuit roll failure. {0}	Refer to error message text.
EID-5004	There is already one 4F {0} provisioned on the set of nodes involved in {1}. The maximum number of 4F {0} rings has been reached for that node.	There is already one 4F BLSR provisioned on the set of nodes involved in the ring. The maximum number of 4F BLSR rings has been reached for that node.
WID-5005	A non-zero hold-off time can violate switching time standards, and should only be used for a circuit with multiple path selectors.	Refer to warning message text.
WID-5006	Warning: Different secondary {0} node should only be used for DRI or Open-ended path protected circuits.	You should use different secondary end point only for DRI or open-ended path protected circuits.
WID-5007	If you change the scope of this view, the contents of this profile editor will be lost.	Refer to warning message text.
WID-5008	Please make sure all the protection groups are in proper state after the cancellation.	Refer to warning message text.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
WID-5009	Circuit {0} not upgradable. No {1} capable {2}s are available at node {3}.	No VT capable STSs are available at the node.
EID-5010	Domain name already exists.	Refer to error message text.
EID-5011	Domain name may not exceed {0} characters.	You may have reached the maximum number of charcters.
WID-5012	Software load on {0} does not support the addition of a node to a 1+1protection group.	Refer to warning message text.
EID-5013	{0} doesn't support Bridge and Roll Feature. Please select a different port.	The specified port does not support Bridge and Roll.
EID-5014	An automatic network layout is already in progress, please wait for it to complete for running it again.	You must for the automatic network layout to complete before running it again.
WID-5015	{0} cannot be applied to {1}.	You cannot apply the admin state operation, specified by {0}, to port count, specified by {1}.
EID-5016	An error was encountered while attempting to provision the {0}. {1}	CTC encountered an error while provisioning the card.
EID-5017	Unable to rollback provisioning, the {0} may be left in an INCOMPLETE state and should be manually removed.	You may have to remove the BLSR manually as it was left incomplete.
EID-5018	{0} is {1} node and cannot be added to {2} network.	You cannot add the node {0} of type {1} to the host node of type {2}. This prevents you from hosting both SONET and SDH nodes in the same session.
EID-5019	Manual mode for this equipment does not support an expected string consisting of all null characters. Please change the expected string or the path trace mode.	The path trace mode does not support strings that consist of null characters. You must either change the expected string or the path trace mode.
WID-5020	Unable to transition port state indirectly because the port aggregates low order circuits: if the port state should be changed, edit it directly via port provisioning	Refer to warning message text.
EID-5021	No nodes are selected. Please choose a node.	Refer to error message text.
WID-5022	Warning: Ethergroup circuits are stateless (i.e., always in service). Current state selection of {0} will be ignored.	Refer to warning message text.
EID-5023	Unable to communicate with node. Operation failed.	CTC encountered a network communication error. Connectivity between CTC and the NE was disrupted, either transiently or permanently.
EID-5024	Overhead circuit will not be upgraded.	Refer to error message text.
WID-5025	The path targeted for this switch request is already active. The switch request can be applied, but traffic will not switch at this time.	Refer to warning message text.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
EID-5026	A 15600 cannot serve as the primary or secondary node in a 4 Fiber {0} circuit. Please change your ring and/or node selections so that a 15600 is not chosen as the primary or secondary node in this 4 Fiber {1} circuit.	Refer to error message text.
WID-5027	The {0} Edit Window for {1} has been closed due to significant provisioning changes. These changes may only be transitory, so you may re-open the {0} Edit Window to view the updated state.	Re-open the BLSR/MS-SPRing edit window to view the updated state of the node.
WID-5028	Warning: This operation should only be used to clean up rolls that are stuck. It may also affect completeness of the circuit. Continue with deletion?	Refer to warning message text.
EID-5033	Unable to load profile. Error decoding characters.	CTC detected an error while decoding characters and could not load the profile.
EID-5034	Unable to load profile. File format error.	CTC detected an error and could not load the profile.
EID-5035	Unable to load profile. File read error.	CTC could not read the file ad hence not able to load the profile.
EID-6000	Platform does not support power monitoring thresholds	Refer to error message text.
EID-6001	One of the XC cards has failures or is missing.	Check whether all the cross connect cards are installed and are working.
EID-6002	One of the XC cards is locked.	Unlock the cross connect card.
EID-6003	Unable to create OSC termination. Ring ID already assigned.	Enter a new ID for the ring and proceed.
EID-6004	Unable to perform a system reset while a BLSR ring is provisioned on the node.	Remove the BLSR ring from the node and proceed with the reset procedure.
EID-6005	Could not assign timing references: - Only two DS1 or BITS interfaces can be specified. - DS1 interfaces cannot be retimed and used as a reference - BITS-2 is not supported on this platform.	Refer to error message text.
EID-6006	Could not assign timing references: - NE reference can only be used if timing mode is LINE. - A BITS reference can only be used if timing mode is not LINE. - A line reference can only be used if timing mode is not EXTERNAL.	Refer to error message text.
WID-6007	Cancelling a software upgrade during standby TSC clock acquisition may result in a traffic outage.	Refer to warning message text.
EID-6008	SF BER and SD BER are not provisionable on the protect line of a protection group.	SF BER and SD BER cannot be provisioned in a protect card as these values are inherited by the protect card or group from the card for which it is offering protection.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
WID-6009	If Autoadjust GFP Buffers is disabled, GFP Buffers Available must be set to an appropriate value based on the distance between the circuit end points.	Refer to warning message text.
WID-6010	If Auto Detection of credits is disabled, Credits Available must be set to a value less than or equal to the number of receive credits on the connected FC end point.	Refer to warning message text.
WID-6011	Idle filtering should be turned off only when required to operate with non-Cisco Fibre Channel/FICON-over-SONET equipment.	Refer to warning message text.
EID-6012	Could not change the retiming configuration. There are circuits on this port.	You cannot change the timing configuration on this port unless the circuits on this port are deleted.
EID-6013	NTP/SNTP server could not be changed. {1}	Refer to error message text.
EID-6014	Operation failed. The reference state is OOS.	Change the Out-of-service state to Active.
EID-6015	Distance Extension cannot be disabled if the port media type is FICON 1Gbps ISL or FICON 2Gbps ISL.	Refer to error message text.
EID-6016	Card mode cannot be changed to Fibre Channel Line Rate if the port media type is FICON 1Gbps ISL or FICON 2Gbps ISL.	Refer to error message text.
EID-6017	The destination of a {0} route cannot be a node IP address.	A node IP address cannot be the destination for a static route.
EID-6018	The destination of a {0} route cannot be the same as the subnet used by the node.	Refer to error message text.
EID-6019	The destination of a static route cannot be 255.255.255.255	The network address such as 255.255.255.255 is not valid. Enter a valid address.
EID-6020	The destination of a static route cannot be the loopback network (127.0.0.0/8)	Refer to error message text.
EID-6021	The subnet mask length for a non-default route must be between 8 and 32.	Length of subnet mask must be within the specified range.
EID-6022	The subnet mask length for a default route must be 0.	Refer to error message text.
EID-6023	The destination of a {0} route cannot be an internal network{1}.	The destination of a static route must not be an internal network.
EID-6024	The destination of a {0} route cannot be a class D (224.0.0.0/4) or class E (240.0.0.0/4) address.	The destination of a static route must not be a class D or class E address.
EID-6025	The destination of a {0} route cannot be a class A broadcast address (x.255.255.255/8)	The destination of a static route must not be a class A broadcast address. It should be (xxx.0.0.0).
EID-6026	The destination of a {0} route cannot be a class B broadcast address (x.x.255.255/16)	The destination of a static route must not be a class B broadcast address.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
EID-6027	The destination of a {0} route cannot be a class C broadcast address (x.x.x.255/24)	The destination of a static route must not be a class C broadcast address.
EID-6028	The destination of a {0} route cannot be the subnet broadcast address associated with a node IP address.	The destination of a static route must not be a subnet broadcast address of a node IP.
EID-6029	The next hop of a static route cannot be the same as the destination of the route or an internal network{0}.	Static route must have the default route as the next hop, and not destination of the route or internal network.
EID-6030	The next hop of a static default route must be the provisioned default router.	The default route is selected for networks that do not have a specific route.
EID-6031	No more static routes can be created.	You have reached the maximum number of static routes.
EID-6032	This static route already exists.	Refer to error message text.
EID-6033	Previous operation is still in progress.	Another operation is in progress. You must try after sometime.
EID-6035	Parent entity does not exist.	Refer to error message text.
EID-6036	Parent PPM entity does not exist.	Create a parent entity for PPM.
EID-6037	Equipment type is not supported.	CTC does not support this equipment.
EID-6038	Invalid PPM port.	Refer to error message text.
EID-6039	Card is part of a regeneration group.	Select another card.
EID-6040	Out of memory.	Refer to error message text.
EID-6041	Port is already present.	Refer to error message text.
EID-6042	Port is used as timing source.	Choose another port as the selected port is being used as timing source.
EID-6043	DCC or GCC is present.	Refer to error message text.
EID-6044	Card or port is part of protection group.	Refer to error message text.
EID-6045	Port has overhead circuit(s).	Refer to error message text.
EID-6046	G.709 configuration is not compatible with data rate.	Refer to error message text.
EID-6047	Port cannot be deleted because its service state is OOS-MA,LPBK&MT.	To delete the port, you must change the port state to OOS-DSBLD.
EID-6048	{0} is {1}.	Trunk port is in the wrong state to carry out the action.
EID-6049	Mode {0} is not supported.	CTC does not support the mode of operation requested on the card.
EID-6050	Some {0} terminations were not {1}d. {2}	Refer to error message text.
WID-6051	All {0} terminations were {1}d successfully. {2}	Refer to warning message text.
EID-6052	The authentication key can not be blank.	Enter an authentication key.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
EID-6053	No more SNMP trap destinations can be created.	You have reached the maximum number of SNMP trap destinations.
EID-6054	{0} is not a valid IP address for an SNMP trap destination.	The IP address specified is invalid as the receiver of SNMP traps
EID-6055	The IP address is already in use.	Refer to error message text.
EID-6056	Invalid SNMP trap destination. {0}	The specified SNMP trap destination is invalid. Choose another destination.
WID-6057	Changing the card mode will result in an automatic reset.	Refer to warning message text.
EID-6058	Max number of GRE tunnels exceeded.	Refer to error message text.
EID-6059	The specified GRE tunnel already exists!	Specify another GRE tunnel.
EID-6060	Cannot {0} GRE tunnel entry: {1}.	Refer to error message text.
EID-6061	Error deleting GRE tunnel entry.	CTC encountered an error while deleting the GRE tunnel entry.
EID-6062	Selected GRE tunnel does not exist.	Create a GRE tunnel and proceed.
EID-6063	Selected router does not exist.	Create a router and proceed.
EID-6064	MAA address list is full.	Refer to error message text.
EID-6065	Selected area address is duplicated.	Enter another area address.
EID-6066	Primary area address can not be removed.	Refer to error message text.
EID-6067	Selected area address does not exist.	Choose another area address.
EID-6068	The GRE NSEL may not be modified while there are GRE Tunnel Routes provisioned.	You can not change the NSEL address if there are tunnels provisioned.
EID-6069	The node is currently in ES mode. Only router #1 may be provisioned.	An End System needs only one provisioned router.
EID-6070	No router selected.	Select a router.
EID-6071	Cannot flush TARP data cache.	You cannot flush the cache in the Tunnel identifier Address Resolution Protocol (TARP) state.
EID-6072	Cannot add TARP data cache entry: {0}	You cannot add the specified cache entry.
WID-6073	TARP request has been initiated. Try refreshing TARP data cache later.	Refer to warning message text.
EID-6074	End System mode only supports one subnet.	Refer to error message text.
EID-6075	Trying to remove MAT entry that does not exit.	CTC is removing the non-existant MAT entry.
EID-6076	Cannot {0} TARP manual adjacency entry: {1}	CTC can not add the specified adjacency entry for reasons unknown.
EID-6077	Area address shall be 1 to 13 bytes long.	Area address should not be more than 13 characters.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
EID-6078	TDC entry with TID {0} does not exist in the table.	The specified Tunnel Identifier does not exist.
EID-6079	Unable to remove TDC entry with TID {0}. Please verify that TARP is enabled.	You must enable TARP inorder to remove the TDC entry.
WID-6080	Router #{0} does not have an area address in common with router #1. Switching from IS L1/L2 to IS L1 in this case will partition your network.	Refer to warning message text.
EID-6081	The limit of 10 RADIUS server entries has been reached.	CTC does not allow more than 10 RADIUS servers.
EID-6082	{0} cannot be empty.	The Shared Secrets field should not be empty.
EID-6083	The entry you selected for editing has been altered by other. Changes cannot be committed.	Refer to error message text.
EID-6084	The RADIUS server entry already exists.	Specify another RADIUS server entry.
WID-6085	Disabling shell access will prevent Cisco TAC from connecting to the vxWork shell to assist users.	Refer to warning message text.
EID-6086	Cannot change card. Card resources are in use.	The card you are trying to remove is being used. Cannot change the card.
EID-6087	Cannot change card. The new card type is invalid or incompatible.	Refer to error message text.
EID-6088	This line cannot be put into loopback while it is in use as a timing source	Refer to error message text.
EID-6089	Interface not found. {0}	CTC cannot find the specified interface.
EID-6090	Interface type not valid for operation. {0}	Choose another interface.
EID-6091	The interface's current state prohibits this operation. {0}	The port is in an invalid state to set loopback.
EID-6092	Operation prohibited for this interface. {0}	CTC does not allow this operation for the specified interface.
EID-6093	Max number of Tarp Data Cache entry exceeded.	You have exceeded the allowed number of characters.
EID-6094	Max number of Manual Adjacency Table entry exceeded.	Refer to error message text.
EID-6095	Invalid Ais/Squelch mode.	Refer to error message text.
EID-6096	Default GRE tunnel route is only allowed on a node without a default static route and a default router of 0.0.0.0	Refer to error message text.
EID-6097	The authorization key does not comply with IOS password restrictions. {0}	Specify another authorization key.
EID-6098	Default static route is not allowed when default GRE tunnel exists	Refer to error message text.
EID-6099	You cannot create a subnet on a disabled router.	Create the subnet on an active router.

Table 4-1 Error Messages (continued)

Error or Warning ID	Error or Warning Message	Description
WID-6100	Disabling a router that has a provisioned subnet is not recommended.	Refer to warning message text.
EID-6101	The MAT entry already exists.	Refer to error message text.
WID-6102	The new card has less bandwidth than the current card. Circuits using VT15 and higher will be deleted.	Refer to warning message text.
EID-6103	The TDC entry already exists.	Specify another entry for TARP Data Cache.
EID-6104	APC ABORTED.	Automatic Power Control is aborted.
EID-6105	The 'Change Card' command is valid for MRC cards only when port 1 is the sole provisioned port.	Refer to error message text.
EID-6106	To delete all RADIUS server entries, RADIUS authentication must be disabled.	Disable Radius authentication and proceed.
EID-6107	The node failed to restart the TELNET service on the selected port. Try using another unreserved port that is not being used within the following ranges: 23, 1001-9999.	Refer to error message text.
EID-6108	There is an active TELNET session.	Restart a TELNET session.

1. EID-3159 can appear if you attempt to perform another switching operation within a certain time interval. This interval is an algorithm of three seconds per working card in the protection group. The maximum interval is 10 seconds.

CHAPTER 5

Performance Monitoring

Performance monitoring (PM) parameters are used by service providers to gather, store, set thresholds for, and report performance data for early detection of problems. In this chapter, PM parameters and concepts are defined for electrical cards, Ethernet cards, optical cards, multirate cards, storage access networking (SAN) cards, and dense wavelength division multiplexing (DWDM) cards in the Cisco ONS 15454.

For information about enabling and viewing PM values, refer to the *Cisco ONS 15454 Procedure Guide*.

Chapter topics include:

Note For additional information regarding PM parameters, refer to Telcordia documents GR-1230-CORE, GR-820-CORE, GR-499-CORE, and GR-253-CORE and the ANSI T1.231 document entitled *Digital Hierarchy - Layer 1 In-Service Digital Transmission Performance Monitoring*.

5.1 Threshold Performance Monitoring

Thresholds are used to set error levels for each PM parameter. You can set individual PM threshold values from the Cisco Transport Controller (CTC) card view Provisioning tab. For procedures on provisioning card thresholds, such as line, path, and SONET thresholds, refer to the *Cisco ONS 15454 Procedure Guide*.

During the accumulation cycle, if the current value of a PM parameter reaches or exceeds its corresponding threshold value, a threshold crossing alert (TCA) is generated by the node and displayed by CTC. TCAs provide early detection of performance degradation. When a threshold is crossed, the node continues to count the errors during a given accumulation period. If zero is entered as the threshold value, generation of TCAs is disabled, but performance monitoring continues.

Note Due to limitations of memory and the number of TCAs generated by different platforms, you can manually add/modify the following two properties to the platform property file (CTC.INI for Windows and .ctcrc for UNIX) to fit the need:**ctc.15xxx.node.tr.lowater=yyy** (where xxx is platform and yyy is the number of the lowater mark. The default lowater mark is 25.)
ctc.15xxx.node.tr.hiwater=yyy (where xxx is platform and yyy is the number of the hiwater mark. The default hiwater mark is 50.)
If the number of the incoming TCA is greater than the hiwater mark, it will keep the latest lowater mark and discard older ones.

Change the threshold if the default value does not satisfy your error monitoring needs. For example, customers with a critical DS-1 installed for 911 calls must guarantee the best quality of service on the line; therefore, they lower all thresholds so that the slightest error raises a TCA.

5.2 Intermediate Path Performance Monitoring

Intermediate path performance monitoring (IPPM) allows transparent monitoring of a constituent channel of an incoming transmission signal by a node that does not terminate that channel. Many large networks only use line terminating equipment (LTE), not path terminating equipment (PTE). Table 5-1 shows ONS 15454 cards that are considered LTE.

Table 5-1 ONS 15454 Line Terminating Equipment

ONS 15454 Electrical LTE	
EC1-12 card	
ONS 15454 Optical LTE	
OC3 IR 4/STM1 SH 1310	OC3 IR/STM1 SH 1310-8
OC12 IR/STM4 SH1310	OC12 LR/STM4 LH1310
OC12 LR/STM4 LH 1550	OC12 IR/STM4 SH 1310-4
OC48 IR 1310[1]	OC48 LR 1550
OC48 IR/STM16 SH AS 1310[1]	OC48 LR/STM16 LH AS 1550
OC48 ELR/STM16 EH 100 GHz	OC48 ELR 200 GHz
OC192 SR/STM64 IO 1310	OC192 IR/STM64 SH 1550
OC192 LR/STM64 LH 1550	OC192 LR/STM64 LH ITU 15xx.xx
TXP_MR_10G	MXP_2.5G_10G
MXP_MR_2.5G	MXPP_MR_2.5G

1. An OC-48 IR card used in a bidirectional line switched ring (BLSR) does not support IPPM during a protection switch.

ONS 15454 Software R3.0 and higher allows LTE cards to monitor near-end PM data on individual synchronous transport signal (STS) payloads by enabling IPPM. After enabling IPPM provisioning on the line card, service providers can monitor large amounts of STS traffic through intermediate nodes, thus making troubleshooting and maintenance activities more efficient.

IPPM occurs only on STS paths that have IPPM enabled, and TCAs are raised only for PM parameters on the IPPM enabled paths. The monitored IPPM parameters are STS CV-P, STS ES-P, STS SES-P, STS UAS-P, and STS FC-P.

Note Far-end IPPM is not supported by all OC-N cards. It is supported by OC3-4 and EC-1 cards. However, SONET path PMs can be monitored by logging into the far-end node directly.

The ONS 15454 performs IPPM by examining the overhead in the monitored path and by reading all of the near-end path PM values in the incoming direction of transmission. The IPPM process allows the path signal to pass bidirectionally through the node completely unaltered.

See Table 5-2 on page 5-4 for detailed information and definitions of specific IPPM parameters.

5.3 Pointer Justification Count Performance Monitoring

Pointers are used to compensate for frequency and phase variations. Pointer justification counts indicate timing errors on SONET networks. When a network is out of synchronization, jitter and wander occur on the transported signal. Excessive wander can cause terminating equipment to slip.

Slips cause different effects in service. Voice service has intermittent audible clicks. Compressed voice technology has short transmission errors or dropped calls. Fax machines lose scanned lines or experience dropped calls. Digital video transmission has distorted pictures or frozen frames. Encryption service loses the encryption key, causing data to be transmitted again.

Pointers provide a way to align the phase variations in STS and VT payloads. The STS payload pointer is located in the H1 and H2 bytes of the line overhead. Clocking differences are measured by the offset in bytes from the pointer to the first byte of the STS synchronous payload envelope (SPE) called the J1 byte. Clocking differences that exceed the normal range of 0 to 782 can cause data loss.

There are positive (PPJC) and negative (NPJC) pointer justification count parameters. PPJC is a count of path-detected (PPJC-PDET-P) or path-generated (PPJC-PGEN-P) positive pointer justifications. NPJC is a count of path-detected (NPJC-PDET-P) or path-generated (NPJC-PGEN-P) negative pointer justifications depending on the specific PM name. PJCDIFF is the absolute value of the difference between the total number of detected pointer justification counts and the total number of generated pointer justification counts. PJCS-PDET-P is a count of the one-second intervals containing one or more PPJC-PDET or NPJC-PDET. PJCS-PGEN-P is a count of the one-second intervals containing one or more PPJC-PGEN or NPJC-PGEN.

A consistent pointer justification count indicates clock synchronization problems between nodes. A difference between the counts means that the node transmitting the original pointer justification has timing variations with the node detecting and transmitting this count. Positive pointer adjustments occur when the frame rate of the SPE is too slow in relation to the rate of the STS-1.

You must enable PPJC and NPJC performance monitoring parameters for LTE cards. See Table 5-1 on page 5-2 for a list of Cisco ONS 15454 LTE cards. In CTC, the count fields for PPJC and NPJC PMs appear white and blank unless they are enabled on the card view Provisioning tab.

See Table 5-2 on page 5-4 for detailed information and definitions of specific pointer justification count PM parameters.

5.4 Performance Monitoring Parameter Definitions

Table 5-2 gives definitions for each type of PM parameter found in this chapter.

Table 5-2 Performance Monitoring Parameters

Parameter	Definition
AISS-P	AIS Seconds Path (AISS-P) is a count of one-second intervals containing one or more alarm indication signal (AIS) defects.
BBE-PM	Path Monitoring Background Block Errors (BBE-PM) indicates the number of background block errors recorded in the optical transport network (OTN) path during the PM time interval.
BBE-SM	Section Monitoring Background Block Errors (BBE-SM) indicates the number of background block errors recorded in the OTN section during the PM time interval.
BBER-PM	Path Monitoring Background Block Errors Ratio (BBER-PM) indicates the background block errors ratio recorded in the OTN path during the PM time interval.
BBER-SM	Section Monitoring Background Block Errors Ratio (BBER-SM) indicates the background block errors ratio recorded in the OTN section during the PM time interval.
BIT-EC	Bit Errors Corrected (BIT-EC) indicated the number of bit errors corrected in the DWDM trunk line during the PM time interval.
CSS	Controlled Slip Seconds (CSS) indicates the count of the seconds when at least one or more controlled slips have occurred.
CSS-P	Controlled Slip Seconds Path (CSS-P) indicates the count of the seconds when at least one or more controlled slips have occurred.
CVCP-P	Code Violation CP-bit Path (CVCP-P) is a count of CP-bit parity errors occurring in the accumulation period.
CVCP-PFE	Code Violation CP-bit Path (CVCP-PFE) is a parameter that is counted when the three far-end block error (FEBE) bits in an M-frame are not all collectively set to 1.
CGV	Code Group Violations (CGV) is a count of received code groups that do not contain a start or end delimiter.
CV-L	Line Code Violation (CV-L) indicates the number of coding violations occurring on the line. This parameter is a count of bipolar violations (BPVs) and excessive zeros (EXZs) occurring over the accumulation period.
CV-P	Near-End STS Path Coding Violations (CV-P) is a count of BIP errors detected at the STS path layer (that is, using the B3 byte). Up to eight BIP errors can be detected per frame; each error increments the current CV-P second register.
CV-PFE	Far-End STS Path Coding Violations (CV-PFE) is a count of BIP errors detected at the STS path layer (that is, using the B3 byte). Up to eight BIP errors can be detected per frame; each error increments the current CV-PFE second register.

Table 5-2 Performance Monitoring Parameters (continued)

Parameter	Definition
CVP-P	Code Violation Path (CVP-P) is a code violation parameter for M23 applications. CVP-P is a count of P-bit parity errors occurring in the accumulation period.
CV-S	Section Coding Violation (CV-S) is a count of bit interleaved parity (BIP) errors detected at the section layer (that is, using the B1 byte in the incoming SONET signal). Up to eight section BIP errors can be detected per STS-N frame; each error increments the current CV-S second register.
CV-V	Code Violation VT Layer (CV-V) is a count of the BIP errors detected at the VT path layer. Up to two BIP errors can be detected per VT superframe, with each error incrementing the current CV-V second register.
DCG	Data Code Groups (DCG) is a count of received data code groups that do not contain ordered sets.
ESA-P	Path Errored Seconds-A (ESA-P) is the count of 1-second intervals with exactly one CRC-6 error and no AIS or severely errored framing (SEF) defects.
ESB-P	Path Errored Seconds-B (Rx ESB-P) is a count of 1-second intervals with between 2 and 319 CRC-6 errors and no AIS or SEF.
ESCP-P	Errored Seconds CP-bit Path (ESCP-P) is a count of seconds containing one or more CP-bit parity errors, one or more SEF defects, or one or more AIS defects. ESCP-P is defined for the C-bit parity application.
ESCP-PFE	Far-End Errored Seconds CP-bit Path (ESCP-PFE) is a count of one-second intervals containing one or more M-frames with the three FEBE bits not all collectively set to 1 or one or more far-end SEF/AIS defects.
ES-L	Line Errored Seconds (ES-L) is a count of the seconds containing one or more anomalies (BPV + EXZ) and/or defects (that is, loss of signal) on the line.
ES-NP	
ES-P	Near-End STS Path Errored Seconds (ES-P) is a count of the seconds when at least one STS path BIP error was detected. An AIS Path (AIS-P) defect (or a lower-layer, traffic-related, near-end defect) or a Loss of Pointer Path (LOP-P) defect can also cause an ES-P.
ES-PFE	Far-End STS Path Errored Seconds (ES-PFE) is a count of the seconds when at least one STS path BIP error was detected. An AIS-P defect (or a lower-layer, traffic-related, far-end defect) or an LOP-P defect can also cause an STS ES-PFE.
ES-PM	Path Monitoring Errored Seconds (ES-PM) indicates the errored seconds recorded in the OTN path during the PM time interval.
ESP-P	Errored Seconds Path (ESP-P) is a count of seconds containing one or more P-bit parity errors, one or more SEF defects, or one or more AIS defects.
ESR-PM	Path Monitoring Errored Seconds Ratio (ESR-PM) indicates the errored seconds ratio recorded in the OTN path during the PM time interval.

Table 5-2 Performance Monitoring Parameters (continued)

Parameter	Definition
ESR-SM	Section Monitoring Errored Seconds Ratio (ESR-SM) indicates the errored seconds ratio recorded in the OTN section during the PM time interval.
ES-S	Section Errored Seconds (ES-S) is a count of the number of seconds when at least one section-layer BIP error was detected or an SEF or loss of signal (LOS) defect was present.
ES-SM	Section Monitoring Errored Seconds (ES-SM) indicates the errored seconds recorded in the OTN section during the PM time interval.
ES-V	Errored Seconds VT Layer (ES-V) is a count of the seconds when at least one VT Path BIP error was detected. An AIS Virtual Tributary (VT) (AIS-V) defect (or a lower-layer, traffic-related, near-end defect) or an LOP VT (LOP-V) defect can also cause an ES-V.
FC-L	Line Failure Count (FC-L) is a count of the number of near-end line failure events. A failure event begins when an AIS Line (AIS-L) failure is declared or when a lower-layer, traffic-related, near-end failure is declared. This failure event ends when the failure is cleared. A failure event that begins in one period and ends in another period is counted only in the period where it begins.
FC-P	Near-End STS Path Failure Counts (FC-P) is a count of the number of near-end STS path failure events. A failure event begins when an AIS-P failure, an LOP-P failure, a UNEQ-P failure, or a Section Trace Identifier Mismatch Path (TIM-P) failure is declared. A failure event also begins if the STS PTE that is monitoring the path supports Three-Bit (Enhanced) Remote Failure Indication Path Connectivity (ERFI-P-CONN) for that path. The failure event ends when these failures are cleared.
FC-PFE	Far-End STS Path Failure Counts (FC-PFE) is a count of the number of near-end STS path failure events. A failure event begins when an AIS-P failure, an LOP-P failure, a UNEQ-P failure, or a TIM-P failure is declared. A failure event also begins if the STS PTE that is monitoring the path supports ERFI-P-CONN for that path. The failure event ends when these failures are cleared.
FC-PM	Path Monitoring Failure Counts (FC-PM) indicates the failure counts recorded in the OTN path during the PM time interval.
FC-SM	Section Monitoring Failure Counts (FC-SM) indicates the failure counts recorded in the OTN section during the PM time interval.
IOS	Idle Ordered Sets (IOS) is a count of received packets containing idle ordered sets.
IPC	Invalid Packets (IPC) is the count of received packets that contain errored data code groups that have start and end delimiters.
LBCL-MIN	Laser Bias Current Line—Minimum (LBCL-MIN) is the minimum percentage of laser bias current.
LBCL-AVG	Laser Bias Current Line—Average (LBCL-AVG) is the average percentage of laser bias current.
LBCL-MAX	Laser Bias Current Line—Maximum (LBCL-MAX) is the maximum percentage of laser bias current.

Table 5-2 Performance Monitoring Parameters (continued)

Parameter	Definition
LOFC	Loss of Frame Count (LOFC)
LOSS-L	Line Loss of Signal (LOSS-L) is a count of one-second intervals containing one or more LOS defects.
NIOS	Non-Idle Ordered Sets (NIOS) is a count of received packets containing non-idle ordered sets.
NPJC-PDET-P	Negative Pointer Justification Count, STS Path Detected (NPJC-PDET-P) is a count of the negative pointer justifications detected on a particular path in an incoming SONET signal.
NPJC-PGEN-P	Negative Pointer Justification Count, STS Path Generated (NPJC-PGEN-P) is a count of the negative pointer justifications generated for a particular path to reconcile the frequency of the SPE with the local clock.
OPR	Optical Power Received (OPR) is the measure of average optical power received as a percentage of the nominal OPR.
OPR-AVG	Average Receive Optical Power (dBm)
OPR-MAX	Maximum Receive Optical Power (dBm)
OPR-MIN	Minimum Receive Optical Power (dBm)
OPT	Optical Power Transmitted (OPT) is the measure of average optical power transmitted as a percentage of the nominal OPT.
OPT-AVG	Average Transmit Optical Power (dBm)
OPT-MAX	Maximum Transmit Optical Power (dBm)
OPT-MIN	Minimum Transmit Optical Power (dBm)
OPWR-AVG	Optical Power - Average (OPWR-AVG) is the measure of average optical power on the unidirectional port.
OPWR-MAX	Optical Power - Maximum (OPWR-MAX) is the measure of maximum value of optical power on the unidirectional port.
OPWR-MIN	Optical Power - Minimum (OPWR-MIN) is the measure of minimum value of optical power on the unidirectional port.
PJCDIFF-P	Pointer Justification Count Difference, STS Path (PJCDIFF-P) is the absolute value of the difference between the total number of detected pointer justification counts and the total number of generated pointer justification counts. That is, PJCDiff-P is equal to (PPJC-PGEN-P – NPJC-PGEN-P) – (PPJC-PDET-P – NPJC-PDET-P).
PJNEG	Pointer Justification Negative (PJNEG)
PJPOS	Pointer Justification Positive (PJPOS)
PPJC-PDET-P	Positive Pointer Justification Count, STS Path Detected (PPJC-PDET-P) is a count of the positive pointer justifications detected on a particular path in an incoming SONET signal.
PPJC-PGEN-P	Positive Pointer Justification Count, STS Path Generated (PPJC-PGEN-P) is a count of the positive pointer justifications generated for a particular path to reconcile the frequency of the SPE with the local clock.

Table 5-2 Performance Monitoring Parameters (continued)

Parameter	Definition
PJCS-PDET-P	Pointer Justification Count Seconds, STS Path Detect (NPJCS-PDET-P) is a count of the one-second intervals containing one or more PPJC-PDET or NPJC-PDET.
PJCS-PGEN-P	Pointer Justification Count Seconds, STS Path Generate (PJCS-PGEN-P) is a count of the one-second intervals containing one or more PPJC-PGEN or NPJC-PGEN.
PSC	In a 1 + 1 protection scheme for a working card, Protection Switching Count (PSC) is a count of the number of times service switches from a working card to a protection card plus the number of times service switches back to the working card. For a protection card, PSC is a count of the number of times service switches to a working card from a protection card plus the number of times service switches back to the protection card. The PSC PM parameter is only applicable if revertive line-level protection switching is used.
PSC-R	In a four-fiber bidirectional line switched ring (BLSR), Protection Switching Count-Ring (PSC-R) is a count of the number of times service switches from a working line to a protection line plus the number of times it switches back to a working line. A count is only incremented if ring switching is used.
PSC-S	In a four-fiber BLSR, Protection Switching Count-Span (PSC-S) is a count of the number of times service switches from a working line to a protection line plus the number of times it switches back to the working line. A count is only incremented if span switching is used.
PSC-W	For a working line in a two-fiber BLSR, Protection Switching Count-Working (PSC-W) is a count of the number of times traffic switches away from the working capacity in the failed line and back to the working capacity after the failure is cleared. PSC-W increments on the failed working line and PSC increments on the active protect line. For a working line in a four-fiber BLSR, PSC-W is a count of the number of times service switches from a working line to a protection line plus the number of times it switches back to the working line. PSC-W increments on the failed line and PSC-R or PSC-S increments on the active protect line.
PSD	Protection Switching Duration (PSD) applies to the length of time, in seconds, that service is carried on another line. For a working line, PSD is a count of the number of seconds that service was carried on the protection line. For the protection line, PSD is a count of the seconds that the line was used to carry service. The PSD PM is only applicable if revertive line-level protection switching is used.
PSD-R	In a four-fiber BLSR, Protection Switching Duration-Ring (PSD-R) is a count of the seconds that the protection line was used to carry service. A count is only incremented if ring switching is used.

Table 5-2 Performance Monitoring Parameters (continued)

Parameter	Definition
PSD-S	In a four-fiber BLSR, Protection Switching Duration-Span (PSD-S) is a count of the seconds that the protection line was used to carry service. A count is only incremented if span switching is used.
SASCP-P	SEF/AIS Seconds CP-bit Path (SASCP-P) is a count of one-second intervals containing one or more SEFs or one or more AIS defects on the path.
SASP	SEF/AIS Seconds (SASP) is a count of one-second intervals containing one or more SEFs or one or more AIS defects on the path.
SASP-P	SEF/AIS Seconds Path (SASP-P) is a count of one-second intervals containing one or more SEFs or one or more AIS defects on the path.
SEF-S	Severely Errored Framing Seconds (SEFS-S) is a count of the seconds when an SEF defect was present. An SEF defect is expected to be present during most seconds when an LOS or loss of frame (LOF) defect is present. However, there can be situations when the SEFS-S parameter is only incremented based on the presence of the SEF defect.
SESCP-P	Severely Errored Seconds CP-bit Path (SESCP-P) is a count of seconds containing more than 44 CP-bit parity errors, one or more SEF defects, or one or more AIS defects.
SESCP-PFE	Severely Errored Seconds CP-bit Path (SESCP-PFE) is a count of one-second intervals containing one or more far-end SEF/AIS defects, or one or more 44 M-frames with the three FEBE bits not all collectively set to 1.
SES-L	Line Severely Errored Seconds (SES-L) is a count of the seconds containing more than a particular quantity of anomalies (BPV + EXZ $\geq$ 44) and/or defects on the line.
SES-P	Near-End STS Path Severely Errored Seconds (SES-P) is a count of the seconds when K (2400) or more STS path BIP errors were detected. An AIS-P defect (or a lower-layer, traffic-related, near-end defect) or an LOP-P defect can also cause an SES-P.
SES-PFE	Far-End STS Path Severely Errored Seconds (SES-PFE) is a count of the seconds when K (2400) or more STS path BIP errors were detected. An AIS-P defect (or a lower-layer, traffic-related, far-end defect) or an LOP-P defect can also cause an SES-PFE.
SES-PM	Path Monitoring Severely Errored Seconds (SES-PM) indicates the severely errored seconds recorded in the OTN path during the PM time interval.
SESP-P	Severely Errored Seconds Path (SESP-P) is a count of seconds containing more than 44 P-bit parity violations, one or more SEF defects, or one or more AIS defects.
SES-S	Section Severely Errored Seconds (SES-S) is a count of the seconds when K (see Telcordia GR-253 for value) or more section-layer BIP errors were detected or an SEF or LOS defect was present.
SES-SM	Section Monitoring Severely Errored Seconds (SES-SM) indicates the severely errored seconds recorded in the OTN section during the PM time interval.

Table 5-2 Performance Monitoring Parameters (continued)

Parameter	Definition
SESR-PM	Path Monitoring Severely Errored Seconds Ratio (SESR-PM) indicates the severely errored seconds ratio recorded in the OTN path during the PM time interval.
SESR-SM	Section Monitoring Severely Errored Seconds Ratio (SESR-SM) indicates the severely errored seconds ratio recorded in the OTN section during the PM time interval.
SES-V	Severely Errored Seconds VT Layer (SES-V) is a count of seconds when K (600) or more VT Path BIP errors were detected. An AIS-V defect (or a lower-layer, traffic-related, near-end defect) or an LOP-V defect can also cause SES-V.
UAS-L	Line Unavailable Seconds (UAS-L) is a count of the seconds when the line is unavailable. A line becomes unavailable when ten consecutive seconds occur that qualify as SES-Ls, and it continues to be unavailable until ten consecutive seconds occur that do not qualify as SES-Ls.
UASCP-P	Unavailable Seconds CP-bit Path (UASCP-P) is a count of one-second intervals when the DS-3 path is unavailable. A DS-3 path becomes unavailable when ten consecutive SESCP-Ps occur. The ten SESCP-Ps are included in unavailable time. After the DS-3 path becomes unavailable, it becomes available again when ten consecutive seconds with no SESCP-Ps occur. The ten seconds with no SESCP-Ps are excluded from unavailable time.
UASCP-PFE	Unavailable Seconds CP-bit Path (UASCP-PFE) is a count of one-second intervals when the DS-3 path becomes unavailable. A DS-3 path becomes unavailable when ten consecutive far-end CP-bit SESs occur. The ten CP-bit SESs are included in unavailable time. After the DS-3 path becomes unavailable, it becomes available again when ten consecutive seconds occur with no CP-bit SESs. The ten seconds with no CP-bit SESs are excluded from unavailable time.
UAS-P	Near-End STS Path Unavailable Seconds (UAS-P) is a count of the seconds when the STS path was unavailable. An STS path becomes unavailable when ten consecutive seconds occur that qualify as SES-Ps, and continues to be unavailable until ten consecutive seconds occur that do not qualify as SES-Ps.
UAS-PFE	Far-End STS Path Unavailable Seconds (UAS-PFE) is a count of the seconds when the STS path was unavailable. An STS path becomes unavailable when ten consecutive seconds occur that qualify as SES-PFEs, and continues to be unavailable until ten consecutive seconds occur that do not qualify as SES-PFEs.
UAS-PM	Path Monitoring Unavailable Seconds (UAS-PM) indicates the unavailable seconds recorded in the OTN path during the PM time interval.

Table 5-2 Performance Monitoring Parameters (continued)

Parameter	Definition
UASP-P	Unavailable Seconds Path (UASP-P) is a count of one-second intervals when the DS-3 path is unavailable. A DS-3 path becomes unavailable when ten consecutive SESP-Ps occur. The ten SESP-Ps are included in unavailable time. After the DS-3 path becomes unavailable, it becomes available again when ten consecutive seconds with no SESP-Ps occur. The ten seconds with no SESP-Ps are excluded from unavailable time.
UAS-SM	Section Monitoring Unavailable Seconds (UAS-SM) indicates the unavailable seconds recorded in the OTN section during the PM time interval.
UAS-V	Unavailable Seconds VT Layer (UAS-V) is a count of the seconds when the VT path was unavailable. A VT path becomes unavailable when ten consecutive seconds occur that qualify as SES-Vs, and it continues to be unavailable until ten consecutive seconds occur that do not qualify as SES-Vs.
UNC-WORDS	Uncorrectable Words (UNC-WORDS) is the number of uncorrectable words detected in the DWDM trunk line during the PM time interval.
VPC	Valid Packets (VPC) is a count of received packets that contain non-errored data code groups that have start and end delimiters.

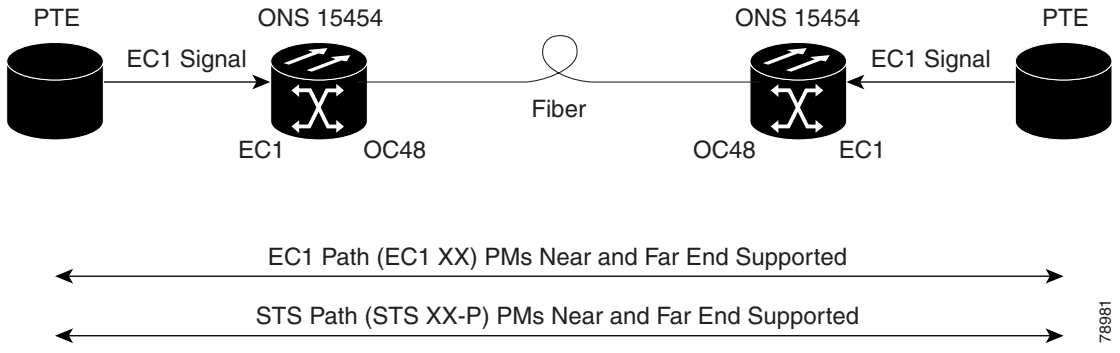
5.5 Performance Monitoring for Electrical Cards

The following sections define PM parameters for the EC1-12, DS1/E1-56, DS1-14, DS1N-14, DS3-12, DS3-12E, DS3N-12, DS3N-12E, DS3i-N-12, DS3XM-6, DS3XM-12, and DS3/EC1-48 cards.

5.5.1 EC1-12 Card Performance Monitoring Parameters

Figure 5-1 shows signal types that support near-end and far-end PMs. Figure 5-2 shows where overhead bytes detected on the application specific integrated circuits (ASICs) produce PM parameters for the EC1-12 card.

Figure 5-1 Monitored Signal Types for the EC1-12 Card



Note The XX in Figure 5-1 represents all PMs listed in Table 5-3 with the given prefix and/or suffix.

Figure 5-2 PM Read Points on the EC1-12 Card

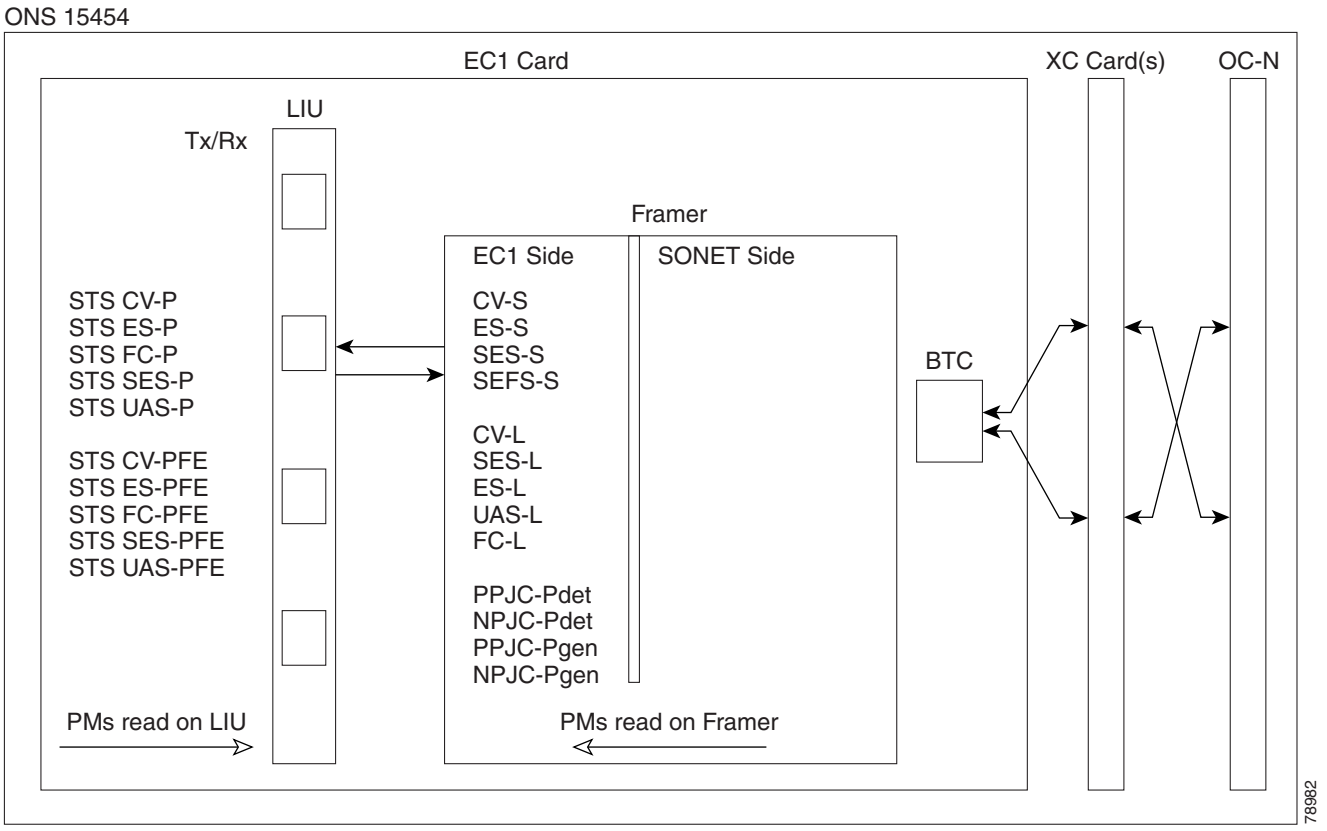


Table 5-3 lists the PM parameters for the EC1-12 cards.

Table 5-3 EC1-12 Card PMs

Section (NE)	Line (NE)	STS Path (NE)	Line (FE)	STS Path (FE)
CV-S	CV-L	CV-P	CV-LFE	CV-PFE
ES-S	ES-L	ES-P	ES-LFE	ES-PFE
SES-S	SES-L	SES-P	SES-LFE	SES-PFE
SEF-S	UAS-L	UAS-P	UAS-LFE	UAS-PFE
	FC-L	FC-P	FC-LFE	FC-PFE
		PPJC-PDET-P		
		NPJC-PDET-P		
		PPJC-PGEN-P		
		NPJC-PGEN-P		
		PJCS-PDET-P		
		PJCS-PGEN-P		
		PJC-DIFF-P		

5.5.2 DS1/E1-56 Card Performance Monitoring Parameters

Figure 5-3 shows signal types that support near-end and far-end PMs. Figure 5-4 shows where overhead bytes detected on the ASICs produce PM parameters for the DS1/E1-56 card.

Figure 5-3 Monitored Signal Types for the DS1/E1-56 Card

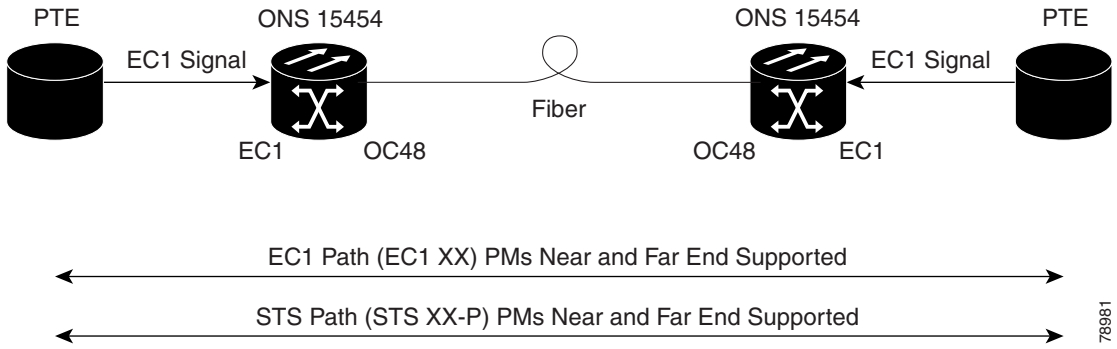


Figure 5-4 PM Read Points on the DS1/E1-56 Card

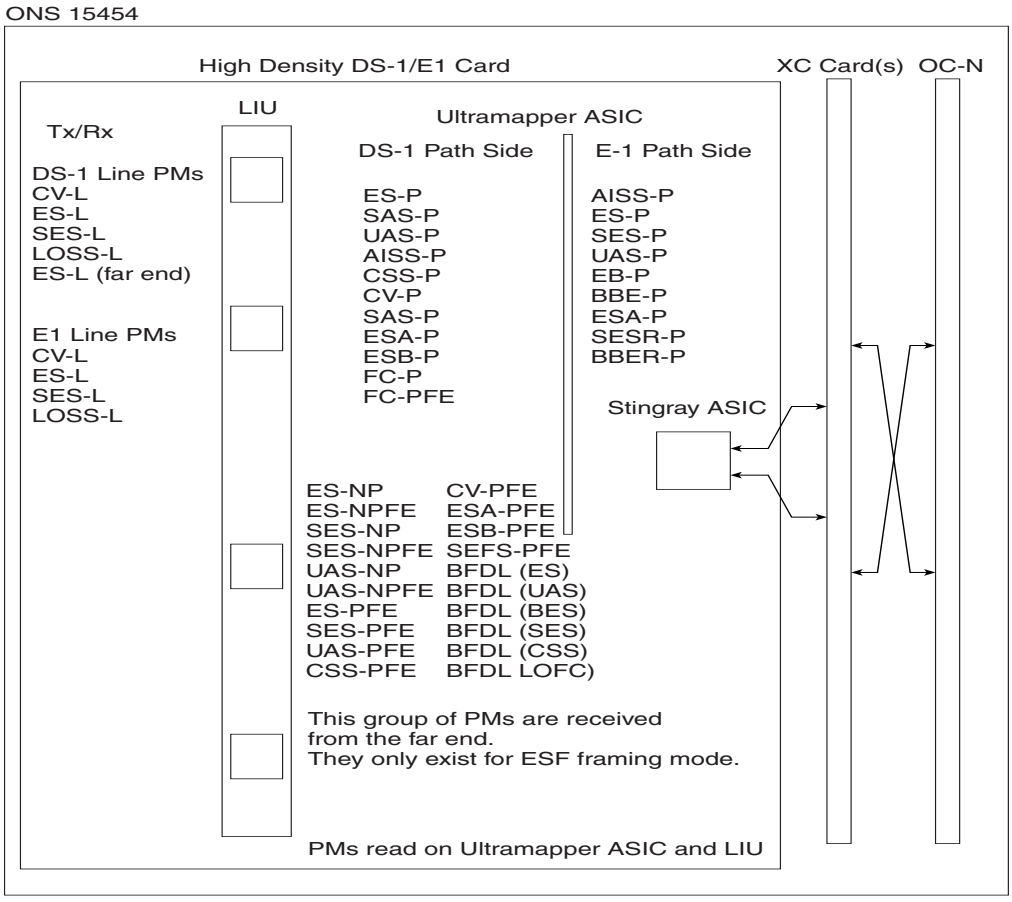


Table 5-4 lists the PM parameters for the DS1/E1-56 card.

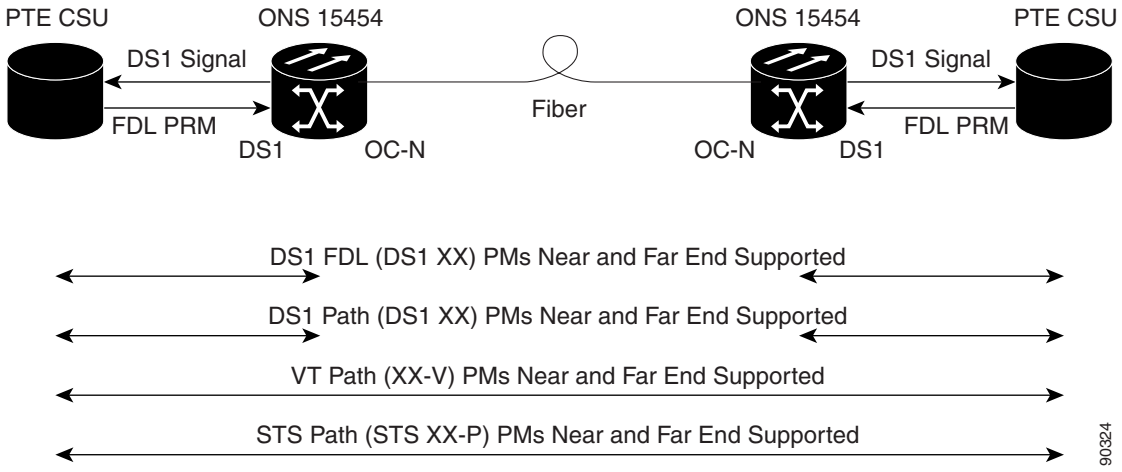
Table 5-4 DS1/E1-56 Card PMs

Line (NE)	Line (FE)	Rx Path (NE)	Tx Path (NE)	STS Path (NE)	Rx Path (FE)	STS Path (FE)	Network Path	BFDL (FE)
CV-L ES-L SES-L LOSS-L	CV-L ES-L	AISS-P CV-P ES-P SES-P SAS-P UAS-P CSS-P ESA-P ESB-P SEFS-P	AISS-P CV-P ES-P SES-P UAS-P BBER-P SESR-P ESR-P	CV-P ES-P SES-P UAS-P FC-P	ES-PFE ESA-PFE ESB-PFE CV-PFE CSS-PFE SEFS-PFE SES-PFE UAS-PFE	CV-PFE ES-PFE SES-PFE UAS-PFE FC-PFE	ES-NP ES-NPFE SES-NP SES-NPFE UAS-NP UAS-NPFE	CSS ES SES BES UAS LOFC

5.5.3 DS1-14 and DS1N-14 Card Performance Monitoring Parameters

Figure 5-5 shows the signal types that support near-end and far-end PMs.

Figure 5-5 Monitored Signal Types for the DS1-14 and DS1N-14 Cards



Note The XX in Figure 5-5 represents all PMs listed in Table 5-5 with the given prefix and/or suffix.

Figure 5-6 shows where overhead bytes detected on the ASICs produce PM parameters for the DS1-14 and DS1N-14 cards.

Figure 5-6 PM Read Points on the DS1-14 and DS1N-14 Cards

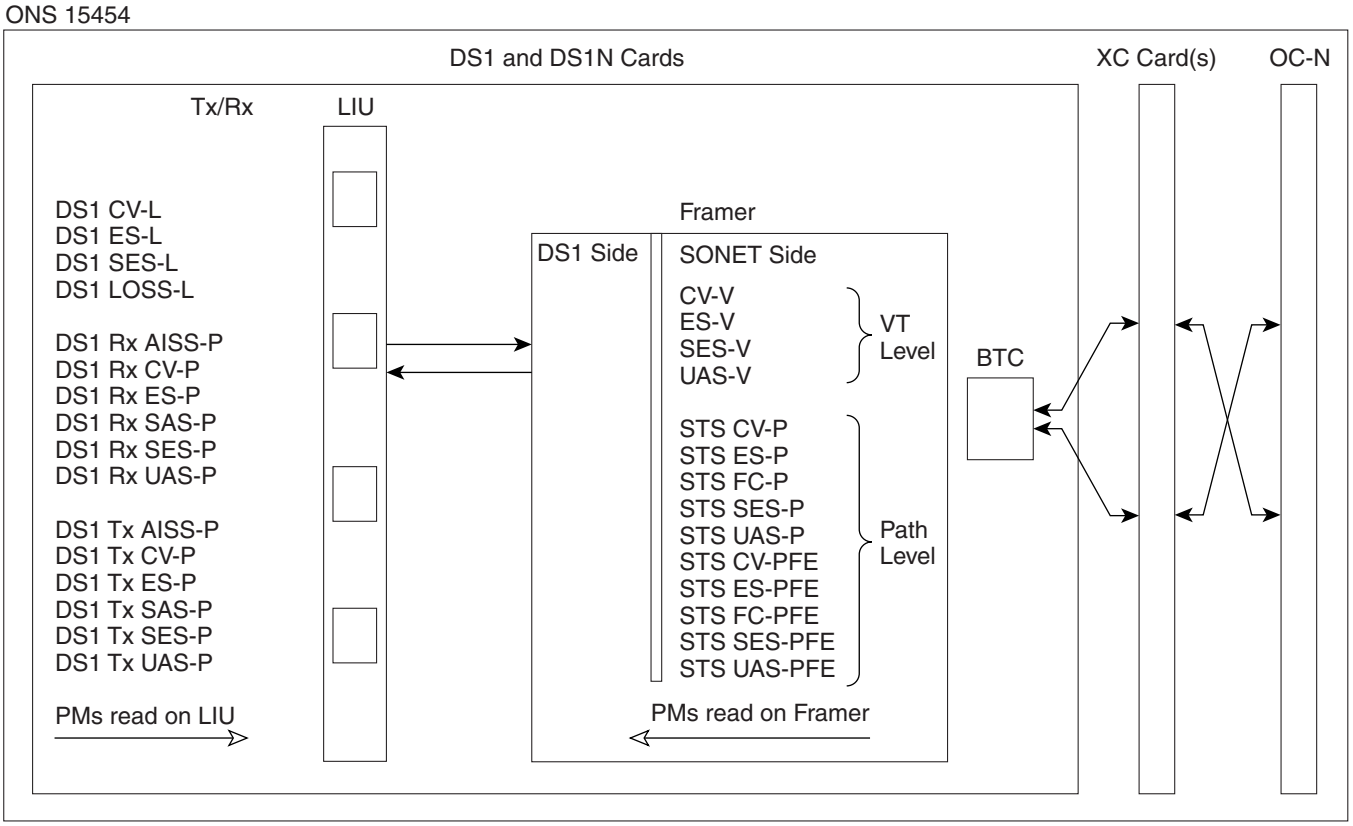


Table 5-5 describes the PM parameters for the DS1-14 and DS1N-14 cards.

Table 5-5 DS1-14 and DS1N-14 Card PMs

Line (NE)	Line (FE)	Rx Path (NE)	Tx Path (NE)	VT Path (NE)	STS Path (NE)	Rx Path (FE)	VT Path (FE)	STS Path (FE)
CV-L ES-L SES-L LOSS-L	CV-L ES-L	AISS-P CV-P ES-P SAS-P SES-P UAS-P CSS-P ESA-P ESB-P SEFS-P	AISS-P CV-P ES-P SAS-P SES-P UAS-P	CV-V ES-V SES-V UAS-V	CV-P ES-P SES-P UAS-P FC-P	ES-PFE ESA-PFE ES-B-PFE CV-PFE CSS-PFE SEFS-PFE SES-PFE UAS-PFE	CV-VFE ES-VFE SES-VFE UAS-VFE	CV-PFE ES-PFE SES-PFE UAS-PFE FC-PFE

Note Far-end DS1 performance monitoring values are valid only when the DS1 line is set to extended super frame (ESF).

5.5.3.1 DS-1 Facility Data Link Performance Monitoring

Facility Data Link (FDL) performance monitoring enables an ONS 15454 DS1N-14 card to calculate and report DS-1 error rate performance measured at both the near-end and far-end of the FDL. The far-end information is reported as received on the FDL in a performance report message (PRM) from an intelligent channel service unit (CSU).

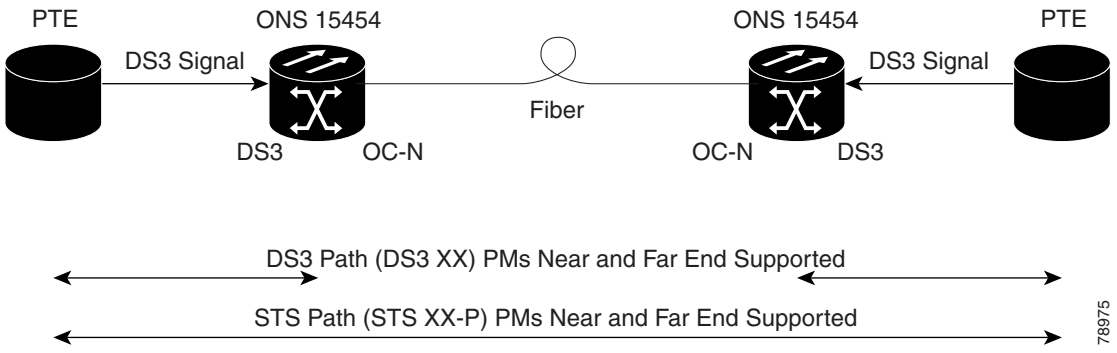
To monitor DS-1 FDL PM values, the DS-1 must be set to use ESF format and the FDL must be connected to an intelligent CSU. For procedures for provisioning ESF on the DS1N-14 card, refer to the *Cisco ONS 15454 Procedure Guide*.

The monitored DS-1 FDL PM parameters are CV-PFE, ES-PFE, ESA-PFE, ESB-PFE, SES-PFE, SEFS-PFE, CSS-PFE, UAS-PFE, FC-PFE, and ES-LFE. See Table 5-2 on page 5-4 for detailed information and definitions of specific FDL DS1 PM parameters.

5.5.4 DS3-12 and DS3N-12 Card Performance Monitoring Parameters

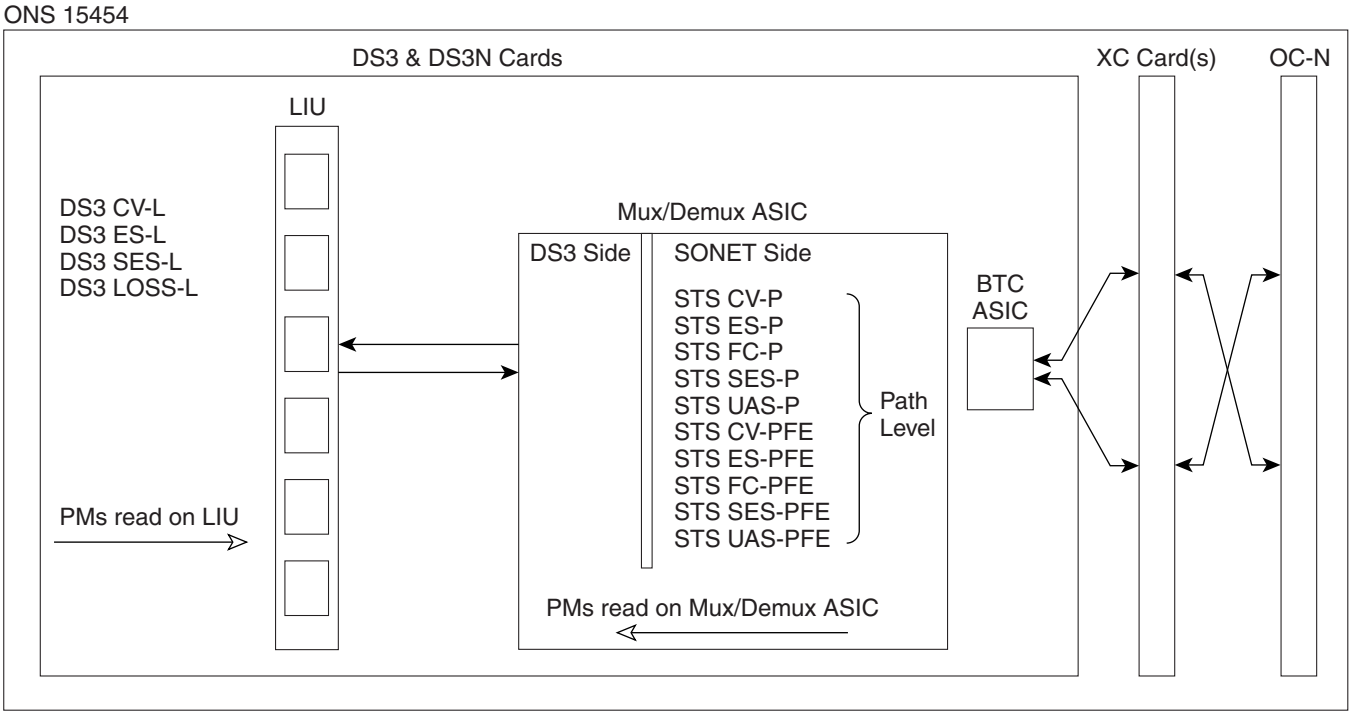
Figure 5-7 shows the signal types that support near-end and far-end PMs. Figure 5-8 shows where overhead bytes detected on the ASICs produce PM parameters for the DS3-12 and DS3N-12 cards.

Figure 5-7 Monitored Signal Types for the DS3-12 and DS3N-12 Cards



Note The XX in Figure 5-7 represents all PMs listed in Table 5-6 with the given prefix and/or suffix.

Figure 5-8 PM Read Points on the DS3-12 and DS3N-12 Cards



The PM parameters for the DS3-12 and DS3N-12 cards are described in Table 5-6.

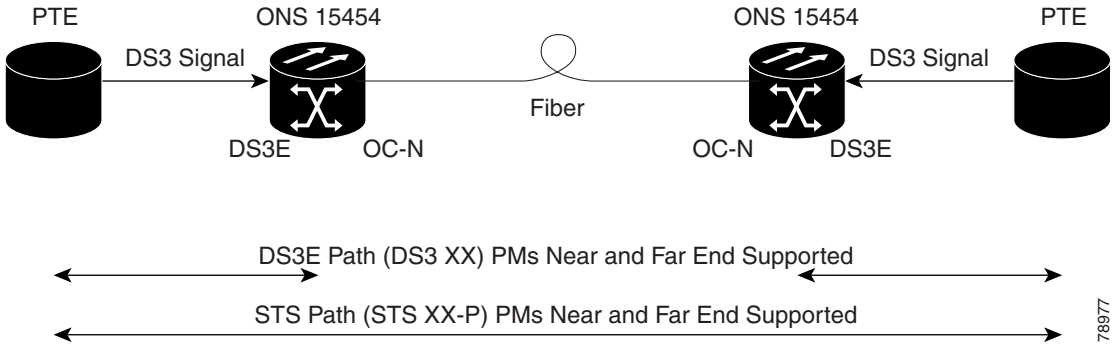
Table 5-6 DS3-12 and DS3N-12 Card PMs

Line (NE)	STS Path (NE)	STS Path (FE)
CV-L	CV-P	CV-PFE
ES-L	ES-P	ES-PFE
SES-L	SES-P	SES-PFE
LOSS-L	UAS-P	UAS-PFE
	FC-P	FC-PFE

5.5.5 DS3-12E and DS3N-12E Card Performance Monitoring Parameters

Figure 5-9 shows the signal types that support near-end and far-end PMs.

Figure 5-9 Monitored Signal Types for the DS3-12E and DS3N-12E Cards



Note The XX in Figure 5-9 represents all PMs listed in Table 5-7 with the given prefix and/or suffix.

Figure 5-10 shows where overhead bytes detected on the ASICs produce PM parameters for the DS3-12E and DS3N-12E cards.

Figure 5-10 PM Read Points on the DS3-12E and DS3N-12E Cards

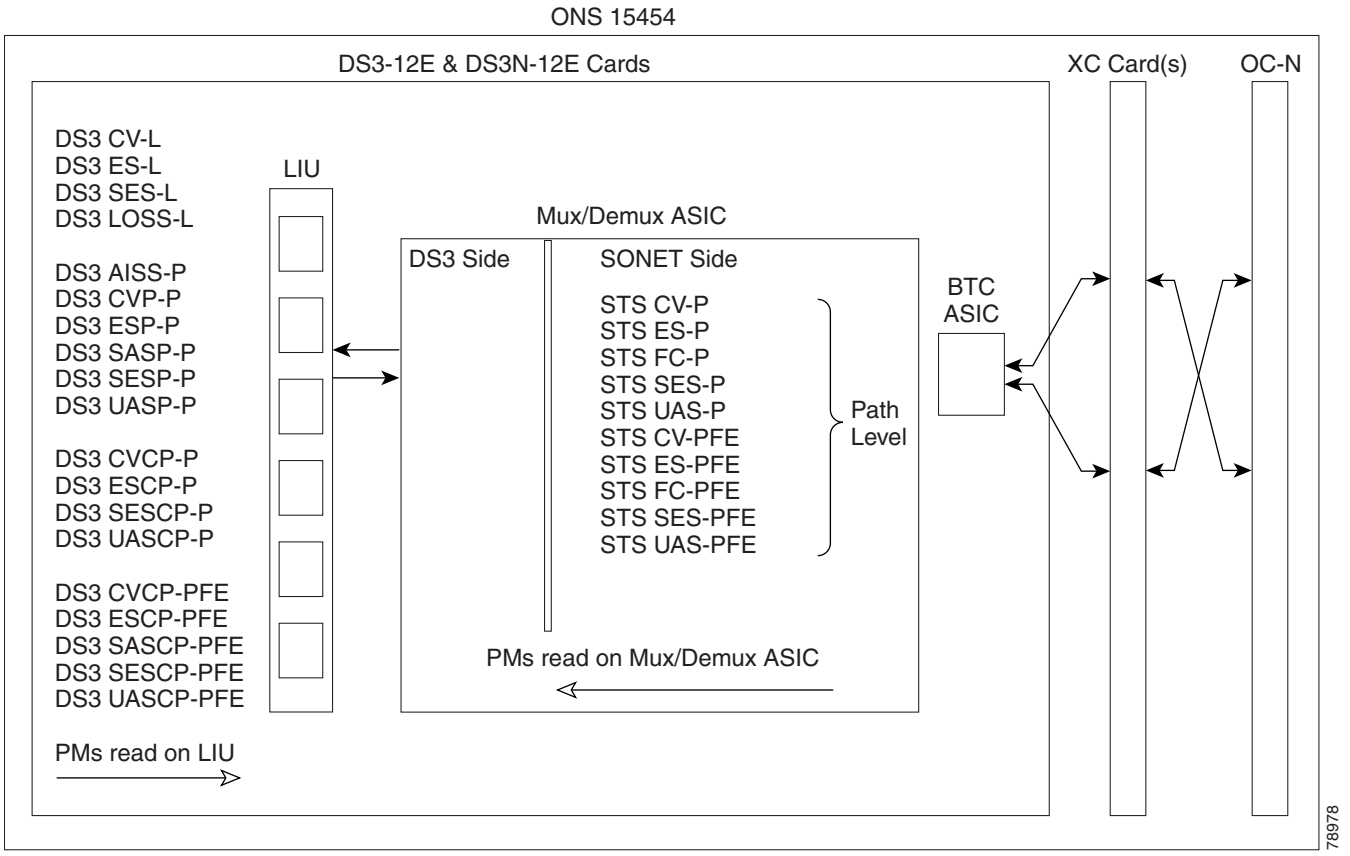


Table 5-7 describes the PM parameters for the DS3-12E and DS3N-12E cards.

Table 5-7 DS3-12E and DS3N-12E Card PMs

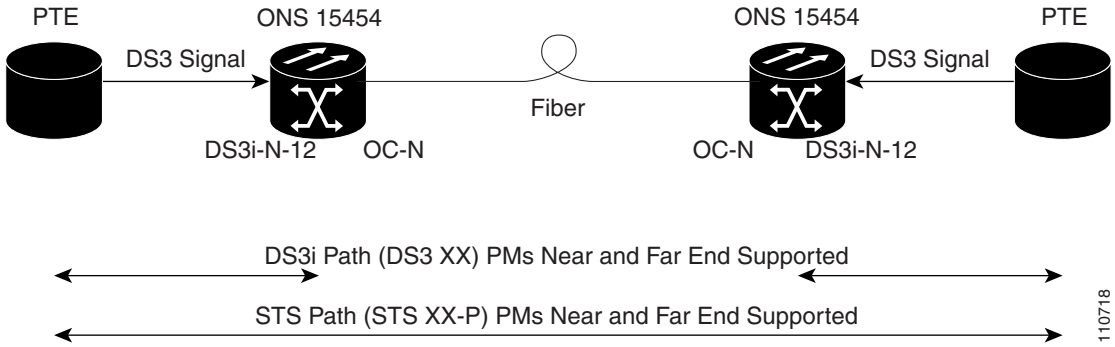
Line (NE)	Path (NE)	STS Path (NE)	Path (FE)[1]	STS Path (FE)
CV-L	AISS-P	CV-P	CVCP-PFE	CV-PFE
ES-L	CV-P	ES-P	ESCP-PFE	ES-PFE
SES-L	ES-P	SES-P	SASCP-P	SES-PFE
LOSS-L	SAS-P[2]	UAS-P	SESCP-PFE	UAS-PFE
	SES-P	FC-P	UASCP-PFE	FC-PFE
	UAS-P			
	CVCP-P			
	ESCP-P			
	SASCP-P			
	SESCP-P			
	UASCP-P			

1. The C-bit PMs (PMs that contain the text "CP-P") are applicable only if the line format is C-bit.
2. DS3(N)-12E cards support SAS-P only on the receive (Rx) path.

5.5.6 DS3i-N-12 Card Performance Monitoring Parameters

Figure 5-11 shows the signal types that support near-end and far-end PMs.

Figure 5-11 Monitored Signal Types for the DS3i-N-12 Cards



Note The XX in Figure 5-11 represents all PMs listed in Table 5-8 with the given prefix and/or suffix.

Figure 5-12 shows where overhead bytes detected on the ASICs produce PM parameters for the DS3i-N-12 cards.

Figure 5-12 PM Read Points on the DS3i-N-12 Cards

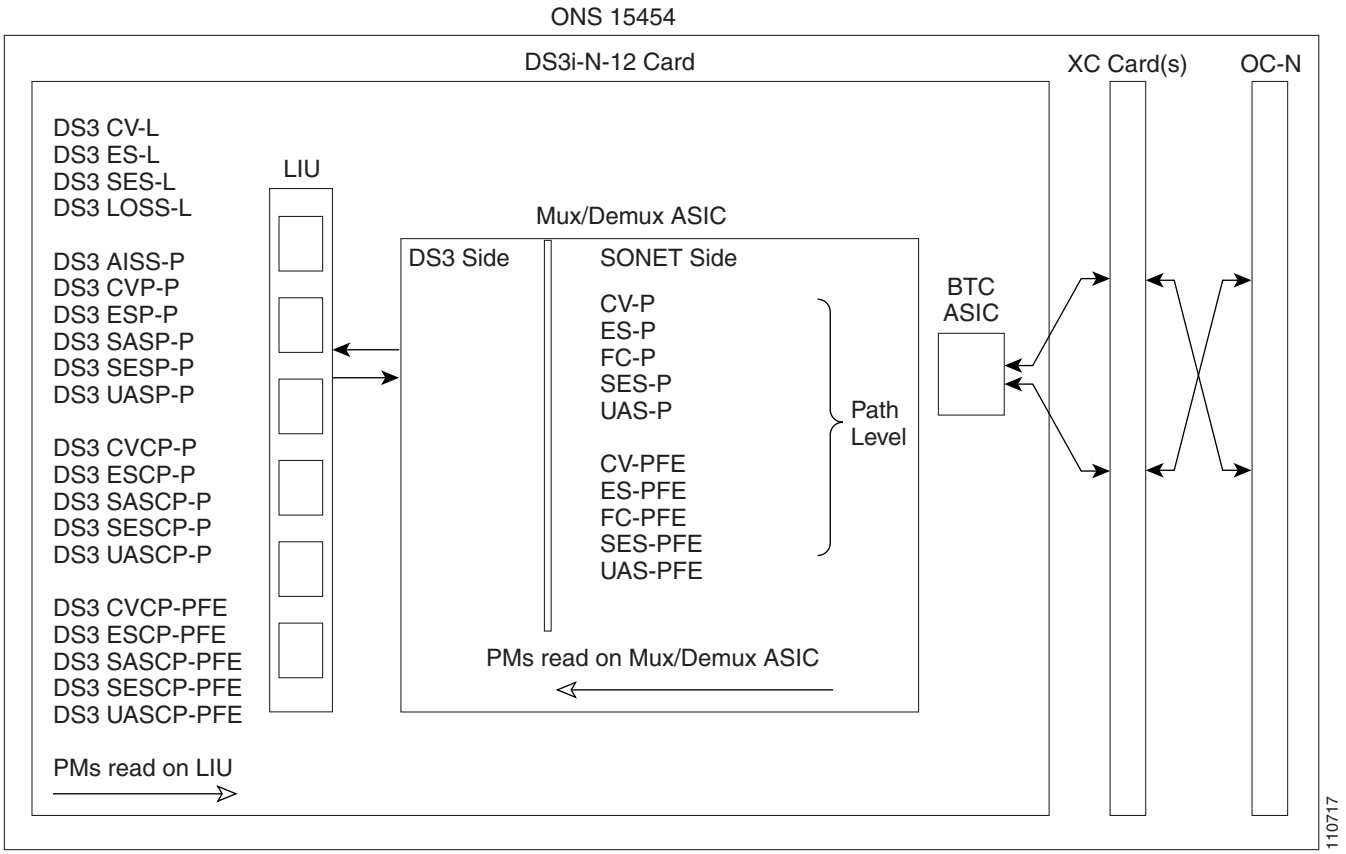


Table 5-8 describes the PM parameters for the DS3i-N-12 card.

Table 5-8 DS3i-N-12 Card PMs

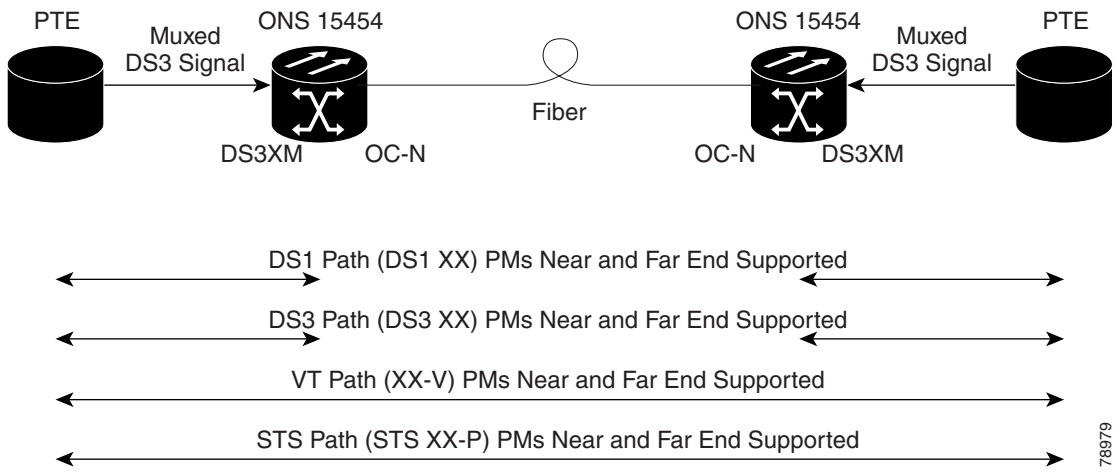
Line (NE)	Path (NE)	STS Path (NE)	Path (FE)[1]	STS Path (FE)
CV-L	AISSP-P	CV-P	CVCP-PFE	CV-PFE
ES-L	CVP-P	ES-P	ESCP-PFE	ES-PFE
SES-L	ESP-P	SES-P	SASCP-PFE	SES-PFE
LOSS-L	SASP-P[2]	UAS-P	SESCP-PFE	UAS-PFE
	SESP-P	FC-P	UASCP-PFE	FC-PFE
	UASP-P			
	CVCP-P			
	ESCP-P			
	SASCP-P			
	SESCP-P			
	UASCP-P			

1. The C-Bit PMs (PMs that contain the text “CP-P”) are applicable only if the line format is C-Bit.
2. DS3i-N-12 cards support SAS-P only on the Rx path.

5.5.7 DS3XM-6 Card Performance Monitoring Parameters

Figure 5-13 shows the signal types that support near-end and far-end PMs.

Figure 5-13 Monitored Signal Types for the DS3XM-6 Card



Note The XX in Figure 5-13 represents all PMs listed in Table 5-9 with the given prefix and/or suffix.

Figure 5-14 shows where the overhead bytes detected on the ASICs produce PM parameters for the DS3XM-6 card.

Figure 5-14 PM Read Points on the DS3XM-6 Card

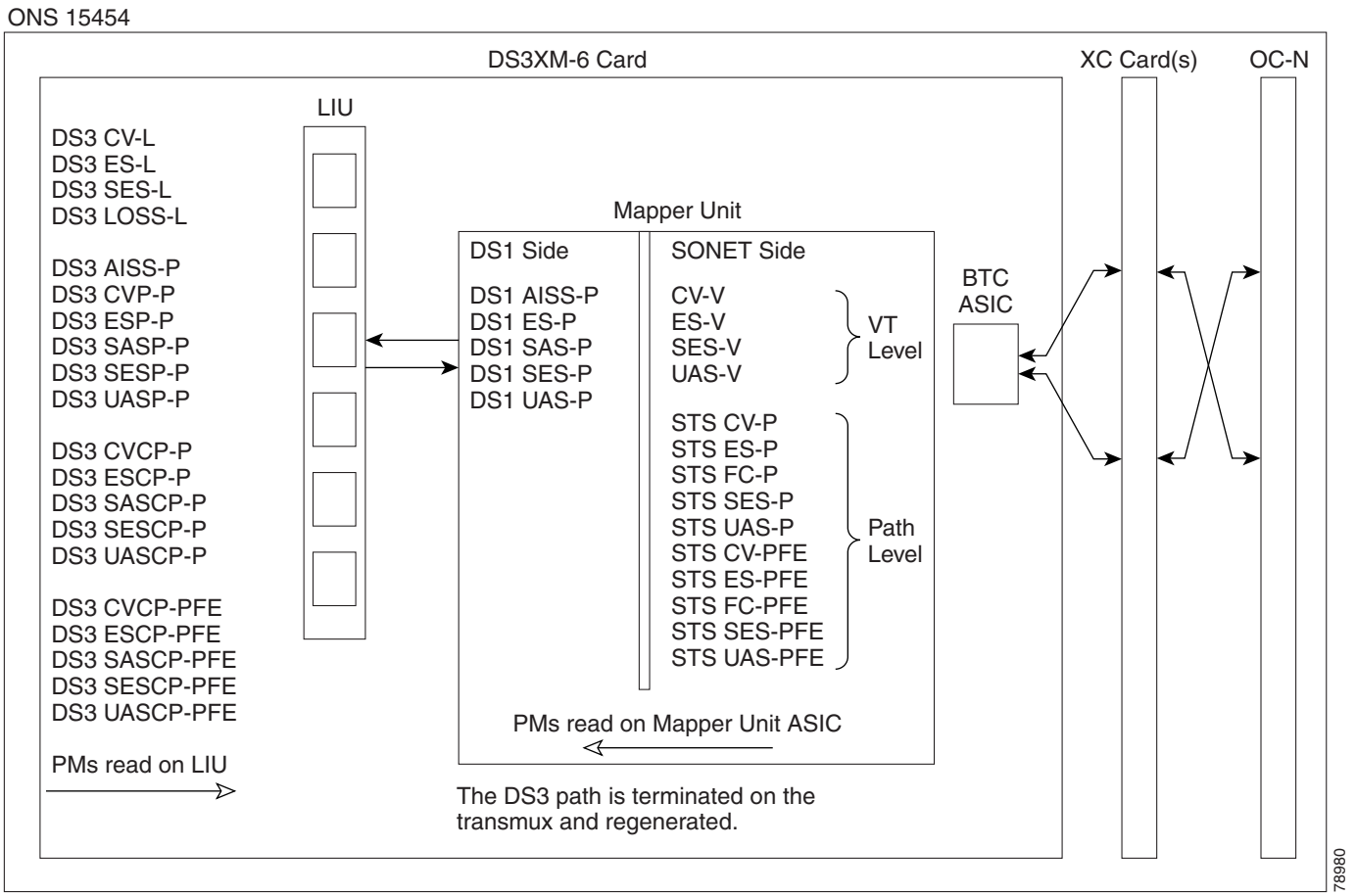


Table 5-9 lists the PM parameters for the DS3XM-6 cards.

Table 5-9 DS3XM-6 Card PMs

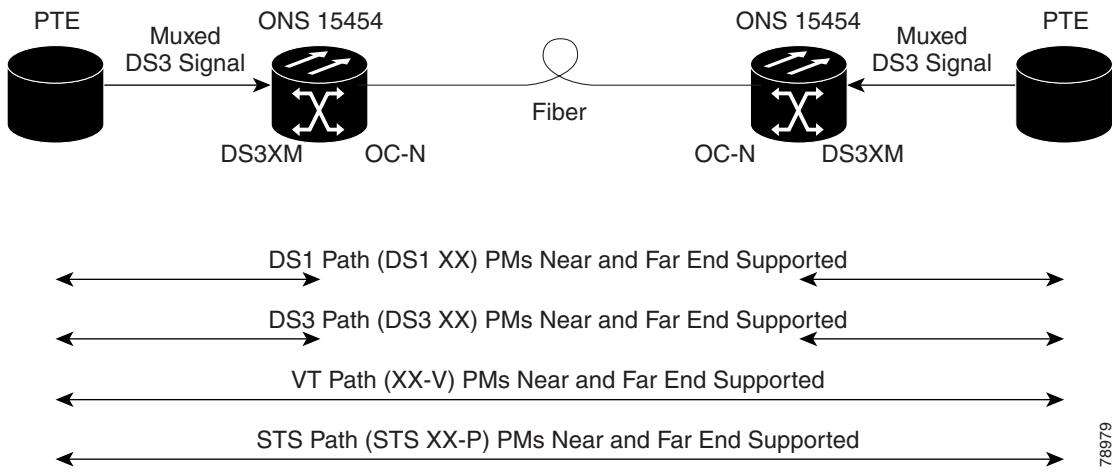
DS3 Line (NE)	DS3 Path (NE)[1]	DS1 Path (NE)	VT Path (NE)	STS Path (NE)	DS3 Path (FE)[1]	VT Path (FE)	STS Path (FE)
CV-L	AISS-P	AISS-P	CV-V	CV-P	CVCP-PFE	CV-VFE	CV-PFE
ES-L	CVP-P	ES-P	ES-V	ES-P	ESCP-PFE	ES-VFE	ES-PFE
SES-L	ESP-P	SAS-P[2]	SES-V	SES-P	SASCP-PFE	SES-VFE	SES-PFE
LOSS-L	SASP-P[2]	SES-P	UAS-V	UAS-P	SESCP-PFE	UAS-VFE	UAS-PFE
	SESP-P	UAS-P		FC-P	UASCP-PFE		FC-PFE
	UASP-P						
	ESCP-P						
	SASCP-P						
	SESCP-P						
	UASCP-P						
	CVCP-P						

1. The C-Bit PMs (PMs that contain the text “CP-P”) are applicable only if the line format is C-Bit.
2. DS3XM-6 cards support SAS-P only on the Rx path.

5.5.8 DS3XM-12 Card Performance Monitoring Parameters

Figure 5-15 shows the signal types that support near-end and far-end PMs.

Figure 5-15 Monitored Signal Types for the DS3XM-12 Card



Note The XX in Figure 5-15 represents all PMs listed in Table 5-10 with the given prefix and/or suffix.

Figure 5-16 shows where the overhead bytes detected on the ASICs produce PM parameters for the DS3XM-12 card.

Figure 5-16 PM Read Points on the DS3XM-12 Card

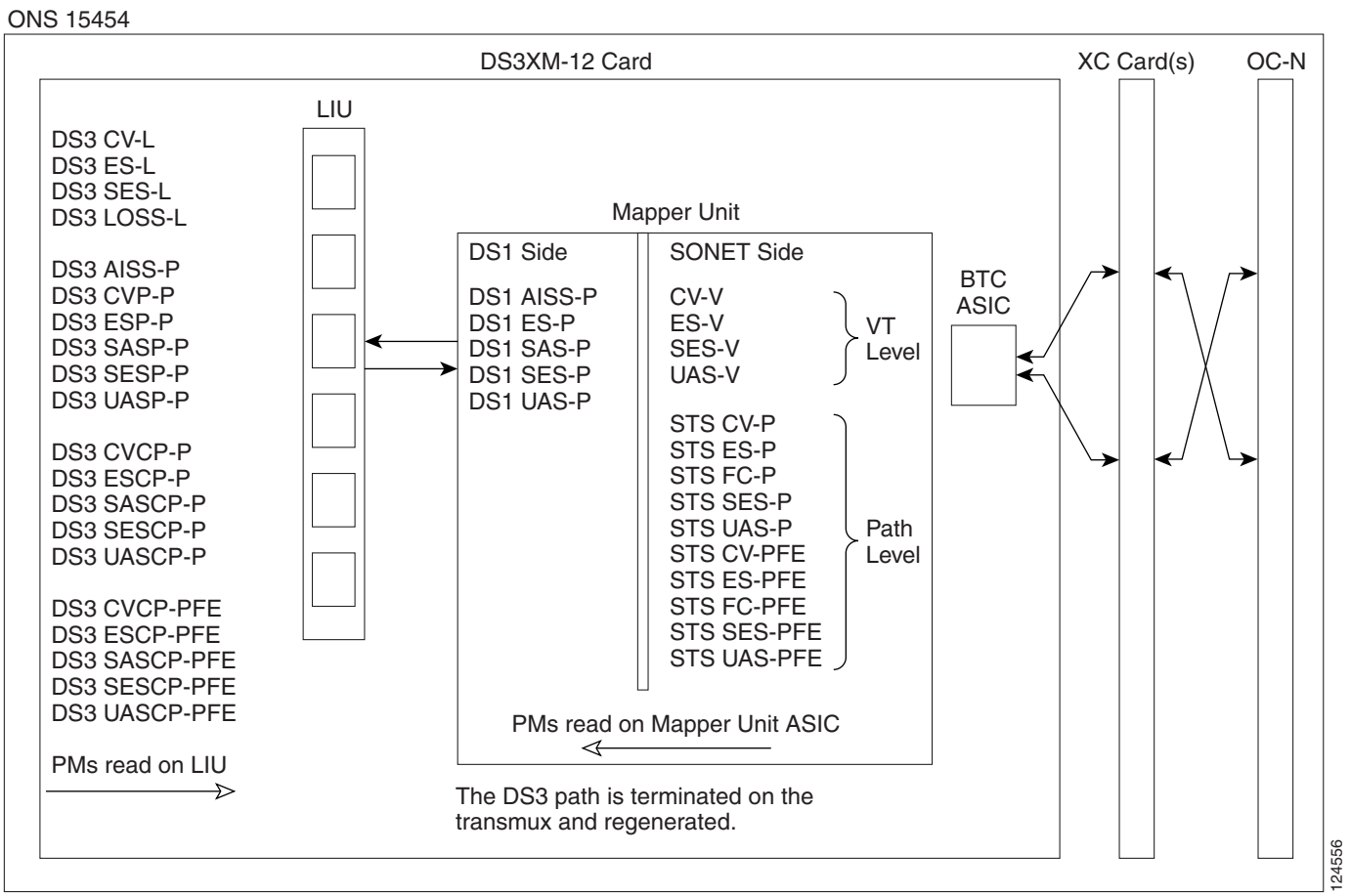


Table 5-10 lists the PM parameters for the DS3XM-12 cards.

Table 5-10 DS3XM-12 Card PMs

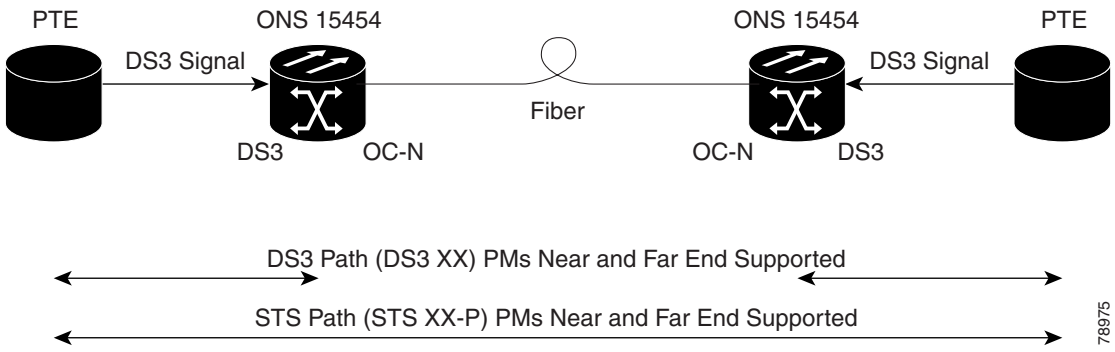
DS3 Line (NE)	DS3 Path (NE)[1]	DS1 Path (NE)	VT Path (NE)	STS Path (NE)	DS3 Path (FE)[1]	VT Path (FE)	STS Path (FE)	BFDL (FE)
CV-L	AISS-P	AISS-P	CV-V	CV-P	CVCP-PFE	CV-VFE	CV-PFE	CSS
ES-L	CV-P	CV-P	ES-V	ES-P	ESCP-PFE	ES-VFE	ES-PFE	ES
SES-L	ES-P	ES-P	SES-V	SES-P	SASCP-PFE	SES-VFE	SES-PFE	SES
LOSS-L	SAS-P[2]	FC-P	UAS-V	UAS-P	SESCP-PFE	UAS-VFE	UAS-PFE	BES
	SES-P	SAS-P[2]		FC-P	UASCP-PFE		FC-PFE	UAS
	UAS-P	SES-P						LOFC
	ESCP-P	UAS-P						
	SESCP-P	CSS-P						
	UASCP-P	ESA-P						
	CVCP-P	ESB-P						
		SEFS-P						

1. The C-Bit PMs (PMs that contain the text “CP-P”) are applicable only if the line format is C-Bit.
2. DS3XM-12 cards support SAS-P only on the Rx path.

5.5.9 DS3/EC1-48 Card Performance Monitoring Parameters

Figure 5-17 shows the signal types that support near-end and far-end PMs.

Figure 5-17 Monitored Signal Types for the DS3/EC1-48 Card



Note The XX in Figure 5-17 represents all PMs listed in Table 5-11 with the given prefix and/or suffix.

Figure 5-18 shows where the overhead bytes detected on the ASICs produce PM parameters for the DS3-EC1-48 card.

Figure 5-18 PM Read Points on the DS3/EC1-48 Card

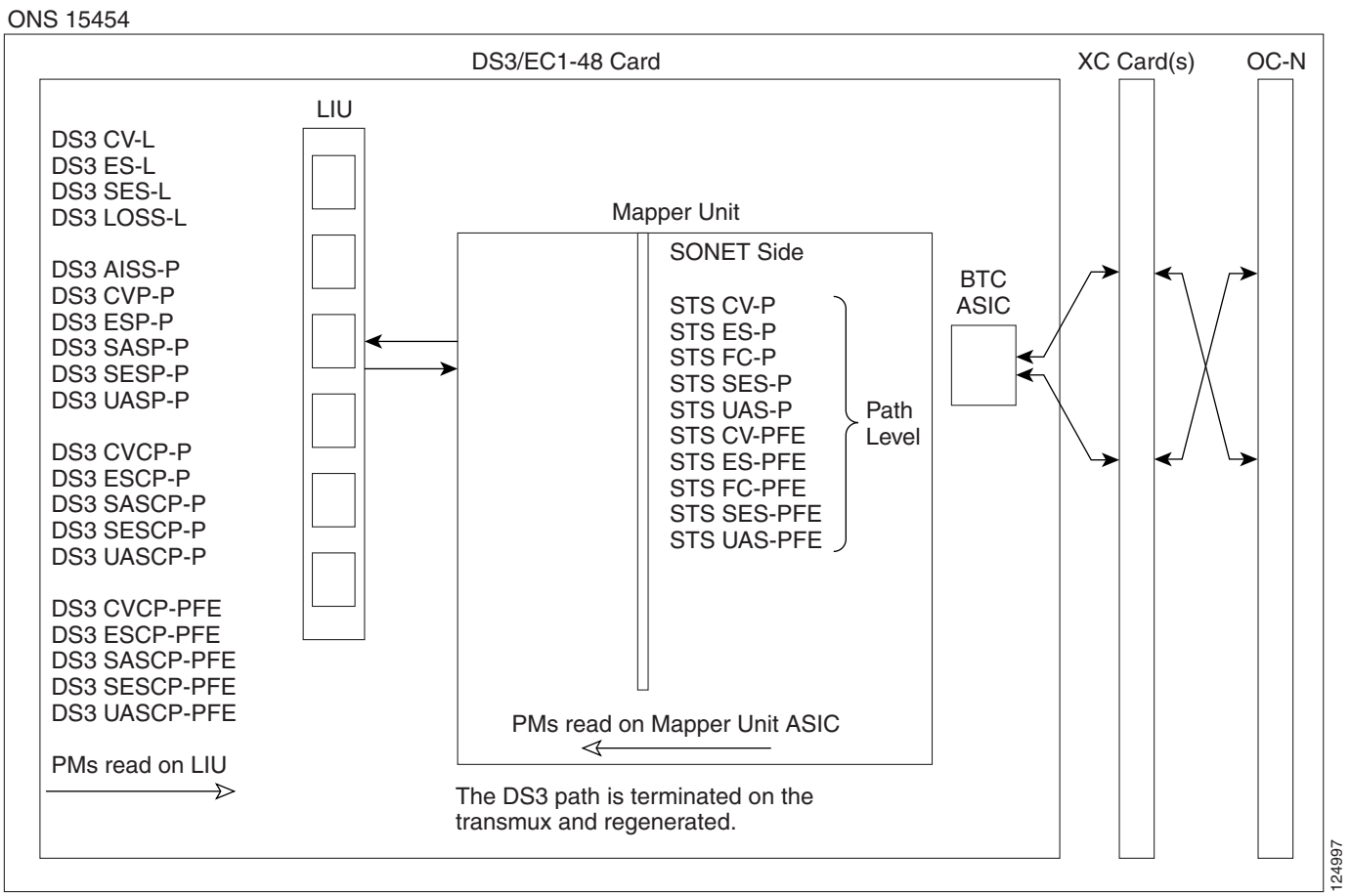


Table 5-11 lists the PM parameters for the DS3/EC1-48 cards.

Table 5-11 DS3/EC1-48 Card PMs

DS3 Line (NE)	DS3 Path (NE)[1]	STS Path (NE)	DS3 Path (FE)[1]	STS Path (FE)
CV-L	AISS-P	CV-P	CVCP-PFE	CV-PFE
ES-L	CVP-P	ES-P	ESCP-PFE	ES-PFE
SES-L	ESP-P	SES-P	SASCP-PFE	SES-PFE
LOSS-L	SASP-P[2]	UAS-P	SESCP-PFE	UAS-PFE
	SESP-P	FC-P	UASCP-PFE	FC-PFE
	UASP-P			
	ESCP-P			
	SASCP-P			
	SESCP-P			
	UASCP-P			
	CVCP-P			

1. The C-Bit PMs (PMs that contain the text “CP-P”) are applicable only if the line format is C-Bit.
2. DS3/EC1-48 cards support SAS-P only on the Rx path.

5.6 Performance Monitoring for Ethernet Cards

The following sections define PM parameters and definitions for the ONS 15454 E-Series, G-Series, ML-Series, and CE100T-8 Ethernet cards.

5.6.1 E-Series Ethernet Card Performance Monitoring Parameters

CTC provides Ethernet performance information, including line-level parameters, port bandwidth consumption, and historical Ethernet statistics. The E-Series Ethernet performance information is divided into the Statistics, Utilization, and History tabbed windows within the card view Performance tab window.

5.6.1.1 E-Series Ethernet Statistics Window

The Ethernet Statistics window lists Ethernet parameters at the line level. The Statistics window provides buttons to change the statistical values shown. The Baseline button resets the displayed statistics values to zero. The Refresh button manually refreshes statistics. Auto-Refresh sets a time interval at which automatic refresh occurs.

Table 5-12 defines the E-Series Ethernet card statistics parameters.

Table 5-12 E-Series Ethernet Statistics Parameters

Parameter	Definition
Link Status	Indicates whether link integrity is present; up means present, and down means not present.
Rx Packets	Number of packets received since the last counter reset.
Rx Bytes	Number of bytes received since the last counter reset.
Tx Packets	Number of packets transmitted since the last counter reset.
Tx Bytes	Number of bytes transmitted since the last counter reset.
Rx Total Errors	Total number of receive errors.
Rx FCS	Number of packets with a frame check sequence (FCS) error. FCS errors indicate frame corruption during transmission.
Rx Alignment	Number of packets with alignment errors; alignment errors are received incomplete frames.
Rx Runts	Measures undersized packets with bad cyclic redundancy check (CRC) errors.
Rx Shorts	Measures undersized packets with good CRC errors.
Rx Oversized + Jabbers	Measures oversized packets and jabbers. Size is greater than 1522 errors regardless of CRC errors.
Tx Collisions	Number of transmit packets that are collisions; the port and the attached device transmitting at the same time causes collisions.
Tx Late Collisions	Number of frames that were not transmitted since they encountered a collision outside of the normal collision window (late collision events should occur only rarely).

Table 5-12 E-Series Ethernet Statistics Parameters (continued)

Parameter	Definition
Tx Excessive Collisions	Number of transmissions that are consecutive collisions.
Tx Deferred	Number of transmitted packets deferred.

5.6.1.2 E-Series Ethernet Utilization Window

The Utilization window shows the percentage of transmit (Tx) and receive (Rx) line bandwidth used by the Ethernet ports during consecutive time segments. The Mode field displays the real-time mode status, such as 100 Full, which is the mode setting configured on the E-Series port. However, if the E-Series port is set to autonegotiate the mode (Auto), this field shows the result of the link negotiation between the E-Series and the peer Ethernet device attached directly to the E-Series port.

The Utilization window provides an Interval drop-down list that enables you to set time intervals of 1 minute, 15 minutes, 1 hour, and 1 day. Line utilization is calculated with the following formulas:

Rx = (inOctets + inPkts * 20) * 8 / 100% interval * maxBaseRate

Tx = (outOctets + outPkts * 20) * 8 / 100% interval * maxBaseRate

The interval is defined in seconds. The maxBaseRate is defined by raw bits per second in one direction for the Ethernet port (that is, 1 Gbps). The maxBaseRate for E-Series Ethernet cards is shown in Table 5-13.

Table 5-13 maxBaseRate for STS Circuits

STS	maxBaseRate
STS-1	51840000
STS-3c	155000000
STS-6c	311000000
STS-12c	622000000

Note Line utilization numbers express the average of ingress and egress traffic as a percentage of capacity.

Note The E-Series Ethernet card is a Layer 2 device or switch and supports Trunk Utilization statistics. The Trunk Utilization statistics are similar to the Line Utilization statistics, but shows the percentage of circuit bandwidth used rather than the percentage of line bandwidth used. The Trunk Utilization statistics are accessed through the card view Maintenance tab.

5.6.1.3 E-Series Ethernet History Window

The Ethernet History window lists past Ethernet statistics for the previous time intervals. Depending on the selected time interval, the History window displays the statistics for each port for the number of previous time intervals as shown in Table 5-14. The parameters are defined in Table 5-12 on page 5-27.

Table 5-14 Ethernet History Statistics per Time Interval

Time Interval	Number of Previous Intervals Displayed
1 minute	60
15 minutes	32
1 hour	24
1 day (24 hours)	7

5.6.2 G-Series Ethernet Card Performance Monitoring Parameters

CTC provides Ethernet performance information, including line-level parameters, port bandwidth consumption, and historical Ethernet statistics. The G-Series Ethernet performance information is divided into the Statistics, Utilization, and History tabbed windows within the card view Performance tab window.

5.6.2.1 G-Series Ethernet Statistics Window

The Ethernet Statistics window lists Ethernet parameters at the line level. The Statistics window provides buttons to change the statistical values shown. The Baseline button resets the displayed statistics values to zero. The Refresh button manually refreshes statistics. Auto-Refresh sets a time interval at which automatic refresh occurs. The G-Series Statistics window also has a Clear button. The Clear button sets the values on the card to zero, but does not reset the G-Series card.

Table 5-15 defines the G-Series Ethernet card statistics parameters.

Table 5-15 G-Series Ethernet Statistics Parameters

Parameter	Definition
Time Last Cleared	A time stamp indicating the last time statistics were reset.
Link Status	Indicates whether the Ethernet link is receiving a valid Ethernet signal (carrier) from the attached Ethernet device; up means present, and down means not present.
Rx Packets	Number of packets received since the last counter reset.
Rx Bytes	Number of bytes received since the last counter reset.
Tx Packets	Number of packets transmitted since the last counter reset.
Tx Bytes	Number of bytes transmitted since the last counter reset.
Rx Total Errors	Total number of receive errors.
Rx FCS	Number of packets with a FCS error. FCS errors indicate frame corruption during transmission.
Rx Alignment	Number of packets with received incomplete frames.
Rx Runts	Measures undersized packets with bad CRC errors.
Rx Shorts	Measures undersized packets with good CRC errors.
Rx Jabbers	The total number of frames received that exceed the 1548-byte maximum and contain CRC errors.
Rx Giants	Number of packets received that are greater than 1530 bytes in length.

Table 5-15 G-Series Ethernet Statistics Parameters (continued)

Parameter	Definition
Rx Pause Frames	Number of received Ethernet IEEE 802.3z pause frames.
Tx Pause Frames	Number of transmitted IEEE 802.3z pause frames.
Rx Pkts Dropped Internal Congestion	Number of received packets dropped due to overflow in G-Series frame buffer.
Tx Pkts Dropped Internal Congestion	Number of transmit queue drops due to drops in the G-Series frame buffer.
HDLC Errors	High-level data link control (HDLC) errors received from SONET/SDH (see Note).
Rx Unicast Packets	Number of unicast packets received since the last counter reset.
Tx Unicast Packets	Number of unicast packets transmitted.
Rx Multicast Packets	Number of multicast packets received since the last counter reset.
Tx Multicast Packets	Number of multicast packets transmitted.
Rx Broadcast Packets	Number of broadcast packets received since the last counter reset.
Tx Broadcast Packets	Number or broadcast packets transmitted.

Note Do not use the HDLC errors counter to count the number of frames dropped because of HDLC errors, because each frame can fragment into several smaller frames during HDLC error conditions and spurious HDLC frames can be generated. If HDLC error counters are incrementing when no SONET path problems should be present, it might indicate a problem with the quality of the SONET path. For example, a SONET protection switch generates a set of HDLC errors. However, the actual values of these counters are less significant than the fact that they are changing.

5.6.2.2 G-Series Ethernet Utilization Window

The Utilization window shows the percentage of Tx and Rx line bandwidth used by the Ethernet ports during consecutive time segments. The Mode field displays the real-time mode status, such as 100 Full, which is the mode setting configured on the G-Series port. However, if the G-Series port is set to autonegotiate the mode (Auto), this field shows the result of the link negotiation between the G-Series and the peer Ethernet device attached directly to the G-Series port.

The Utilization window provides an Interval drop-down list that enables you to set time intervals of 1 minute, 15 minutes, 1 hour, and 1 day. Line utilization is calculated with the following formulas:

Rx = (inOctets + inPkts * 20) * 8 / 100% interval * maxBaseRate

Tx = (outOctets + outPkts * 20) * 8 / 100% interval * maxBaseRate

The interval is defined in seconds. The maxBaseRate is defined by raw bits per second in one direction for the Ethernet port (that is, 1 Gbps). The maxBaseRate for G-Series Ethernet cards is shown in Table 5-13.

Note Line utilization numbers express the average of ingress and egress traffic as a percentage of capacity.

Note Unlike the E-Series, the G-Series card does not have a display of Trunk Utilization statistics, because the G-Series card is not a Layer 2 device or switch.

5.6.2.3 G-Series Ethernet History Window

The Ethernet History window lists past Ethernet statistics for the previous time intervals. Depending on the selected time interval, the History window displays the statistics for each port for the number of previous time intervals as shown in Table 5-14 on page 5-29. The listed parameters are defined in Table 5-15 on page 5-29.

5.6.3 ML-Series Ethernet Card Performance Monitoring Parameters

CTC provides Ethernet performance information for line-level parameters and historical Ethernet statistics. The ML-Series Ethernet performance information is divided into the Ether Ports and Packet-over-SONET (POS) Ports tabbed windows within the card view Performance tab window.

5.6.3.1 ML-Series Ether Ports Window

Table 5-16 defines the ML-Series Ethernet card Ether Ports PM parameters.

Table 5-16 ML-Series Ether Ports PM Parameters

Parameter	Definition
ifInOctets	Number of bytes received since the last counter reset.
rxTotalPackets	Number of packets received.
ifInUcastPkts	Number of unicast packets received since the last counter reset.
ifInMulticast Pkts	Number of multicast packets received since the last counter reset.
ifInBroadcast Pkts	Number of broadcast packets received since the last counter reset.
ifInDiscards	The number of inbound packets that were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
ifOutOctets	Number of bytes transmitted since the last counter reset.
txTotalPkts	Number of transmitted packets.
ifOutUcast Pkts	Number of unicast packets transmitted.
ifOutMulticast Pkts	Number of multicast packets transmitted.
ifOutBroadcast Pkts	Number or broadcast packets transmitted.
dot3StatsAlignmentErrors	A count of frames received on a particular interface that are not an integral number of octets in length and do not pass the FCS check.
dot3StatsFCSErrors	A count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check.

Table 5-16 ML-Series Ether Ports PM Parameters (continued)

Parameter	Definition
etherStatsUndersizePkts	The total number of packets received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.
etherStatsOversizePkts	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed. Note that for tagged interfaces, this number becomes 1522 bytes.
etherStatsJabbers	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error).
etherStatsCollissions	Number of transmit packets that are collisions; the port and the attached device transmitting at the same time caused collisions.
etherStatsDropEvents	Number of received frames dropped at the port level.
rx PauseFrames	Number of received Ethernet 802.3z pause frames.
mediaIndStatsOversize Dropped	Number of received oversized packages that are dropped.
mediaIndStatsTxFrames TooLong	Number of received frames that are too long. The maximum is the programmed max frame size (for virtual SAN [VSAN] support); if the maximum frame size is set to default, then the maximum is a 2112 byte payload plus the 36 byte header, which is a total of 2148 bytes.

5.6.3.2 ML-Series POS Ports Window

In the ML-Series POS Ports window, the parameters displayed depend on the framing mode employed by the ML-Series card. The two framing modes for the POS port on the ML-Series card are HDLC and frame-mapped generic framing procedure (GFP-F). For more information on provisioning a framing mode, refer to *Cisco ONS 15454 Procedure Guide*.

Table 5-17 defines the ML-Series Ethernet card POS Ports HDLC parameters. Table 5-18 defines the ML-Series Ethernet card POS Ports GFP-F parameters.

Table 5-17 ML-Series POS Ports Parameters for HDLC Mode

Parameter	Definition
ifInOctets	Number of bytes received since the last counter reset.
rxTotalPkts	Number of packets received.
ifOutOctets	Number of bytes transmitted since the last counter reset.
tx TotalPkts	Number of transmitted packets.
etherStatsDropEvents	Number of received frames dropped at the port level.
rxPktsDropped Internal Congestion	Number of received packets dropped due to overflow in frame buffer.
mediaIndStatsRxFrames Truncated	Number of received frames with a length of 36 bytes or less.

Table 5-17 ML-Series POS Ports Parameters for HDLC Mode (continued)

Parameter	Definition
mediaIndStatsRxFrames TooLong	Number of received frames that are too long. the maximum is the programmed maximum frame size (for VSAN support); if the maximum frame size is set to default, then the maximum is the 2112 byte payload plus the 36 byte header, which is a total of 2148 bytes.
mediaIndStatsRxFrames BadCRC	Number of received frames with CRC errors.
mediaIndStatsRxShort Pkts	Number of received packets that are too small.
hdlcInOctets	Number of bytes received (from the SONET/SDH path) prior to the bytes undergoing HLDC decapsulation by the policy engine.
hdlcRxAborts	Number of received packets aborted on input.
hdlcOutOctets	Number of bytes transmitted (to the SONET/SDH path) after the bytes undergoing HLDC encapsulation by the policy engine.

Table 5-18 ML-Series POS Ports Parameters for GFP-F Mode

Parameter	Meaning
etherStatsDropEvents	Number of received frames dropped at the port level.
rx PktsDroppedInternal Congestion	Number of received packets dropped due to overflow in the frame buffer.
gfpStatsRxFrame	Number of received GFP frames.
gfpStatsTxFrame	Number of transmitted GFP frames.
gfpStatsRxOctets	Number of GFP bytes received.
gfpStatsTxOctets	Number of GFP bytes transmitted.
gfpStatsRxSBitErrors	Sum of all the single bit errors. In the GFP CORE HDR at the GFP-T receiver, these are correctable.
gfpStatsRxMBitErrors	Sum of all the multiple bit errors. In the GFP CORE HDR at the GFP-T receiver, these are uncorrectable.
gfpStatsRxTypeInvalid	Number of receive packets dropped due to Client Data Frame UPI errors.
gfpStatsRxCRCErrors	Number of packets received with a payload FCS error.
gfpStatsLFDRaised	Count of core HEC CRC multiple bit errors. **Note** This count is only of eHec multiple bit errors when in frame. This can be looked at as a count of when the state machine goes out of frame.
gfpStatsCSFRaised	Number of GFP Client signal fail frames detected at the GFP-T receiver.
mediaIndStatsRxFrames Truncated	Number of received frames that are too long. The maximum is the programmed maximum frame size (for VSAN support); if the maximum frame size is set to default, then the maximum is the 2112 byte payload plus the 36 byte header, which is a total of 2148 bytes.

Table 5-18 ML-Series POS Ports Parameters for GFP-F Mode (continued)

Parameter	Meaning
mediaIndStatsRxFramesTooLong	Number of received frames with CRC error.s
mediaIndStatsRxShortPkts	Number of received packets that are too small.

5.6.4 CE-Series Ethernet Card Performance Monitoring Parameters

CTC provides Ethernet performance information, including line-level parameters, port bandwidth consumption, and historical Ethernet statistics. The CE-Series card Ethernet performance information is divided into Ether Ports and POS Ports tabbed windows within the card view Performance tab window.

5.6.4.1 CE-Series Card Ether Port Statistics Window

The Ethernet Ether Ports Statistics window lists Ethernet parameters at the line level. The Statistics window provides buttons to change the statistical values shown. The Baseline button resets the displayed statistics values to zero. The Refresh button manually refreshes statistics. Auto-Refresh sets a time interval at which automatic refresh occurs. The CE-Series Statistics window also has a Clear button. The Clear button sets the values on the card to zero, but does not reset the CE-Series card.

During each automatic cycle, whether auto-refreshed or manually refreshed (using the Refresh button), statistics are added cumulatively and are not immediately adjusted to equal total received packets until testing ends. To see the final PM count totals, allow a few moments for the PM window statistics to finish testing and update fully. PM counts are also listed in the CE-Series card Performance > History window.

Table 5-19 defines the CE-Series card Ethernet port parameters.

Table 5-19 CE-Series Ether Port PM Parameters

Parameter	Definition
Time Last Cleared	A time stamp indicating the last time statistics were reset.
Link Status	Indicates whether the Ethernet link is receiving a valid Ethernet signal (carrier) from the attached Ethernet device; up means present, and down means not present.
ifInOctets	Number of bytes received since the last counter reset.
rxTotalPkts	Number of received packets.
ifInUcastPkts	Number of unicast packets received since the last counter reset.
ifInMulticastPkts	Number of multicast packets received since the last counter reset.
ifInBroadcastPkts	Number of broadcast packets received since the last counter reset.
ifInDiscards	The number of inbound packets that were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free buffer space.
ifInErrors	The number of inbound packets (or transmission units) that contained errors preventing them from being deliverable to a higher-layer protocol.
ifOutOctets	Number of bytes transmitted since the last counter reset.

Table 5-19 CE-Series Ether Port PM Parameters (continued)

Parameter	Definition
txTotalPkts	Number of transmitted packets.
ifOutUcastPkts	Number of unicast packets transmitted.
ifOutMulticastPkts	Number of multicast packets transmitted.
ifOutBroadcastPkts	Number of broadcast packets transmitted.
dot3StatsAlignment Errors	A count of frames received on a particular interface that are not an integral number of octets in length and do not pass the FCS check.
dot3StatsFCSErrors	A count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check.
dot3StatsSingleCollision Frames	A count of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly on collision.
dot3StatsFrameTooLong	A count of frames received on a particular interface that exceed the maximum permitted frame size.
etherStatsUndersizePkts	The total number of packets received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.
etherStatsFragments	The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets) and had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error). **Note** It is entirely normal for etherStatsFragments to increment. This is because it counts both runts (which are normal occurrences due to collisions) and noise hits.
etherStatsPkts64Octets	The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).
etherStatsPkts65to127 Octets	The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
etherStatsPkts128to255 Octets	The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
etherStatsPkts256to511 Octets	The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
etherStatsPkts512to1023 Octets	The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
etherStatsPkts1024to1518Octets	The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).
etherStatsBroadcastPkts	The total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets.

Table 5-19 CE-Series Ether Port PM Parameters (continued)

Parameter	Definition
etherStatsMulticastPkts	The total number of good packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.
etherStatsOversizePkts	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed. Note that for tagged interfaces, this number becomes 1522 bytes.
etherStatsJabbers	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error).
etherStatsOctets	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets
etherStatsCollisions	Number of transmit packets that are collisions; the port and the attached device transmitting at the same time caused collisions.
etherStatsCRCAlign Errors	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error).
etherStatsDropEvents	Number of received frames dropped at the port level.

5.6.4.2 CE-Series Card Ether Ports Utilization Window

The Ether Ports Utilization window shows the percentage of Tx and Rx line bandwidth used by the Ethernet ports during consecutive time segments. The Utilization window provides an Interval drop-down list that enables you to set time intervals of 1 minute, 15 minutes, 1 hour, and 1 day. Line utilization is calculated with the following formulas:

Rx = (inOctets + inPkts * 20) * 8 / 100% interval * maxBaseRate

Tx = (outOctets + outPkts * 20) * 8 / 100% interval * maxBaseRate

The interval is defined in seconds. The maxBaseRate is defined by raw bits per second in one direction for the Ethernet port (that is, 1 Gbps). The maxBaseRate for CE-Series Ethernet cards is shown in Table 5-13.

Note Line utilization numbers express the average of ingress and egress traffic as a percentage of capacity.

5.6.4.3 CE-Series Card Ether Ports History Window

The Ethernet Ether Ports History window lists past Ethernet statistics for the previous time intervals. Depending on the selected time interval, the History window displays the statistics for each port for the number of previous time intervals as shown in Table 5-14 on page 5-29. The listed parameters are defined in Table 5-15 on page 5-29.

5.6.4.4 CE-Series Card POS Ports Statistics Parameters

The Ethernet POS Ports statistics window lists Ethernet POS parameters at the line level. Table 5-20 defines the CE-Series Ethernet card POS Ports parameters.

Table 5-20 CE-Series Card POS Ports Parameters

Parameter	Definition
Time Last Cleared	A time stamp indicating the last time that statistics were reset.
Link Status	Indicates whether the Ethernet link is receiving a valid Ethernet signal (carrier) from the attached Ethernet device; up means present, and down means not present.
ifInOctets	Number of bytes received since the last counter reset.
rxTotalPkts	Number of received packets.
ifInDiscards	The number of inbound packets that were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free buffer space.
ifInErrors	The number of inbound packets (or transmission units) that contained errors preventing them from being deliverable to a higher-layer protocol.
ifOutOctets	Number of bytes transmitted since the last counter reset.
txTotalPkts	Number of transmitted packets.
ifOutOversizePkts	Packets greater than 1518 bytes transmitted out a port.
gfpStatsRxSBitErrors	Sum of all the single bit errors. In the GFP CORE HDR at the GFP-T receiver, these are correctable.
gfpStatsRxMBitErrors	Sum of all the multiple bit errors. In the GFP CORE HDR at the GFP-T receiver, these are uncorrectable.
gfpStatsRxTypeInvalid	Number of receive packets dropped due to Client Data Frame UPI errors.
gfpStatsRxCRCErrors	Number of packets received with a payload FCS error.
gfpStatsRxCIDInvalid	Number of packets with invalid CID.
gfpStatsCSFRaised	Number of GFP Client signal fail frames detected at the GFP-T receiver.
ifInPayloadCrcErrors	Received payload CRC errors.
ifOutPayloadCrcErrors	Transmitted payload CRC errors.

5.6.4.5 CE-Series Card POS Ports Utilization Window

The POS Ports Utilization window shows the percentage of Tx and Rx line bandwidth used by the POS ports during consecutive time segments. The Utilization window provides an Interval drop-down list that enables you to set time intervals of 1 minute, 15 minutes, 1 hour, and 1 day. Line utilization is calculated with the following formulas:

Rx = (inOctets * 8) / (interval * maxBaseRate)

Tx = (outOctets * 8) / (interval * maxBaseRate)

The interval is defined in seconds. The maxBaseRate is defined by raw bits per second in one direction for the Ethernet port (that is, 1 Gbps). The maxBaseRate for CE-Series cards is shown in Table 5-13 on page 5-28.

Note Line utilization numbers express the average of ingress and egress traffic as a percentage of capacity.

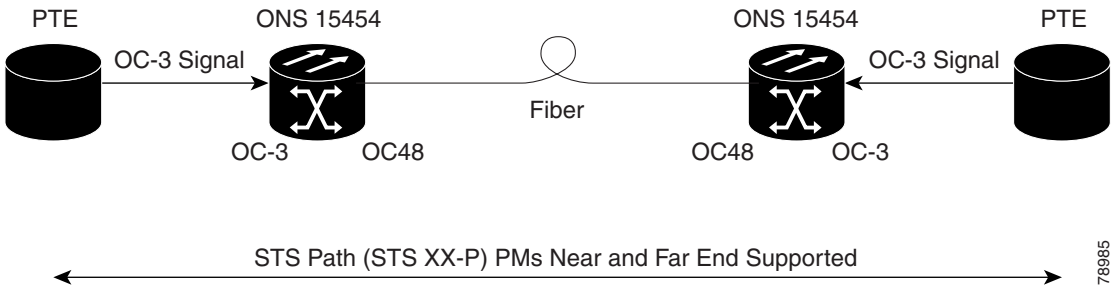
5.6.4.6 CE-Series Card Ether Ports History Window

The Ethernet POS Ports History window lists past Ethernet POS ports statistics for the previous time intervals. Depending on the selected time interval, the History window displays the statistics for each port for the number of previous time intervals as shown in Table 5-14 on page 5-29. The listed parameters are defined in Table 5-19 on page 5-34.

5.7 Performance Monitoring for Optical Cards

This section lists PM parameters for ONS 15454 optical cards, including the OC-3, OC-12, OC-48, and OC-192 cards. Figure 5-19 shows the signal types that support near-end and far-end PMs.

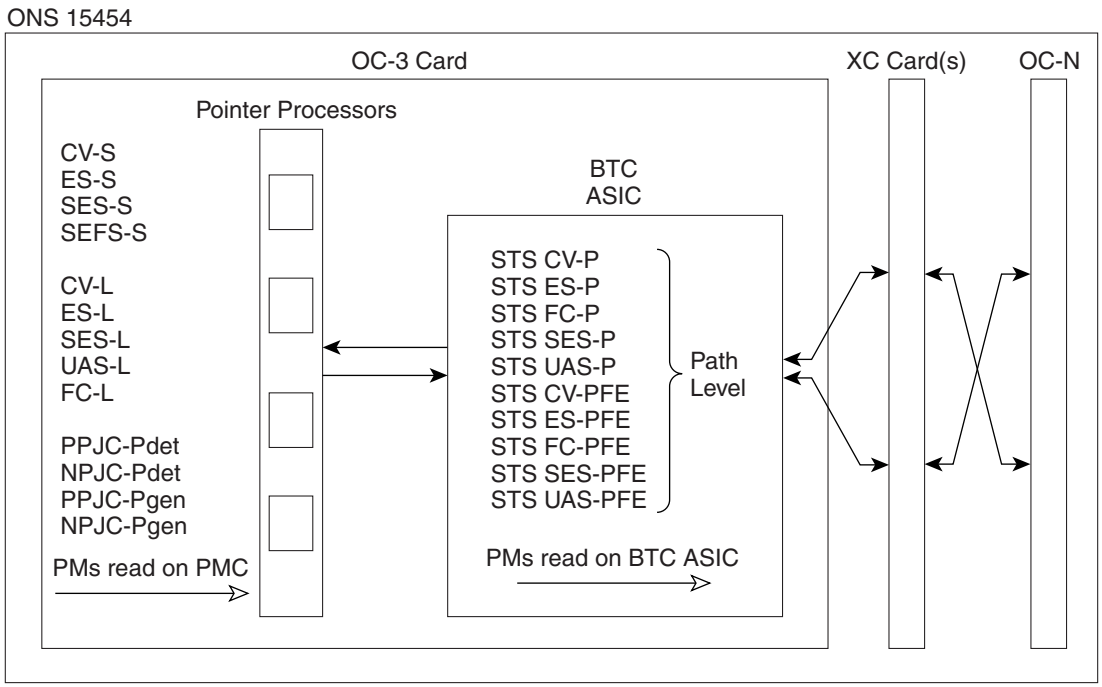
Figure 5-19 Monitored Signal Types for the OC-3 Cards



Note The XX in Figure 5-19 represents all PMs listed in Table 5-21, Table 5-22, and Table 5-23 with the given prefix and/or suffix.

Figure 5-20 shows where overhead bytes detected on the ASICs produce PM parameters for the OC3 IR 4 SH 1310 and OC3 IR SH 1310-8 cards.

Figure 5-20 PM Read Points on the OC-3 Cards



Note For PM locations relating to protection switch counts, see the Telcordia GR-253-CORE document.

Table 5-21 and Table 5-22 list the PM parameters for OC-3 cards.

Table 5-21 OC-3 Card PMs

Section (NE)	Line (NE)	STS Path (NE)	Line (FE)	STS Path (FE)[1]
CV-S	CV-L	CV-P	CV-LFE	CV-PFE
ES-S	ES-L	ES-P	ES-LFE	ES-PFE
SES-S	SES-L	SES-P	SES-LFE	SES-PFE
SEF-S	UAS-L	UAS-P	UAS-LFE	UAS-PFE
	FC-L	FC-P	FC-LFE	FC-PFE
	PSC (1+1)	PPJC-PDET		
	PSD (1+1)	NPJC-PDET		
		PPJC-PGEN		
		NPJC-PGEN		
		PPJC-PDET-P		
		PPJC-PGEN-P		
		PJC-DIFF		

1. The STS Path (FE) PMs are valid only for the OC3-4 card on ONS 15454.

Table 5-22 OC3-8 Card PMs

Section (NE)	Line (NE)	Physical Layer (NE)	STS Path (NE)	Line (FE)	STS Path (FE)
CV-S	CV-L	LBCL	CV-P	CV-LFE	CV-PFE
ES-S	ES-L	OPT	ES-P	ES-LFE	ES-PFE
SES-S	SES-L	OPR	SES-P	SES-LFE	SES-PFE
SEF-S	UAS-L		UAS-P	UAS-LFE	UAS-PFE
	FC-L		FC-P	FC-LFE	FC-PFE
	PSC (1+1)		PPJC-PDET-P		
	PSD (1+1)		NPJC-PDET-P		
			PPJC-PGEN-P		
			NPJC-PGEN-P		
			PJCS-PDET-P		
			PJCS-PGEN-P		
			PJC-DIFF-P		

Table 5-23 lists the PM parameters for OC-12, OC-48, and OC-192 cards.

Table 5-23 OC-12, OC-48, OC-192 Card PMs

Section (NE)	Line (NE)	STS Path (NE)	Line (FE)
CV-S	CV-L	CV-P	CV-L
ES-S	ES-L	ES-P	ES-L
SES-S	SES--L	SES-P	SES-L
SEF-S	UASL	UAS-P	UAS-L
	FC-L	FC-P	FC-L
	PSC (1+1, 2F BLSR)	PPJC-PDET-P	
	PSD (1+1, 2F BLSR)	NPJC-PDET-P	
	PSC-W (4F BLSR)	PPJC-PGEN-P	
	PSD-W (4F BLSR)	NPJC-PGEN-P	
	PSC-S (4F BLSR)	PJCS-PGEN-P	
	PSD-S (4F BLSR)	PJCS-PDET-P	
	PSC-R (4F BLSR)	PJC-DIFF-P	
	PSD-R (4F BLSR)		

5.8 Performance Monitoring for Multirate Cards

This section lists PM parameters for the optical mutirate card, also known as the MRC-12 card.

Figure 5-21 shows where overhead bytes detected on the ASICs produce PM parameters for the MRC-12 card.

Figure 5-21 PM Read Points for the MRC-12 Card

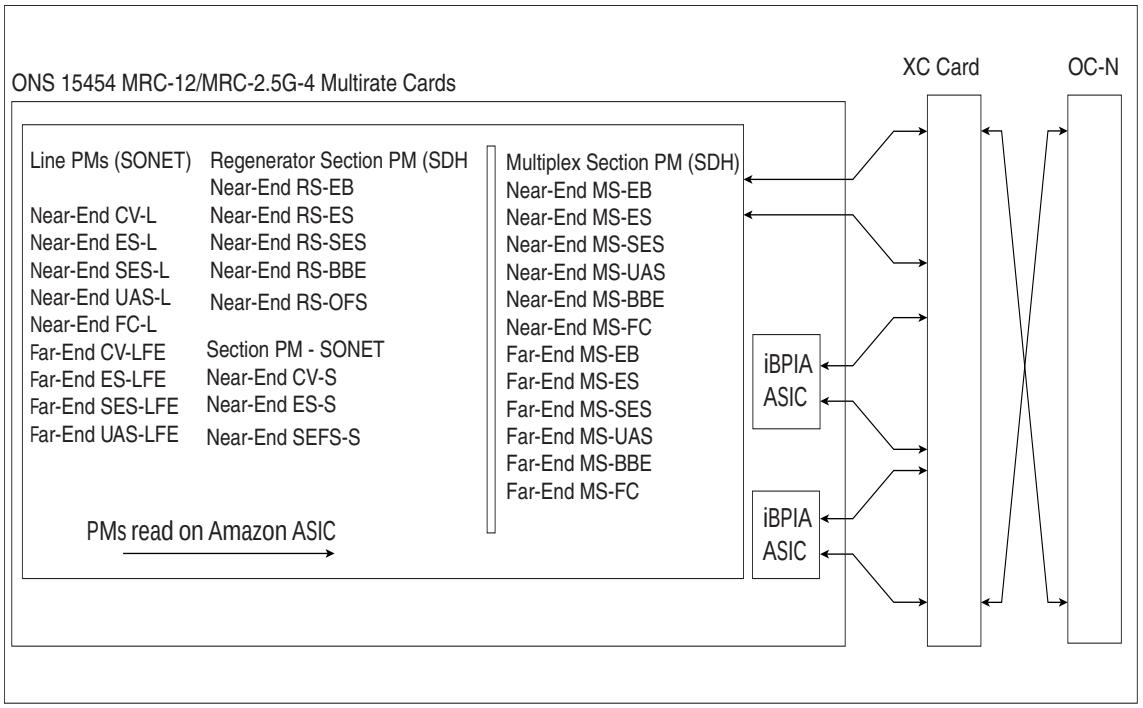


Table 5-24 lists the PM parameters for MRC-12 cards.

Table 5-24 MRC-12 Card PMs

Section (NE)	Line (NE)	Line (FE)
CV-S	CV-L	CV-L
ES-S	ES-L	ES-L
SEF-S	SES-L	SES-L
	UASL	UAS-L
	FC-L	FC-L

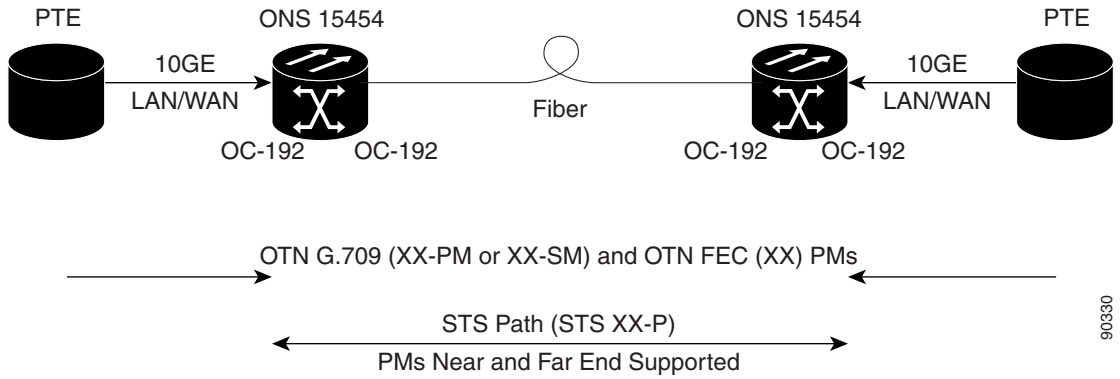
5.9 Performance Monitoring for Transponder and Muxponder Cards

This section lists PM parameters for transponder cards (TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, and TXP_MR_10E), and muxponder cards (MXP_2.5G_10G, MXP_25G_10E, MXP_MR_2.5G, and MXPP_MR_2.5G).

The MXP_MR_2.5G and MXPP_MR_2.5G cards also have payload performance information, divided into Statistics, Utilization, History, and SONET PM tabbed windows within the card view Performance tab Payload PM window. See the "5.9.1 MXP_MR_2.5G/MXPP_MR_2.5G Payload Statistics Window" section on page 5-44, the "5.9.2 MXP_MR_2.5G/MXPP_MR_2.5G Payload Utilization Window" section on page 5-45, and the "5.9.3 MXP_MR_2.5G/MXPP_MR_2.5G Payload History Window" section on page 5-45 for payload PM information for MXP_MR_2.5G and MXPP_MR_2.5G cards.

Figure 5-22 shows the signal types that support near-end and far-end PMs for the TXP_MR_10G card. The signal types for the remaining transponder and muxponder cards are similar to the TXP_MR_10G card.

Figure 5-22 Monitored Signal Types



Note The XX in Figure 5-22 represents all PMs listed in Table 5-25 with the given prefix and/or suffix.

Figure 5-23 shows where overhead bytes detected on the ASICs produce PM parameters for the TXP_MR_10G card. The remaining transponder and muxponder cards perform similarly to this illustration.

Figure 5-23 PM Read Points for TXP_MR_10G Card

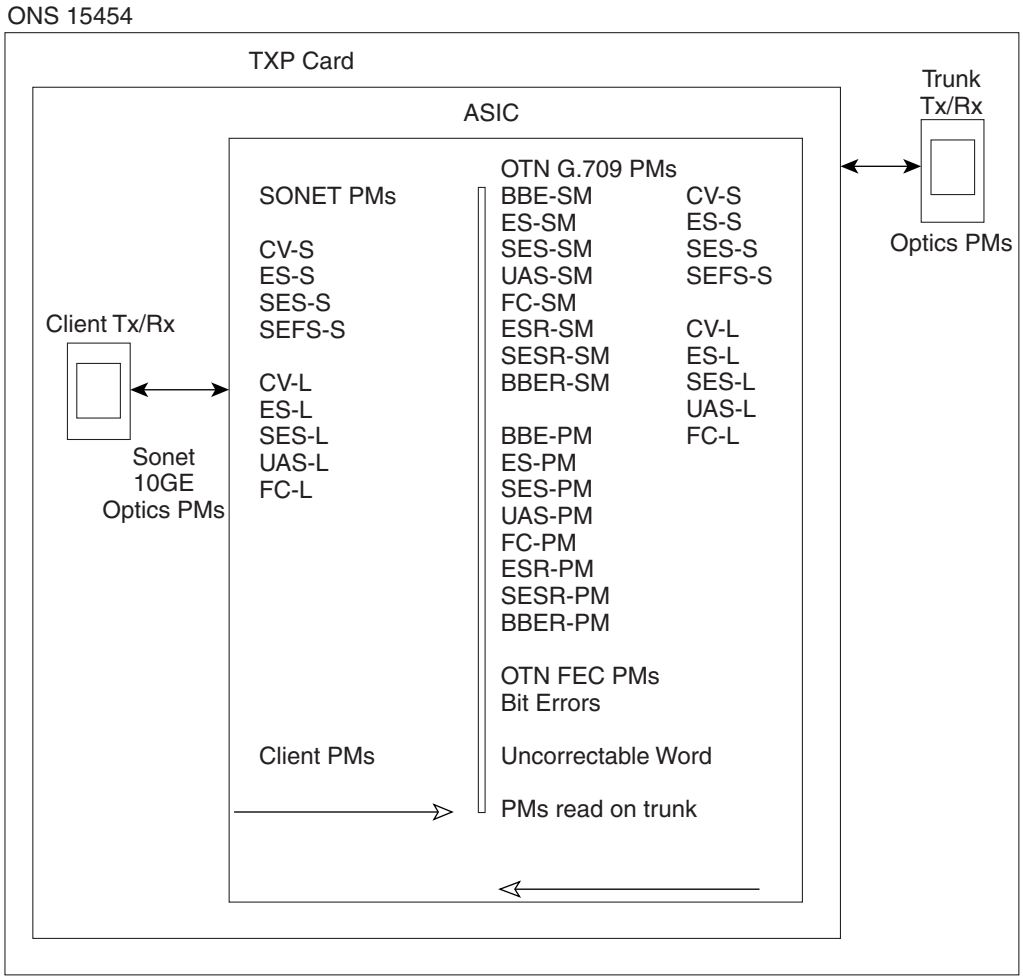


Table 5-25 describes the PM parameters for the TXP_MR_10G, TXP_MR_2.5G, TXPP_MR_2.5G, TXP_MR_10E, MXP_2.5G_10G, MXP_2.5G_10E, MXP_MR_2.5G, and MXPP_MR_2.5G cards.

Table 5-25 Muxponder and Transponder Card PMs

SONET Layer Far-End (FE)[1, 2]	SONET Layer Near-End (NE)[1, 2]	OTN Layer (NE and FE)[3]	Optics (NE)[1, 4]	8B10B (NE)[5]	FEC (NE)[3]
CV-L	CV-S	ES-PM	LBC	CGV	BIT-EC
ES-L	CV-L	ES-SM	OPT	DCG	UNC-WORDS
SES-L	ES-S	ESR-PM	OPR	IOS	
UAS-L	ES-L	ESR-SM		IPC	
FC-L	SES-S	SES-PM		NIOS	
	SES-L	SES-SM		VPC	
	SEF-S	SESR-PM			
	UAS-L	SESR-SM			
	FC-L	UAS-PM			
		UAS-SM			
		BBE-PM			
		BBE-SM			
		BBER-PM			
		BBER-SM			
		FC-PM			
		FC-SM			

1. Applicable to OCH and CLNT facilities.
2. For MXP_MR_2.5G and MXPP_MR_2.5G cards, these parameters are defined in the Performance > Payload PM > SONET PM tabs within the card view.
3. Applicable to OCH facility.
4. TXP_MR_2.5G and TXPP_MR_2.5G card ESCON payload does not support optics PMs on the client port due to Small Form-factor Pluggable (SFP)-imposed restrictions.
5. Applicable to TXP_MR_2.5G and TXPP_MR_2.5G cards only.

5.9.1 MXP_MR_2.5G/MXPP_MR_2.5G Payload Statistics Window

The Payload PM Statistics window lists parameters at the line level. The Statistics window provides buttons to change the statistical values shown. The Baseline button resets the displayed statistics values to zero. The Refresh button manually refreshes statistics. Auto-Refresh sets a time interval at which automatic refresh occurs. The Statistics window also has a Clear button. The Clear button sets the values on the card to zero. All counters on the card are cleared. Table 5-26 defines the MXP_MR_2.5G and MXPP_MR_2.5G card statistics parameters.

Table 5-26 MXP_MR_2.5G/MXPP_MR_2.5G Statistics PMs

Parameter	Definition
8b/10b Errors	A count of 10b errors received by the serial/deserializer (serdes 8b/10b).
Running Disparity Count	A count of errors that affect the disparity of the received data stream.
Invalid CRC Error	A count of invalid CRCs.
Rx Frames	A count of the number of frames received without errors.
Tx Frames	A count of the number of transmitted frames.

Table 5-26 MXP_MR_2.5G/MXPP_MR_2.5G Statistics PMs (continued)

Parameter	Definition
Tx Bytes	A count of the number of bytes transmitted from the frame since the last counter reset.
Rx Link Reset (Only for FC Mode)	A count of the received link resets.

5.9.2 MXP_MR_2.5G/MXPP_MR_2.5G Payload Utilization Window

The Payload PM Utilization window shows the percentage of Tx and Rx line bandwidth used by the ports during consecutive time segments. The Utilization window provides an Interval drop-down list that enables you to set time intervals of 1 minute, 15 minutes, 1 hour, and 1 day. Line utilization is calculated with the following formulas:

Rx = (inOctets + inPkts * 20) * 8 / 100% interval * maxBaseRate

Tx = (outOctets + outPkts * 20) * 8 / 100% interval * maxBaseRate

The interval is defined in seconds. The maxBaseRate is defined by raw bits per second in one direction for the port (that is, 1 Gbps). The maxBaseRate for MXP_MR_2.5G and MXPP_MR_2.5G cards is shown in Table 5-13.

Note Line utilization numbers express the average of ingress and egress traffic as a percentage of capacity.

5.9.3 MXP_MR_2.5G/MXPP_MR_2.5G Payload History Window

The Payload PM History window lists past statistics for the previous time intervals. Depending on the selected time interval, the History window displays the statistics for each port for the number of previous time intervals as shown in Table 5-14 on page 5-29. The listed parameters are defined in Table 5-26 on page 5-44.

5.10 Performance Monitoring for Storage Access Networking Cards

The following sections define PM parameters and definitions for the SAN card, also known as the FC_MR-4 or Fibre Channel card.

CTC provides FC_MR-4 performance information, including line-level parameters, port bandwidth consumption, and historical statistics. The FC_MR-4 card performance information is divided into the Statistics, Utilization, and History tabbed windows within the card view Performance tab window.

5.10.1 FC_MR-4 Statistics Window

The Statistics window lists parameters at the line level. The Statistics window provides buttons to change the statistical values shown. The Baseline button resets the displayed statistics values to zero. The Refresh button manually refreshes statistics. Auto-Refresh sets a time interval at which automatic

refresh occurs. The Statistics window also has a Clear button. The Clear button sets the values on the card to zero. All counters on the card are cleared. Table 5-27 defines the FC_MR-4 card statistics parameters.

Table 5-27 FC_MR-4 Statistics Parameters

Parameter	Definition
Time Last Cleared	A time stamp indicating the last time statistics were reset.
Link Status	Indicates whether the Fibre Channel link is receiving a valid Fibre Channel signal (carrier) from the attached Fibre Channel device; up means present, and down means not present.
Rx Frames	A count of the number of Fibre Channel frames received without errors.
Rx Bytes	A count of the number of bytes received without error for the Fibre Channel payload.
Tx Frames	A count of the number of transmitted Fibre Channel frames.
Tx Bytes	A count of the number of bytes transmitted from the Fibre Channel frame.
8b/10b Errors	A count of 10b errors received by the serial/deserializer (serdes 8b/10b).
Encoding Disparity Errors	A count of the disparity errors received by serdes.
Link Recoveries	A count of the FC_MR-4 software-initiated link recovery attempts toward the FC line side because of SONET protection switches.
Rx Frames bad CRC	A count of the received Fibre Channel frames with errored CRCs.
Tx Frames bad CRC	A count of the transmitted Fibre Channel frames with errored CRCs.
Rx Undersized Frames	A count of the received Fibre Channel frames less than 36 bytes including CRC, start of frame (SOF), and end of frame (EOF).
Rx Oversized Frames	A count of the received Fibre Channel frames greater than 2116 bytes of the payload. Four bytes are allowed for supporting VSAN tags sent.
GFP Rx HDR Single-bit Errors	A count of generic framing procedure (GFP) single bit errors in the core header error check (CHEC).
GFP Rx HDR Multi-bit Errors	A count of GFP multibit errors in CHEC.
GGFP Rx Frames Invalid Type	A count of GFP invalid user payload identifier (UPI) field in the type field.
GFP Rx Superblk CRC Errors	A count of superblock CRC errors in the transparent GFP frame.

5.10.2 FC_MR-4 Utilization Window

The Utilization window shows the percentage of Tx and Rx line bandwidth used by the ports during consecutive time segments. The Utilization window provides an Interval drop-down list that enables you to set time intervals of 1 minute, 15 minutes, 1 hour, and 1 day. Line utilization is calculated with the following formulas:

Rx = (inOctets + inPkts * 24) * 8 / 100% interval * maxBaseRate

Tx = (outOctets + outPkts * 24) * 8 / 100% interval * maxBaseRate

The interval is defined in seconds. The maxBaseRate is defined by raw bits per second in one direction for the port (that is, 1 Gbps or 2 Gbps). The maxBaseRate for FC_MR-4 cards is shown in Table 5-28.

Table 5-28 maxBaseRate for STS Circuits

STS	maxBaseRate
STS-24	850000000
STS-48	850000000 x 2[1]

1. For 1 Gbps of bit rate being transported, there are only 850 Mbps of actual data because of 8b->10b conversion. Similarly, for 2 Gbps of bit rate being transported, there are only 1700 Mbps (850 Mbps x 2) of actual data.

Note Line utilization numbers express the average of ingress and egress traffic as a percentage of capacity.

5.10.3 FC_MR-4 History Window

The History window lists past FC_MR-4 statistics for the previous time intervals. Depending on the selected time interval, the History window displays the statistics for each port for the number of previous time intervals as shown in Table 5-29. The listed parameters are defined in Table 5-27 on page 5-46.

Table 5-29 FC_MR-4 History Statistics per Time Interval

Time Interval	Number of Intervals Displayed
1 minute	60 previous time intervals
15 minutes	32 previous time intervals
1 hour	24 previous time intervals
1 day (24 hours)	7 previous time intervals

5.11 Performance Monitoring for DWDM Cards

The following sections define PM parameters and definitions for the ONS 15454 OPT-PRE, OPT-BST, 32MUX-O, 32DMX-O, 32DMX, 4MD-xx.x, AD-1C-xx.x, AD-2C-xx.x, AD-4C-xx.x, AD-1B-xx.x, AD-4B-xx.x, OSCM, OSC-CSM, and 32WSS DWDM cards.

5.11.1 Optical Amplifier Card Performance Monitoring Parameters

The PM parameters for the OPT-PRE and OPT-BST cards are listed Table 5-30.

Table 5-30 Optical PM Parameters for OPT-PRE and OPT-BST Cards.

Optical Line	Optical Amplifier Line
OPT	OPR

5.11.2 Multiplexer and Demultiplexer Card Performance Monitoring Parameters

The PM parameters for the 32MUX-O, 32WSS, 32DMX, and 32DMX-O cards are listed in Table 5-31.

Table 5-31 Optical PMs for 32MUX-O and 32DMX-O Cards

Optical Channel	Optical Line
OPR	OPT

5.11.3 4MD-xx.x Card Performance Monitoring Parameters

The PM parameters for the 4MD-xx.x cards are listed in Table 5-32.

Table 5-32 Optical PMs for 4MD-xx.x Cards

Optical Channel	Optical Band
OPR	OPT

5.11.4 OADM Channel Filter Card Performance Monitoring Parameters

The PM parameters for the AD-1C-xx.x, AD-2C-xx.x, and AD-4C-xx.x cards are listed in Table 5-33.

Table 5-33 Optical PMs for AD-1C-xx.x, AD-2C-xx.x, and AD-4C-xx.x Cards

Optical Channel	Optical Line
OPR	OPT

5.11.5 OADM Band Filter Card Performance Monitoring Parameters

The PM parameters for the AD-1B-xx.x and AD-4B-xx.x cards are listed in Table 5-34.

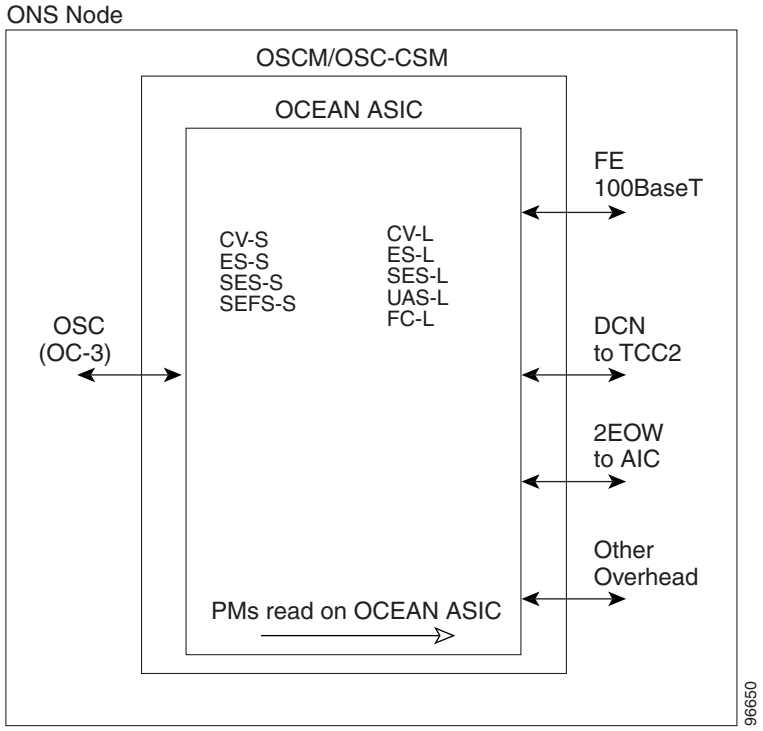
Table 5-34 Optical PMs for AD-1B-xx.x and AD-4B-xx.x Cards

Optical Line	Optical Band
OPR	OPT

5.11.6 Optical Service Channel Card Performance Monitoring Parameters

Figure 5-24 shows where overhead bytes detected on the ASICs produce PM parameters for the OSCM and OSC-CSM cards.

Figure 5-24 PM Read Points on OSCM and OSC-CSM Cards



The PM parameters for the OSCM and OSC-CSM cards are described in Table 5-35.

Table 5-35 OSCM/OSC-CSM (OC3) Card PMs

Section (NE)[1]	Line (NE/FE)[1]	Optics (NE)[2]
CV-S ES-S SES-S SEF-S	CV-L ES-L SES-L UAS-L FC-L	OPWR

1. Applicable to OC3
2. Applicable to OTS facilities

SNMP

This chapter explains Simple Network Management Protocol (SNMP) as implemented by the Cisco ONS 15454.

For SNMP setup information, refer to the *Cisco ONS 15454 Procedure Guide*.

Chapter topics include:

6.1 SNMP Overview

SNMP is an application-layer communication protocol that allows ONS 15454 network devices to exchange management information among these systems and with other devices outside the network. Through SNMP, network administrators can manage network performance, find and solve network problems, and plan network growth.

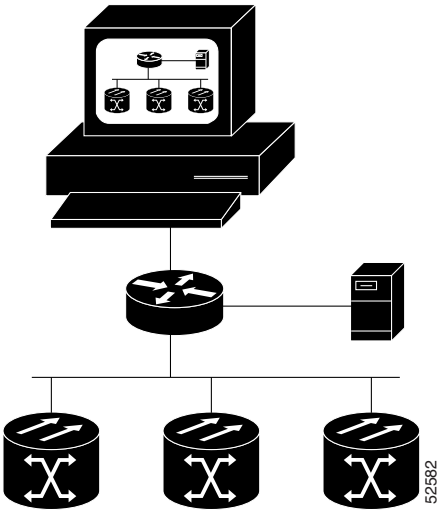
The ONS 15454 uses SNMP for asynchronous event notification to a network management system (NMS). ONS SNMP implementation uses standard Internet Engineering Task Force (IETF) management information bases (MIBs) to convey node-level inventory, fault, and performance management information for generic read-only management of DS-1, DS-3, SONET, and Ethernet technologies. SNMP allows a generic SNMP manager such as HP OpenView Network Node Manager (NNM) or Open Systems Interconnection (OSI) NetExpert to be utilized for limited management functions.

The Cisco ONS 15454 supports SNMP Version 1 (SNMPv1) and SNMP Version 2c (SNMPv2c). These versions share many features, but SNMPv2c includes additional protocol operations and 64-bit performance monitoring support. This chapter describes both versions and gives SNMP configuration parameters for the ONS 15454.

Note The CERENT-MSDWDM-MIB.mib, CERENT-FC-MIB.mib, and CERENT-GENERIC-PM-MIB.mib in the CiscoV2 directory support 64-bit performance monitoring counters. The SNMPv1 MIB in the CiscoV1 directory does not contain 64-bit performance monitoring counters, but supports the lower and higher word values of the corresponding 64-bit counter. The other MIB files in the CiscoV1 and CiscoV2 directories are identical in content and differ only in format.

Figure 6-1 illustrates the basic layout idea of an SNMP-managed network.

Figure 6-1 Basic Network Managed by SNMP

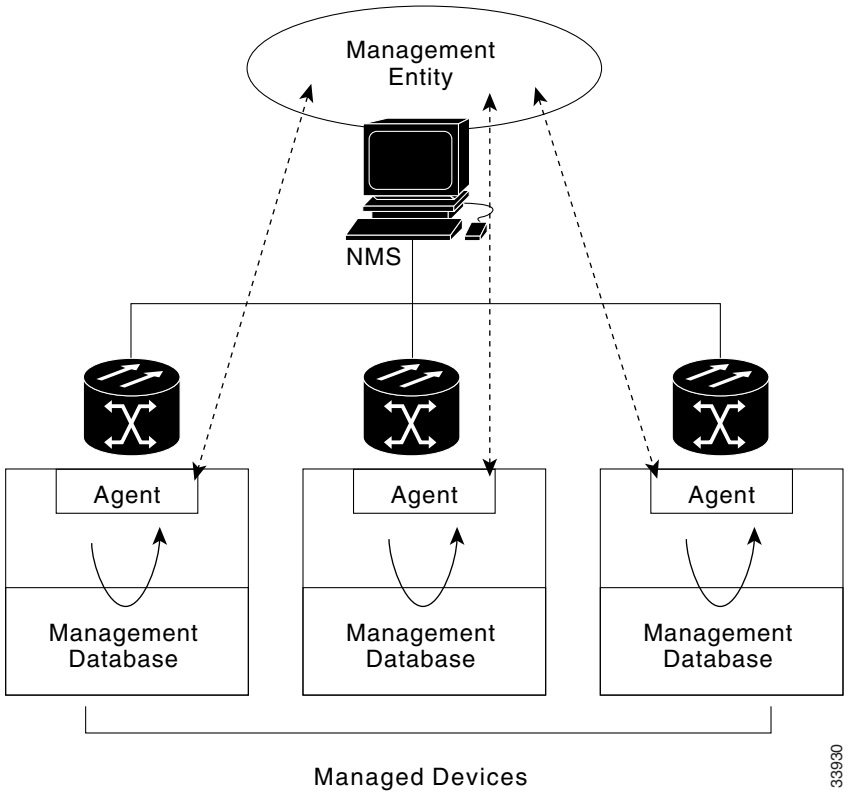


6.2 Basic SNMP Components

In general terms, an SNMP-managed network consists of a management system, agents, and managed devices.

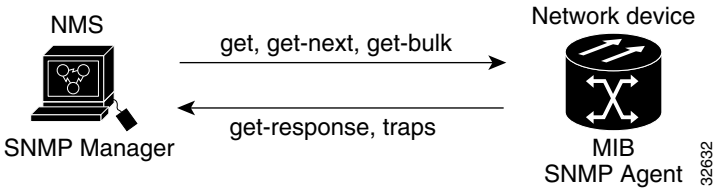
A management system such as HP OpenView executes monitoring applications and controls managed devices. Management systems execute most of the management processes and provide the bulk of memory resources used for network management. A network might be managed by one or more management systems. Figure 6-2 illustrates the relationship between the network manager, the SNMP agent, and the managed devices.

Figure 6-2 Example of the Primary SNMP Components



An agent (such as SNMP) residing on each managed device translates local management information data, such as performance information or event and error information caught in software traps, into a readable form for the management system. Figure 6-3 illustrates SNMP agent get-requests that transport data to the network management software.

Figure 6-3 Agent Gathering Data from a MIB and Sending Traps to the Manager



The SNMP agent captures data from MIBs, which are device parameter and network data repositories, or from error or change traps.

A managed element—such as a router, access server, switch, bridge, hub, computer host, or network element (such as an ONS 15454)—is accessed through the SNMP agent. Managed devices collect and store management information, making it available through SNMP to other management systems having the same protocol compatibility.

6.3 SNMP External Interface Requirement

Since all SNMP requests come from a third-party application, the only external interface requirement is that a third-part SNMP client application can upload RFC 3273 SNMP MIB variables in the etherStatsHighCapacityTable, etherHistoryHighCapacityTable, or mediaIndependentTable.

6.4 SNMP Version Support

The ONS 15454 supports SNMPv1 and SNMPv2c traps and get requests. The ONS 15454 SNMP MIBs define alarms, traps, and status. Through SNMP, NMS applications can query a management agent for data from functional entities such as Ethernet switches and SONET multiplexers using a supported MIB.

Note ONS 15454 MIB files in the CiscoV1 and CiscoV2 directories are almost identical in content except for the difference in 64-bit performance monitoring features. The CiscoV2 directory contains three MIBs with 64-bit performance monitoring counters:. CERENT-MSDWDM-MIB.mib, CERENT-FC-MIB.mib, and CERENT-GENERIC-PM-MIB.mib The CiscoV1 directory does not contain any 64-bit counters, but it does support the lower and higher word values used in 64-bit counters. The two directories also have somewhat different formats.

6.5 SNMP Message Types

The ONS 15454 SNMP agent communicates with an SNMP management application using SNMP messages. Table 6-1 describes these messages.

Table 6-1 ONS 15454 SNMP Message Types

Operation	Description
get-request	Retrieves a value from a specific variable.
get-next-request	Retrieves the value following the named variable; this operation is often used to retrieve variables from within a table. With this operation, an SNMP manager does not need to know the exact variable name. The SNMP manager searches sequentially to find the needed variable from within the MIB.
get-response	Replies to a get-request, get-next-request, get-bulk-request, or set-request sent by an NMS.
get-bulk-request	Fills the get-response with up to the max-repetition number of get-next interactions, similar to a get-next-request.
set-request	Provides remote network monitoring (RMON) MIB.
trap	Indicates that an event has occurred. An unsolicited message is sent by an SNMP agent to an SNMP manager.

6.6 SNMP Management Information Bases

Section 6.6.1 lists IETF-standard MIBs that are implemented in the ONS 15454 and shows their compilation order. Section 6.6.2 lists proprietary MIBs for the ONS 15454 and shows their compilation order. Section 6.6.3 contains information about the generic threshold and performance monitoring MIBs that can be used to monitor any network element (NE) contained in the network.

6.6.1 IETF-Standard MIBs for the ONS 15454

Table 6-2 lists the IETF-standard MIBs implemented in the ONS 15454 SNMP agents.

First compile the MIBs in Table 6-2. Compile the Table 6-3 MIBs next.

Caution If you do not compile MIBs in the correct order, one or more might not compile correctly.

Table 6-2 IETF Standard MIBs Implemented in the ONS 15454 System

RFC[1] Number	Module Name	Title/Comments
—	IANAifType-MIB.mib	Internet Assigned Numbers Authority (IANA) ifType
1213	RFC1213-MIB-rfc1213.mib	Management Information Base for Network
1907	SNMPV2-MIB-rfc1907.mib	Management of TCP/IP-based Internets: MIB-II Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)
1253	RFC1253-MIB-rfc1253.mib	OSPF Version 2 Management Information Base
1493	BRIDGE-MIB-rfc1493.mib	Definitions of Managed Objects for Bridges (This defines MIB objects for managing MAC bridges based on the IEEE 802.1D-1990 standard between Local Area Network [LAN] segments.)
2819	RMON-MIB-rfc2819.mib	Remote Network Monitoring Management Information Base
2737	ENTITY-MIB-rfc2737.mib	Entity MIB (Version 2)
2233	IF-MIB-rfc2233.mib	Interfaces Group MIB using SNMPv2
2358	EtherLike-MIB-rfc2358.mib	Definitions of Managed Objects for the Ethernet-like Interface Types
2493	PerfHist-TC-MIB-rfc2493.mib	Textual Conventions for MIB Modules Using Performance History Based on 15 Minute Intervals
2495	DS1-MIB-rfc2495.mib	Definitions of Managed Objects for the DS1, E1, DS2 and E2 Interface Types
2496	DS3-MIB-rfc2496.mib	Definitions of Managed Object for the DS3/E3 Interface Type
2558	SONET-MIB-rfc2558.mib	Definitions of Managed Objects for the SONET/SDH Interface Type

Table 6-2 IETF Standard MIBs Implemented in the ONS 15454 System (continued)

RFC[1] Number	Module Name	Title/Comments
2674	P-BRIDGE-MIB-rfc2674.mib Q-BRIDGE-MIB-rfc2674.mib	Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions
3273	HC-RMON-MIB	The MIB module for managing remote monitoring device implementations, augmenting the original RMON MIB as specified in RFC 2819 and RFC 1513 and RMON-2 MIB as specified in RFC 2021

1. RFC = Request for Comment

6.6.2 Proprietary ONS 15454 MIBs

Each ONS 15454 is shipped with a software CD containing applicable proprietary MIBs. Table 6-3 lists the proprietary MIBs for the ONS 15454.

Table 6-3 ONS 15454 Proprietary MIBs

MIB Number	Module Name
1	CERENT-GLOBAL-REGISTRY.mib
2	CERENT-TC.mib
3	CERENT-454.mib
4	CERENT-GENERIC.mib (not applicable to ONS 15454)
5	CISCO-SMI.mib
6	CISCO-VOA-MIB.mib
7	CERENT-MSDWDM-MIB.mib
8	CISCO-OPTICAL-MONITOR-MIB.mib
9	CERENT-HC-RMON-MIB.mib
10	CERENT-ENVMON-MIB.mib
11	CERENT-GENERIC-PM-MIB.mib

Note If you cannot compile the proprietary MIBs correctly, log into the Technical Support Website at http://www.cisco.com/techsupport or call Cisco TAC (1 800 553-2447).

Note When SNMP indicates that the wavelength is unknown, it means that the corresponding card (MXP_2.5G_10E, TXP_MR_10E, MXP_2.5G_10G, TXP_MR_10G, TXP_MR_2.5G, or TXPP_MR_2.5G) works with the first tunable wavelength. For more information about MXP and TXP cards, refer to the *Cisco ONS 15454 DWDM Installation and Operations Guide*.

6.6.3 Generic Threshold and Performance Monitoring MIBs

In Release 6.0, a new MIB called CERENT-GENERIC-PM-MIB allows network management stations (NMS) to use a single, generic MIB for accessing threshold and performance monitoring data of different interface types. The MIB is generic in the sense that it is not tied to any particular kind of interface. The MIB objects can be used to obtain threshold values, current performance monitoring (PM) counts, and historic PM statistics for each kind of monitor and any supported interval at the near end and far end.

Previously existing MIBs in the ONS 15454 system provide some of these counts. For example, SONET interface 15-minute current PM counts and historic PM statistics are available using the SONET-MIB. DS-1 and DS-3 counts and statistics are available through the DS1-MIB and DS-3 MIB respectively. The generic MIB provides these types of information and also fetches threshold values and single-day statistics. In addition, the MIB supports optics and dense wavelength division multiplexing (DWDM) threshold and performance monitoring information.

The CERENT-GENERIC-PM-MIB is organized into three different tables:

- cerentGenericPmThresholdTable
- cerentGenericPmStatsCurrentTable
- cerentGenericPmStatsIntervalTable

The cerentGenericPmThresholdTable is used to obtain the threshold values for the monitor types. It is indexed based on the interface index (cerentGenericPmThresholdIndex), monitor type (cerentGenericPmThresholdMonType), location (cerentGenericPmThresholdLocation), and time period (cerentGenericPmThresholdPeriod). The syntax of cerentGenericPmThresholdMonType is type cerentMonitorType, defined in CERENT-TC.mib. The syntax of cerentGenericPmThresholdLocation is type cerentLocation, defined in CERENT-TC.mib. The syntax of cerentGenericPmThresholdPeriod is type cerentPeriod, defined in CERENT-TC.mib.

Threshold values can be provided in 64-bit and 32-bit formats. (For more information about 64-bit counters, see the "6.10.2 HC-RMON-MIB Support" section on page 6-18.) The 64-bit values in cerentGenericPmThresholdHCValue can be used with agents that support SNMPv2. The two 32-bit values (cerentGenericPmThresholdValue and cerentGenericPmThresholdOverFlowValue) can be used by NMSs that only support SNMPv1. The objects compiled in the cerentGenericPmThresholdTable are shown in Table 6-4.

Table 6-4 cerentGenericPmThresholdTable

Index Objects	Information Objects
cerentGenericPmThresholdIndex	cerentGenericPmThresholdValue
cerentGenericPmThresholdMonType	cerentGenericPmThresholdOverFlowValue
cerentGenericPmThresholdLocation	cerentGenericPmThresholdHCValue
cerentGenericPmThresholdPeriod	—

The second table within the MIB, cerentGenericPmStatsCurrentTable, compiles the current performance monitoring (PM) values for the monitor types. The table is indexed based on interface index (cerentGenericPmStatsCurrentIndex), monitor type (cerentGenericPmStatsCurrentMonType), location (cerentGenericPmStatsCurrentLocation) and time period (cerentGenericPmStatsCurrentPeriod). The syntax of cerentGenericPmStatsCurrentIndex is type cerentLocation, defined in CERENT-TC.mib. The syntax of cerentGenericPmStatsCurrentMonType is type cerentMonitor, defined in CERENT-TC.mib. The syntax of cerentGenericPmStatsCurrentPeriod is type cerentPeriod, defined in CERENT-TC.mib.

The cerentGenericPmStatsCurrentTable validates the current PM value using the cerentGenericPmStatsCurrentValid object and registers the number of valid intervals with historical PM statistics in the cerentGenericPmStatsCurrentValidIntervals object.

PM values are provided in 64-bit and 32-bit formats. The 64-bit values in cerentGenericPmStatsCurrentHCValue can be used with agents that support SNMPv2. The two 32-bit values (cerentGenericPmStatsCurrentValue and cerentGenericPmStatsCurrentOverFlowValue) can be used by NMS that only support SNMPv1. The cerentGenericPmStatsCurrentTable is shown in Table 6-5.

Table 6-5 cerentGenericPmStatsCurrentTable

Index Objects	Informational Objects
cerentGenericPmStatsCurrentIndex	cerentGenericPmStatsCurrentValue
cerentGenericPmStatsCurrentMonType	cerentGenericPmStatsCurrentOverFlowValue
cerentGenericPmStatsCurrentLocation	cerentGenericPmStatsCurrentHCValue
cerentGenericPmStatsCurrentPeriod	cerentGenericPmStatsCurrentValidData
—	cerentGenericPmStatsCurrentValidIntervals

The third table in the MIB, cerentGenericPmStatsIntervalTable, obtains historic PM values for the monitor types. This table is indexed based on the interface index, monitor type, location, time period, and interval number. It validates the current PM value in the cerentGenericPmStatsIntervalValid object.

This table is indexed based on interface index (cerentGenericPmStatsIntervalIndex), monitor type (cerentGenericPMStatsIntervalMonType), location (cerentGenericPmStatsIntervalLocation), and period (cerentGenericPmStatsIntervalPeriod). The syntax of cerentGenericPmStatsIntervalIndex is type cerentLocation, defined in CERENT-TC.mib. The syntax of cerentGenericPmStatsIntervalMonType is type cerentMonitor, defined in CERENT-TC.mib. The syntax of cerentGernicPmStatsIntervalPeriod is type cerentPeriod, defined in CERENT-TC.mib.

The table provides historic PM values in 64-bit and 32-bit formats. The 64-bit values contained in the cerentGenericPmStatsIntervalHCValue table can be used with SNMPv2 agents. The two 32-bit values (cerentGenericPmStatsIntervalValue and cerentGenericPmStatsIntervalOverFlowValue) can be used by SNMPv1 NMS. The cerentGenericPmStatsIntervalTable is shown in Table 6-6.

Table 6-6 cerentGenericPmStatsIntervalTable

Index Objects	Informational Objects
cerentGenericPmStatsIntervalIndex	cerentGenericPmStatsIntervalValue
cerentGenericPmStatsIntervalMonType	cerentGenericPmStatsIntervalOverFlowValue
cerentGenericPmStatsIntervalLocation	cerentGenericPmStatsIntervalHCValue
cerentGenericPmStatsIntervalPeriod	cerentGenericPmStatsIntervalValidData
cerentGenericPmStatsIntervalNumber	—

6.7 SNMP Trap Content

The ONS 15454 generates all alarms and events, such as raises and clears, as SNMP traps. These contain the following information:

- Object IDs that uniquely identify each event with information about the generating entity (the slot or port; synchronous transport signal [STS] and Virtual Tributary [VT]; bidirectional line switched ring [BLSR], Spanning Tree Protocol [STP], etc.).
- Severity and service effect of the alarm (critical, major, minor, or event; service-affecting or non-service-affecting).
- Date and time stamp showing when the alarm occurred.

6.7.1 Generic and IETF Traps

The ONS 15454 supports the generic IETF traps listed in Table 6-7.

Table 6-7 Generic IETF Traps

Trap	From RFC No. MIB	Description
coldStart	RFC1907-MIB	Agent up, cold start.
warmStart	RFC1907-MIB	Agent up, warm start.
authenticationFailure	RFC1907-MIB	Community string does not match.
newRoot	RFC1493/ BRIDGE-MIB	Sending agent is the new root of the spanning tree.
topologyChange	RFC1493/ BRIDGE-MIB	A port in a bridge has changed from Learning to Forwarding or Forwarding to Blocking.
entConfigChange	RFC2737/ ENTITY-MIB	The entLastChangeTime value has changed.
dsx1LineStatusChange	RFC2495/ DS1-MIB	The value of an instance of dsx1LineStatus has changed. The trap can be used by an NMS to trigger polls. When the line status change results from a higher-level line status change (for example, a DS-3), no traps for the DS-1 are sent.
dsx3LineStatusChange	RFC2496/ DS3-MIB	The value of an instance of dsx3LineStatus has changed. This trap can be used by an NMS to trigger polls. When the line status change results in a lower-level line status change (for example, a DS-1), no traps for the lower-level are sent.
risingAlarm	RFC2819/ RMON-MIB	The SNMP trap that is generated when an alarm entry crosses the rising threshold and the entry generates an event that is configured for sending SNMP traps.
fallingAlarm	RFC2819/ RMON-MIB	The SNMP trap that is generated when an alarm entry crosses the falling threshold and the entry generates an event that is configured for sending SNMP traps.

6.7.2 Variable Trap Bindings

Each SNMP trap contains variable bindings that are used to create the MIB tables. ONS 15454 traps and variable bindings are listed in Table 6-8. For each group (such as Group A), all traps within the group are associated with all of its variable bindings.

Table 6-8 ONS 15454 SNMPv2 Trap Variable Bindings

Group	Trap Name(s) Associated with	Variable Binding Number	SNMPv2 Variable Bindings	Description
A	dsx1LineStatusChange (from RFC 2495)	(1)	dsx1LineStatus	This variable indicates the line status of the interface. It contains loopback, failure, received alarm and transmitted alarm information.
		(2)	dsx1LineStatusLastChange	The value of MIB II's sysUpTime object at the time this DS1 entered its current line status state. If the current state was entered prior to the last proxy-agent reinitialization, the value of this object is zero.
		(3)	cerent454NodeTime	The time that an event occurred.
		(4)	cerent454AlarmState	The alarm severity and service-affecting status. Severities are Minor, Major, and Critical. Service-affecting statuses are Service-Affecting and Non-Service Affecting.
		(5)	snmpTrapAddress	The address of the SNMP trap.
B	dsx3LineStatusChange (from RFC 2496)	(1)	dsx3LineStatus	This variable indicates the line status of the interface. It contains loopback state information and failure state information.
		(2)	dsx3LineStatusLastChange	The value of MIB II's sysUpTime object at the time this DS3/E3 entered its current line status state. If the current state was entered prior to the last reinitialization of the proxy-agent, then the value is zero.
		(3)	cerent454NodeTime	The time that an event occurred.

Table 6-8 ONS 15454 SNMPv2 Trap Variable Bindings (continued)

Group	Trap Name(s) Associated with	Variable Binding Number	SNMPv2 Variable Bindings	Description
B (cont.)		(4)	cerent454AlarmState	The alarm severity and service-affecting status. Severities are Minor, Major, and Critical. Service-affecting statuses are Service-Affecting and Non-Service Affecting.
		(5)	snmpTrapAddress	The address of the SNMP trap.
C	coldStart (from RFC 1907)	(1)	cerent454NodeTime	The time that the event occurred.
	warmStart (from RFC 1907)	(2)	cerent454AlarmState	The alarm severity and service-affecting status. Severities are Minor, Major, and Critical. Service-affecting statuses are Service-Affecting and Non-Service Affecting.
	newRoot (from RFC)	(3)	snmpTrapAddress	The address of the SNMP trap.
	topologyChange (from RFC)		—	—
	entConfigChange (from RFC 2737)		—	—
	authenticationFailure (from RFC 1907)		—	—
D1	risingAlarm (from RFC 2819)	(1)	alarmIndex	This variable uniquely identifies each entry in the alarm table. When an alarm in the table clears, the alarm indexes change for each alarm listed.
		(2)	alarmVariable	The object identifier of the variable being sampled.
		(3)	alarmSampleType	The method of sampling the selected variable and calculating the value to be compared against the thresholds.
		(4)	alarmValue	The value of the statistic during the last sampling period.

Table 6-8 ONS 15454 SNMPv2 Trap Variable Bindings (continued)

Group	Trap Name(s) Associated with	Variable Binding Number	SNMPv2 Variable Bindings	Description
D1 (cont.)		(5)	alarmRisingThreshold	When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single event is generated. A single event is also generated if the first sample after this entry is greater than or equal to this threshold.
		(6)	cerent454NodeTime	The time that an event occurred.
		(7)	cerent454AlarmState	The alarm severity and service-affecting status. Severities are Minor, Major, and Critical. Service-affecting statuses are Service-Affecting and Non-Service Affecting.
		(8)	snmpTrapAddress	The address of the SNMP trap.
D2	fallingAlarm (from RFC 2819)	(1)	alarmIndex	This variable uniquely identifies each entry in the alarm table. When an alarm in the table clears, the alarm indexes change for each alarm listed.
		(2)	alarmVariable	The object identifier of the variable being sampled.
		(3)	alarmSampleType	The method of sampling the selected variable and calculating the value to be compared against the thresholds.
		(4)	alarmValue	The value of the statistic during the last sampling period.
		(5)	alarmFallingThreshold	When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, a single event is generated. A single is also generated if the first sample after this entry is less than or equal to this threshold.
		(6)	cerent454NodeTime	The time that an event occurred.

Table 6-8 ONS 15454 SNMPv2 Trap Variable Bindings (continued)

Group	Trap Name(s) Associated with	Variable Binding Number	SNMPv2 Variable Bindings	Description
D2 (cont.)		(7)	cerent454AlarmState	The alarm severity and service-affecting status. Severities are Minor, Major, and Critical. Service-affecting statuses are Service-Affecting and Non-Service Affecting.
		(8)	snmpTrapAddress	The address of the SNMP trap.
E	failureDetectedExternal ToTheNE (from CERENT-454-mib)	(1)	cerent454NodeTime	The time that an event occurred.
		(2)	cerent454AlarmState	The alarm severity and service-affecting status. Severities are Minor, Major, and Critical. Service-affecting statuses are Service-Affecting and Non-Service Affecting.
		(3)	cerent454AlarmObjectType	The entity that raised the alarm. The NMS should use this value to decide which table to poll for further information about the alarm.
		(4)	cerent454AlarmObjectIndex	Every alarm is raised by an object entry in a specific table. This variable is the index of objects in each table; if the alarm is interface-related, this is the index of the interface in the interface table.
		(5)	cerent454AlarmSlotNumber	The slot of the object that raised the alarm. If a slot is not relevant to the alarm, the slot number is zero.
		(6)	cerent454AlarmPortNumber	The port of the object that raised the alarm. If a port is not relevant to the alarm, the port number is zero.
		(7)	cerent454AlarmLineNumber	The object line that raised the alarm. If a line is not relevant to the alarm, the line number is zero.
		(8)	cerent454AlarmObjectName	The TL1-style user-visible name that uniquely identifies an object in the system.

Table 6-8 ONS 15454 SNMPv2 Trap Variable Bindings (continued)

Group	Trap Name(s) Associated with	Variable Binding Number	SNMPv2 Variable Bindings	Description
E (cont.)		(9)	cerent454AlarmAdditionalInfo	Additional information for the alarm object. In the current version of the MIB, this object contains provisioned description for alarms that are external to the NE. If there is no additional information, the value is zero.
		(10)	snmpTrapAddress	The address of the SNMP trap.
F	performanceMonitor ThresholdCrossingAlert (from CERENT-454-mib)	(1)	cerent454NodeTime	The time that an event occurred.
		(2)	cerent454AlarmState	The alarm severity and service-affecting status. Severities are Minor, Major, and Critical. Service-affecting statuses are Service-Affecting and Non-Service Affecting.
		(3)	cerent454AlarmObjectType	The entity that raised the alarm. The NMS should use this value to decide which table to poll for further information about the alarm.
		(4)	cerent454AlarmObjectIndex	Every alarm is raised by an object entry in a specific table. This variable is the index of objects in each table; if the alarm is interface-related, this is the index of the interface in the interface table.
		(5)	cerent454AlarmSlotNumber	The slot of the object that raised the alarm. If a slot is not relevant to the alarm, the slot number is zero.
		(6)	cerent454AlarmPortNumber	The port of the object that raised the alarm. If a port is not relevant to the alarm, the port number is zero.
		(7)	cerent454AlarmLineNumber	The object line that raised the alarm. If a line is not relevant to the alarm, the line number is zero.
		(8)	cerent454AlarmObjectName	The TL1-style user-visible name that uniquely identifies an object in the system.
		(9)	cerent454ThresholdMonitorType	This object indicates the type of metric being monitored.

Table 6-8 ONS 15454 SNMPv2 Trap Variable Bindings (continued)

Group	Trap Name(s) Associated with	Variable Binding Number	SNMPv2 Variable Bindings	Description
F (cont.)		(10)	cerent454ThresholdLocation	Indicates whether the event occurred at the near or far end.
		(11)	cerent454ThresholdPeriod	Indicates the sampling interval period.
		(12)	cerent454ThresholdSetValue	The value of this object is the threshold provisioned by the NMS.
		(13)	cerent454ThresholdCurrentValue	—
		(14)	cerent454ThresholdDetectType	—
		(15)	snmpTrapAddress	The address of the SNMP trap.
G	All other traps (from CERENT-454-MIB) not listed above	(1)	cerent454NodeTime	The time that an event occurred.
		(2)	cerent454AlarmState	The alarm severity and service-affecting status. Severities are Minor, Major, and Critical. Service-affecting statuses are Service-Affecting and Non-Service Affecting.
		(3)	cerent454AlarmObjectType	The entity that raised the alarm. The NMS should use this value to decide which table to poll for further information about the alarm.
		(4)	cerent454AlarmObjectIndex	Every alarm is raised by an object entry in a specific table. This variable is the index of objects in each table; if the alarm is interface-related, this is the index of the interface in the interface table.
		(5)	cerent454AlarmSlotNumber	The slot of the object that raised the alarm. If a slot is not relevant to the alarm, the slot number is zero.
		(6)	cerent454AlarmPortNumber	The port of the object that raised the alarm. If a port is not relevant to the alarm, the port number is zero.
		(7)	cerent454AlarmLineNumber	The object line that raised the alarm. If a line is not relevant to the alarm, the line number is zero.

Table 6-8 ONS 15454 SNMPv2 Trap Variable Bindings (continued)

Group	Trap Name(s) Associated with	Variable Binding Number	SNMPv2 Variable Bindings	Description
G (cont.)		(8)	cerent454AlarmObjectName	The TL1-style user-visible name that uniquely identifies an object in the system.
		(9)	snmpTrapAddress	The address of the SNMP trap.

6.8 SNMP Community Names

Community names are used to group SNMP trap destinations. All ONS 15454 trap destinations can be provisioned as part of SNMP communities in Cisco Transport Controller (CTC). When community names are assigned to traps, the ONS 15454 treats the request as valid if the community name matches one that is provisioned in CTC. In this case, all agent-managed MIB variables are accessible to that request. If the community name does not match the provisioned list, SNMP drops the request.

6.9 Proxy Over Firewalls

SNMP and NMS applications have traditionally been unable to cross firewalls used for isolating security risks inside or from outside networks. Release 6.0 CTC enables network operations centers (NOCs) to access performance monitoring data such as RMON statistics or autonomous messages across firewalls by using an SMP proxy element installed on a firewall.

The application-level proxy transports SNMP protocol data units (PDU) between the NMS and NEs, allowing requests and responses between the NMS and NEs and forwarding NE autonomous messages to the NMS. The proxy agent requires little provisioning at the NOC and no additional provisioning at the NEs.

The firewall proxy is intended for use in a gateway network element-end network element (GNE-ENE) topology with many NEs through a single NE gateway. Up to 64 SNMP requests (such as get, getnext, or getbulk) are supported at any time behind single or multiple firewalls. The proxy interoperates with common NMS such as HP OpenView.

For security reasons, the SNMP proxy feature must be enabled at all receiving and transmitting NEs to function. For instructions to do this, refer to the *Cisco ONS 15454 Procedure Guide*.

6.10 Remote Monitoring

The ONS 15454 incorporates RMON to allow network operators to monitor Ethernet card performance and events. The RMON thresholds are user-provisionable in CTC. Refer to the *Cisco ONS 15454 Procedure Guide* for instructions. Note that otherwise, RMON operation is invisible to the typical CTC user.

ONS 15454 system RMON is based on the IETF-standard MIB RFC 2819 and includes the following five groups from the standard MIB: Ethernet Statistics, History Control, Ethernet History, Alarm, and Event.

6.10.1 64-Bit RMON Monitoring over DCC

The ONS 15454 DCC is implemented over the IP protocol, which is not compatible with Ethernet. The system builds Ethernet equipment History and Statistics tables using HDLC statistics that are gathered over the DCC (running point-topoint protocol, or PPP). This release adds RMON DCC monitoring (for both IP and Ethernet) to monitor the health of remote DCC connections.

In R6.0, the implementation contains two MIBS for DCC interfaces. They are:

- cMediaIndependentTable—standard, rfc3273; the proprietary extension of the HC-RMON MIB used for reporting statistics
- cMediaIndependentHistoryTable—proprietary MIB used to support history

6.10.1.1 Row Creation in MediaIndependentTable

The SetRequest PDU for creating a row in the mediaIndependentTable should contain all the values required to activate a row in a single set operation along with an assignment of the status variable to createRequest (2). The SetRequest PDU for entry creation must have all the object IDs (OIDs) carrying an instance value of 0. That is, all the OIDs should be of the type OID.0.

In order to create a row, the SetRequest PDU should contain the following:

- mediaIndependentDataSource and its desired value
- mediaIndependentOwner and its desired value (The size of mediaIndependentOwner is limited to 32 characters.)
- mediaIndependentStatus with a value of createRequest (2)

The mediaIndependentTable creates a row if the SetRequest PDU is valid according to the above rules. When the row is created, the SNMP agent decides the value of mediaIndependentIndex. This value is not sequentially allotted or contiguously numbered. It changes when an Ethernet interface is added or deleted. The newly created row will have mediaIndependentTable value of valid (1).

If the row already exists, or if the SetRequest PDU values are insufficient or do not make sense, the SNMP agent returns an error code.

Note mediaIndependentTable entries are not preserved if the SNMP agent is restarted.

The mediaIndependentTable deletes a row if the SetRequest PDU contains a mediaIndependentStatus with a value of invalid (4). The varbind's OID instance value identifies the row for deletion. You can recreate a deleted row in the table if desired.

6.10.1.2 Row Creation in cMediaIndependentHistoryControlTable

SNMP row creation and deletion for the cMediaIndependentHistoryControlTable follows the same processes as for the MediaIndependentTable; only the variables differ.

In order to create a row, the SetRequest PDU should contain the following:

- cMediaIndependentHistoryControlDataSource and its desired value
- cMediaIndependentHistoryControlOwner and its desired value
- cMediaIndependentHistoryControlStatus with a value of createRequest (2)

6.10.2 HC-RMON-MIB Support

For the ONS 15454, the implementation of the high-capacity remote monitoring information base (HC-RMON-MIB, or RFC 3273) enables 64-bit support of existing RMON tables. This support is provided with the etherStatsHighCapacityTable and the etherHistoryHighCapacityTable. An additional table, the mediaIndependentTable, and an additional object, hcRMONCapabilities, are also added for this support. All of these elements are accessible by any third-party SNMP client having RFC 3273 support.

6.10.3 Ethernet Statistics RMON Group

The Ethernet Statistics group contains the basic statistics monitored for each subnetwork in a single table called the etherStatsTable.

6.10.3.1 Row Creation in etherStatsTable

The SetRequest PDU for creating a row in this table should contain all the values needed to activate a row in a single set operation, and an assigned status variable to createRequest. The SetRequest PDU object ID (OID) entries must all carry an instance value, or type OID, of 0.

In order to create a row, the SetRequest PDU should contain the following:

- The etherStatsDataSource and its desired value
- The etherStatsOwner and its desired value (size of this value is limited to 32 characters)
- The etherStatsStatus with a value of createRequest (2)

The etherStatsTable creates a row if the SetRequest PDU is valid according to the above rules. When the row is created, the SNMP agent decides the value of etherStatsIndex. This value is not sequentially allotted or contiguously numbered. It changes when an Ethernet interface is added or deleted. The newly created row will have etherStatsStatus value of valid (1).

If the etherStatsTable row already exists, or if the SetRequest PDU values are insufficient or do not make sense, the SNMP agent returns an error code.

Note EtherStatsTable entries are not preserved if the SNMP agent is restarted.

6.10.3.2 Get Requests and GetNext Requests

Get requests and getNext requests for the etherStatsMulticastPkts and etherStatsBroadcastPkts columns return a value of zero because the variables are not supported by ONS 15454 Ethernet cards.

6.10.3.3 Row Deletion in etherStatsTable

To delete a row in the etherStatsTable, the SetRequest PDU should contain an etherStatsStatus “invalid” value (4). The OID marks the row for deletion. If required, a deleted row can be recreated.

6.10.3.4 64-Bit etherStatsHighCapacity Table

The Ethernet statistics group contains 64-bit statistics in the etherStatsHighCapacityTable, which provides 64-bit RMON support for the HC-RMON-MIB. The etherStatsHighCapacityTable is an extension of the etherStatsTable that adds 16 new columns for performance monitoring data in 64-bit format. There is a one-to-one relationship between the etherStatsTable and etherStatsHighCapacityTable when rows are created or deleted in either table.

6.10.4 History Control RMON Group

The History Control group defines sampling functions for one or more monitor interfaces in the historyControlTable. The values in this table, as specified in RFC 2819, are derived from the historyControlTable and etherHistoryTable.

6.10.4.1 History Control Table

The RMON is sampled at one of four possible intervals. Each interval, or period, contains specific history values (also called buckets). Table 6-9 lists the four sampling periods and corresponding buckets.

The historyControlTable maximum row size is determined by multiplying the number of ports on a card by the number of sampling periods. For example, an ONS 15454 E100 card contains 24 ports, which multiplied by periods allows 96 rows in the table. An E1000 card contains 14 ports, which multiplied by four periods allows 56 table rows.

Table 6-9 RMON History Control Periods and History Categories

Sampling Periods (historyControlValue Variable)	Total Values, or Buckets (historyControl Variable)
15 minutes	32
24 hours	7
1 minute	60
60 minutes	24

6.10.4.2 Row Creation in historyControlTable

The SetRequest PDU must be able to activate a historyControlTable row in one single-set operation. In order to do this, the PDU must contain all needed values and have a status variable value of 2 (createRequest). All OIDs in the SetRequest PDU should be type OID.0 type for entry creation.

To create a SetRequest PDU for the historyControlTable, the following values are required:

- The historyControlDataSource and its desired value
- The historyControlBucketsRequested and it desired value
- The historyControlInterval and its desired value
- The historyControlOwner and its desired value
- The historyControlStatus with a value of createRequest (2)

The historyControlBucketsRequested OID value is ignored because the number of buckets allowed for each sampling period, based upon the historyControlInterval value, is already fixed as listed in Table 6-9.

The historyControlInterval value cannot be changed from the four allowed choices. If you use another value, the SNMP agent selects the closest smaller time period from the set buckets. For example, if the set request specifies a 25-minute interval, this falls between the 15-minute (32 bucket) variable and the 60-minute (24 bucket) variable. The SNMP agent automatically selects the lower, closer value, which is 15 minutes, so it allows 32 buckets.

If the SetRequest PDU is valid, a historyControlTable row is created. If the row already exists, or if the SetRequest PDU values do not make sense or are insufficient, the SNMP agent does not create the row and returns an error code.

6.10.4.3 Get Requests and GetNext Requests

These PDUs are not restricted.

6.10.4.4 Row Deletion in historyControl Table

To delete a row from the table, the SetRequest PDU should contain a historyControlStatus value of 4 (invalid). A deleted row can be recreated.

6.10.5 Ethernet History RMON Group

The ONS 15454 implements the etherHistoryTable as defined in RFC 2819. The group is created within the bounds of the historyControlTable and does not deviate from the RFC in its design.

6.10.5.1 64-Bit etherHistoryHighCapacityTable

64-bit Ethernet history for the HC-RMON-MIB is implemented in the etherHistoryHighCapacityTable, which is an extension of the etherHistoryTable. The etherHistoryHighCapacityTable adds four columns for 64-bit performance monitoring data. These two tables have a one-to-one relationship. Adding or deleting a row in one table will effect the same change in the other.

6.10.6 Alarm RMON Group

The Alarm group consists of the alarmTable, which periodically compares sampled values with configured thresholds and raises an event if a threshold is crossed. This group requires the implementation of the event group, which follows this section.

6.10.6.1 Alarm Table

The NMS uses the alarmTable to determine and provision network performance alarmable thresholds.

6.10.6.2 Row Creation in alarmTable

To create a row in the alarmTable, the SetRequest PDU must be able to create the row in one single-set operation. All OIDs in the SetRequest PDU should be type OID.0 type for entry creation. The table has a maximum number of 256 rows.

To create a SetRequest PDU for the alarmTable, the following values are required:

- The alarmInterval and its desired value
- The alarmVariable and its desired value
- The alarmSampleType and its desired value
- The alarmStartupAlarm and its desired value
- The alarmOwner and its desired value
- The alarmStatus with a value of createRequest (2)

If the SetRequest PDU is valid, a historyControlTable row is created. If the row already exists, or if the SetRequest PDU values do not make sense or are insufficient, the SNMP agent does not create the row and returns an error code.

In addition to the required values, the following restrictions must be met in the SetRequest PDU:

- The alarmOwner is a string of length 32 characters.
- The alarmRisingEventIndex always takes value 1.
- The alarmFallingEventIndex always takes value 2.
- The alarmStatus has only two values supported in SETs: createRequest (2) and invalid (4).
- The AlarmVariable is of the type OID.ifIndex, where ifIndex gives the interface this alarm is created on and OID is one of the OIDs supported in Table 6-10.

Table 6-10 OIDs Supported in the AlarmTable

No.	Column Name	OID	Status
1	ifInOctets	{1.3.6.1.2.1.2.2.1.10}	—
2	IfInUcastPkts	{1.3.6.1.2.1.2.2.1.11}	—
3	ifInMulticastPkts	{1.3.6.1.2.1.31.1.1.1.2}	Unsupported in E100/E1000
4	ifInBroadcastPkts	{1.3.6.1.2.1.31.1.1.1.3}	Unsupported in E100/E1000
5	ifInDiscards	{1.3.6.1.2.1.2.2.1.13}	Unsupported in E100/E1000
6	ifInErrors	{1.3.6.1.2.1.2.2.1.14}	—
7	ifOutOctets	{1.3.6.1.2.1.2.2.1.16}	—
8	ifOutUcastPkts	{1.3.6.1.2.1.2.2.1.17}	—
9	ifOutMulticastPkts	{1.3.6.1.2.1.31.1.1.1.4}	Unsupported in E100/E1000
10	ifOutBroadcastPkts	{1.3.6.1.2.1.31.1.1.1.5}	Unsupported in E100/E1000
11	ifOutDiscards	{1.3.6.1.2.1.2.2.1.19}	Unsupported in E100/E1000
12	Dot3StatsAlignmentErrors	{1.3.6.1.2.1.10.7.2.1.2}	—
13	Dot3StatsFCSErrors	{1.3.6.1.2.1.10.7.2.1.3}	—
14	Dot3StatsSingleCollisionFrames	{1.3.6.1.2.1.10.7.2.1.4}	—
15	Dot3StatsMultipleCollisionFrames	{1.3.6.1.2.1.10.7.2.1.5}	—
16	Dot3StatsDeferredTransmissions	{1.3.6.1.2.1.10.7.2.1.7}	—
17	Dot3StatsLateCollisions	{1.3.6.1.2.1.10.7.2.1.8}	—
18	Dot3StatsExcessiveCollisions	{13.6.1.2.1.10.7.2.1.9}	—
19	Dot3StatsFrameTooLong	{1.3.6.1.2.1.10.7.2.1.13}	—
20	Dot3StatsCarrierSenseErrors	{1.3.6.1.2.1.10.7.2.1.11}	Unsupported in E100/E1000

Table 6-10 OIDs Supported in the AlarmTable (continued)

No.	Column Name	OID	Status
21	Dot3StatsSQETestErrors	{1.3.6.1.2.1.10.7.2.1.6}	Unsupported in E100/E1000
22	etherStatsUndersizePkts	{1.3.6.1.2.1.16.1.1.1.9}	—
23	etherStatsFragments	{1.3.6.1.2.1.16.1.1.1.11}	—
24	etherStatsPkts64Octets	{1.3.6.1.2.1.16.1.1.1.14}	—
25	etherStatsPkts65to127Octets	{1.3.6.1.2.1.16.1.1.1.15}	—
26	etherStatsPkts128to255Octets	{1.3.6.1.2.1.16.1.1.1.16}	—
27	etherStatsPkts256to511Octets	{1.3.6.1.2.1.16.1.1.1.17}	—
28	etherStatsPkts512to1023Octets	{1.3.6.1.2.1.16.1.1.1.18}	—
29	etherStatsPkts1024to1518Octets	{1.3.6.1.2.1.16.1.1.1.19}	—
30	EtherStatsBroadcastPkts	{1.3.6.1.2.1.16.1.1.1.6}	—
31	EtherStatsMulticastPkts	{1.3.6.1.2.1.16.1.1.1.7}	—
32	EtherStatsOversizePkts	{1.3.6.1.2.1.16.1.1.1.10}	—
33	EtherStatsJabbers	{1.3.6.1.2.1.16.1.1.1.12}	—
34	EtherStatsOctets	{1.3.6.1.2.1.16.1.1.1.4}	—
35	EtherStatsCollisions	{1.3.6.1.2.1.16.1.1.1.13}	—
36	EtherStatsCollisions	{1.3.6.1.2.1.16.1.1.1.8}	—
37	EtherStatsDropEvents	{1.3.6.1.2.1.16.1.1.1.3}	Unsupported in E100/E1000 and G1000

6.10.6.3 Get Requests and GetNext Requests

These PDUs are not restricted.

6.10.6.4 Row Deletion in alarmTable

To delete a row from the table, the SetRequest PDU should contain an alarmStatus value of 4 (invalid). A deleted row can be recreated. Entries in this table are preserved if the SNMP agent is restarted.

6.10.7 Event RMON Group

The Event group controls event generation and notification. It consists of two tables: the eventTable, which is a read-only list of events to be generated, and the logTable, which is a writable set of data describing a logged event. The ONS 15454 implements the logTable as specified in RFC 2819.

6.10.7.1 Event Table

The eventTable is read-only and unprovisionable. The table contains one row for rising alarms and another for falling ones. This table has the following restrictions:

- The eventType is always log-and-trap (4).

- The eventCommunity value is always a zero-length string, indicating that this event causes the trap to be despatched to all provisioned destinations.
- The eventOwner column value is always “monitor.”
- The eventStatus column value is always valid(1).

6.10.7.2 Log Table

The logTable is implemented exactly as specified in RFC 2819. The logTable is based upon data that is locally cached in a controller card. If there is a controller card protection switch, the existing logTable is cleared and a new one is started on the newly active controller card. The table contains as many rows as provided by the alarm controller.

Numerics

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

X